

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

## دور الضبط الإدارى الإلكتروني 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 الإدارى الإلكتروني فى 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 خياراً حتمياً لجهة الإدارة، وتنعكس تلك الحتمية على النشاط الفردي، حيث إذا لم تفلح جهة الإدارة في الحفاظ على أمنها السيبراني؛ سترتب 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 عائقاً 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 دوراً 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 كالفعلية والتأثير.

**الكلمات الرئيسية:** الأمن السيبراني - الضبط الإداري الإلكتروني - 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 السيبراني يملئ ضرورة الحديث كمقدمة ضرورية ولازمة عن فكرة الوجود القانوني لغايات الدولة، ذلك أن البعض ينكر هذا الوجود من منظور أن الحديث عن مهام الدولة هو الحديث عن وجهة نظر متجاوزة للقانون»<sup>(١)</sup>.

يعد الأمن السيبراني خياراً حتمياً لجهة الإدارة؛ وبالتالي تنعكس تلك الحتمية على النشاط الفردي. فإن لم تفلح جهة الإدارة في الحفاظ على أمنها السيبراني؛ سيترتب على ذلك موجات من الاضطرابات في شبكاتنا السيبرانية، مما يؤثر على دقة ومصداقية البيانات والمعلومات، ويحد من إمكانية تداولها.

لذا إن لم يكن الفضاء السيبراني وسيلة موثوقة بها للاتصال أو التجارة، فسيبتعد الأفراد كما الشركات عن الاستثمار بل وسيؤثر ذلك على الصعيد الدولي في جهود تطوير اختراعات وتكنولوجيات حديثة، وبالتالي سيكون ذلك عائقاً في سبيل التعاون بين الدول، ويزيد من احتمالية ذلك الفرض التقاعس الحكومي في دول العالم - خاصة العالم الثالث - عن توفير وتطبيق الإجراءات الدفاعية اللازمة<sup>(٢)</sup>.

أضف إلى ذلك أنه رغم التطور الكبير في علم الحاسبات الإلكترونية إلا أن مسألة الأمن السيبراني لم تحظ بعد بالتطور المطلوب، فاعتراض المعلومات والتطفل عليها والعبث بها لم يعد حكراً على الجواسيس والخبراء العسكريين؛ وإنما أصبح هوية للأشخاص العاديين مما شكل في حد ذاته تهديداً حقيقياً للمنظمات الحكومية والخاصة<sup>(٣)</sup>.

ومما يزيد الإشكالية تعقيداً «الاستخدام العام للبريد الإلكتروني ووصول الجمهور لمواقع الويب "web sites" عبر الإنترنت، وسهولة الوصول إلى المعلومات في 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، ص ٣٨٨.

(٢) 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.

(٣) باستطاعة طفل لا يتجاوز عمره ١٢ عاماً إطلاق هجوم إلكتروني على أي مؤسسة من أي مكان في العالم.

عن بعد المسافات الجغرافية مما مكن المستخدمين من اصطناع فضاء جديد يسمى «الفضاء السيبرانى» والذي يستعمل أساساً لأغراض شرعية ولكن يمكن أن يخضع لسوء الاستخدام»<sup>(١)</sup>.

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

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

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

## المبحث التمهيدي

### تعريف (القضاء السيبراني والخطر السيبراني والأمن السيبراني)

#### المطلب الأول

#### تعريف القضاء السيبراني

القضاء الإلكتروني أو القضاء السيبراني هو الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني». وبمفهوم أشمل يعرف بأنه «مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمى كل هذه العناصر»<sup>(1)</sup>.

ويذهب البعض إلى أن مصطلح القضاء السيبراني، أو القضاء الإلكتروني، ظهر لأول مرة عام ١٩٨٢، فى رواية خيال علمي، للكاتب William Gibson، باسم Neuromancer، ولا يوجد تعريف واحد، متفق عليه دولياً لمصطلح القضاء السيبراني، إنما بعض التعريفات، المقبولة، على مستويات مختلفة، مثل الأمن القومي، وأمن المعلومات. وبعيداً عن رواية William Gibson، فالقضاء السيبراني لم يعد خيالاً علمياً، بل أصبح واقعاً علمياً، ذا تأثيرات اجتماعية وسياسية واقتصادية<sup>(2)</sup>.

فلغوياً يشتق لفظ Cyber، من الكلمة اللاتينية Kubernts بمعنى قائد الدفة، فى إشارة إلى القيادة والإدارة، إلا أن اللفظ التصق لاحقاً، بكل ما يخص القضاء Space، واستخدم فى كل ما يتعلق بالإنترنت بعد ظهوره وانتشار استخدامه بشكل كبير. فصار من المعلوم أن القضاء السيبراني، أو القضاء الإلكتروني، هو 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](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)

اشتهر المصطلح فى التسعينيات بعدما أصبحت استخدامات الإنترنت والشبكات والاتصال الرقمى تتمو بشكل كبير وأصبح مصطلح القضاء الإلكتروني قادراً على تمثيل العديد من الأفكار والطواهر الجديدة التى ظهرت. يُعتقد أن هناك قواعد وأخلاقيات مشتركة تعود بالنفع المتبادل على الجميع ليتم اتباعها، ويشار إليها باسم أخلاقيات الإنترنت. يرى الكثيرون أن الحق فى الخصوصية هو الحق الأكثر أهمية فى أخلاقيات الإنترنت.

(٢) د/سمير فرج: القضاء السيبراني-مقال منشور بالموقع الإلكتروني لجريدة الأهرام المصرية بتاريخ ٣٠ يوليو ٢٠٢٠- آخر

تحديث ٢٠٢١/٨/٢٠ <https://gate.ahram.org.eg/News/2444508.aspx>

وتعمل فيه شبكات الحواسيب الإلكترونية، في العالم كله، بما في ذلك أجهزة الكمبيوتر، وأنظمة الشبكات، والبرمجيات، وحوسبة المعلومات، ونقلها، وتخزينها، ومستخدميها من البشر والهيئات والمؤسسات<sup>(١)</sup>.

## المطلب الثاني

### تعريف الخطر السيبراني

بداية قبل تعريف الأمن السيبراني يجدر بنا أن نقوم بتعريف الخطر السيبراني، وقد قام بعض الباحثين بتعريفه بأنه: خطر جديد يواجه المؤسسات وجهات الإدارة ويكون مرتبطاً بالتطور التكنولوجي، وتدفعات المعلومات<sup>(٢)</sup>.

وفي اعتقادنا أن الخطر السيبراني 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 أشكال الخطر السيبراني ما بين التهديد بالاضطراب في تدفق المعلومات، أو التهديد باستغلال المعلومات الحساسة، والسرية، والملكية السيبرانية، أو التهديد بانتقاء المعلومات لتحقيق أغراض غير شرعية مختلفة ومتعددة أو التهديد بتدمير المعلومات، أو تدمير مكوناتها الأساسي.

إذن فإن جملة المخاطر السيبرانية تتلخص في عملية جمع المعلومات وتخزينها

(١) د/سمير فرج: المرجع السابق ص ٢.

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

(٢) أ.د/حسام الدين كمال الأهواني-المرجع السابق ص٤، وانظر أيضاً: د /محمد على فارس الزغبى: الحماية القانونية لقواعد

البيانات وفقاً لقانون حق المؤلف-دراسة مقارنة ما بين النظام اللاتيني والنظام الأنجلو أمريكي، ص ٨٥.

وتوزيعها<sup>(١)</sup> وهو ما يتطلب القيام باتخاذ تدابير وإجراءات معينة يطلق عليها الأمن السيبراني.

ويذهب البعض الى أن نشأة المخاوف السيبرانية جاءت بعد تصميم البروتوكول الأساسي لنقل المعلومات عبر شبكة الإنترنت والمعروف اختصاراً باسم (TCP/IP) ، وبعد دخول القطاع التجارى للشبكة<sup>(٢)</sup>.

## المطلب الثالث

### تعريف الأمن السيبراني

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

ويذهب الفقه المقارن إلى تعريف مختصر للأمن السيبراني بأنه "كيفية حماية البيانات والنظم الإلكترونية من الهجمات attack، أو الفقد loss، أو التداخل compromise<sup>(٤)</sup>.

لذا يتسع مفهوم الأمن السيبراني ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفنى لحماية المصادر البيانية (الأجهزة والبرمجيات وبيانات الأفراد، ونحوها) من التجاوزات والتدخلات غير المشروعة التي تقع صدفة أو عمداً

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

(٢) د/ياسر 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 في مجال الحماية القانونية على الإنترنت ٤-٥ شباط ٢٠٠٩ - الهيئة المنظمة للاتصالات في لبنان - أمن الفضاء السيبراني، ص٢ في إشارة إلى الجهود في مجال الأمن السيبراني من خلال لجنة الاتصالات وتكنولوجيا المعلومات التابعة لجامعة الدول العربية، ومثال تلك الجهود القانون الاتحادي لمكافحة الجرائم السيبرانية الصادر في الإمارات العربية المتحدة في شباط ٢٠٠٦، وقانون سعودي صادر في عام ٢٠٠٦ يجرم التنصت، والاعتراض أو الاستفادة من البيانات الإلكترونية دون مسوغ قانوني .

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

عن طريق التسلسل أو كنتيجة لإجراءات خاطئة، لذا تشكل المحاور التالية عماد الأمن السيبراني:

- 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 لوقوع كوارث طبيعية أو صناعية<sup>(١)</sup>.

(١) د/ دلال صادق الجواد. د/ حميد ناصر الفتال، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، ص ١٢.

## المبحث الثاني دور الضبط الإداري الإلكتروني في الرقابة السيبرانية

تجدر الإشارة إلى أن بعض التشريعات تعاني قصوراً تشريعية في الأمن السيبراني، ويتمثل القصور التشريعي أحياناً بالنسبة للأمن السيبراني في حداثة الفعل المؤدى لانتهاك الأمن السيبراني، ومثال ذلك: جريمة الدخول غير المصرح للنظام السيبراني، فالمتبع لتلك الجريمة يجد أنها من الصعوبة بمكان كي تتم معالجتها تشريعياً بشكل كامل بموجب النصوص العقابية التقليدية<sup>(١)</sup>.

ويتهدد الأمن السيبراني للإدارة بصورة كبيرة لاعتماد الإدارة في الوقت الحالي في إدارتها مرافقها 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<sup>(٢)</sup>.

مؤدى ما سبق أن العديد من الدول تلجأ في سبيل حماية أمنها السيبراني إلى وجود أطر تشريعية ورقابية سيبرانية وتطبيق قوانين موضوعية وأخرى إجرائية على العكس من دول أخرى تعتمد على قوانين غير فعالة<sup>(٣)</sup>.

وبالنظر إلى التجربة الأمريكية في تعزيز الأمن السيبراني نجدها تنقسم إلى شقين، أولهما: المعايير الفنية Technical standards وثانيهما: التشريعات والرقابة Legislation and Monitoring وتتناولهما كالتالى<sup>(٤)</sup>:

(١) 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، ص ١٠، 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 في ظل الفكر الجنائي المعاصر». رسالة مقدمة لكلية الحقوق جامعة القاهرة، ٢٠١٢، ص ١٨٢.

## 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<sup>(١)</sup>.

ومن أهم اللجان لجنة الحاسب الآلي والاتصالات التابعة للمجلس القومي للبحوث، وترجع أهمية تلك اللجنة إلى أنها تشفر المعلومات والبيانات "cryptography"<sup>(٢)</sup>.

## ثانياً - التشريعات والرقابة:

لن تكتمل منظومة الأمن السيبراني إلا بوجود إطار تشريعي

- فعلى صعيد الرقابة تم إنشاء فريق الاستعداد في ٢٠٠٣ كجزء رئيسي من وحدة الأمن القومي الافتراضية (National cyper security Division)<sup>(٣)</sup>.

وتختلف أساليب الرقابة السيبرانية بحسب النظام القانوني والبيئة السيبرانية. ومن الأساليب الضبطية الإدارية الحديثة في الولايات المتحدة أسلوب العمل على نحو تكاملي قومي كالمركز المتكامل للتهديد الاستخباراتي والمنشأة في ٢٠١٥ (CTIC) والذي يعمل عن طريق تبادل المعلومات والتهديدات منها الاستخبارات الإلكترونية<sup>(٤)</sup>.

ولكن إذا أمعنا النظر في جهات الضبط الإداري في الولايات المتحدة الأمريكية والتي تعمل على تعزيز الأمن المعلوماتي 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 ص ١٨٢ في إشارة إلى المرجع: Kaspersen (W. K. Henrik) computer crimes and other crimes Against Information Technology in U. S. A., R. I. D. P. 2001, P. 273.

(٣) في اعتقادنا أن أهم ما يميز ذلك الفريق هو شراكة القطاع الخاص مع جهة الإدارة الأمريكية. في إنشائه بغرض تسييق 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 الداخلي وخاصة الإدارة الوطنية للأمن الإلكتروني<sup>(١)</sup>.

ومن جهات الضبط الإداري المهمة أيضاً فى هذا الشأن مكتب المحاسبة والموازنة بالكونجرس؛ حيث إن مدير 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 الأمريكى.

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 المسؤولة عن الأمن السيبرانى، 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. ص ٢٤ 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، وبنوكاً، 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 في المنازعات<sup>(١)</sup>.

إلى جانب ما سبق هناك بعض المؤسسات الحكومية التي تحمي الأمن السيبراني، كمثل: الهيئة القومية للاتصالات والمعلومات، ولجنة التجارة الاتحادية (FTC) والتشريعات على سبيل المثال، قانون حماية الأطفال على الإنترنت، وقانون حرية المعلومات (FOIA) التي تحمي حقوق المستخدم حال تواجده (on line) على الشبكة<sup>(٢)</sup>.

ومثال تلك المؤسسات أيضًا: المركز الوطني لحماية البيئة التحتية التابع للمباحث الفيدرالية الأمريكية<sup>(٣)</sup>، ومكتب رئيس التكنولوجيا وهو مكتب مفوض مباشرة من مدير التحقيقات الفيدرالية الأمريكية، وقسم جرائم الحاسب ومعهد أمن الحاسبات، ووحدة جرائم الإنترنت<sup>(٤)</sup>.

ومن أمثلة جهات الضبط الإداري التي تعزز الأمن السيبراني ما قامت به فرنسا من إنشاء عدة وحدات ومراكز متخصصة ومنها الشرطة الوطنية لمكافحة الجرائم السيبرانية بكل صورها. ومن أهم تلك الوحدات أيضًا المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات للاتصالات، ومن مهام ذلك المكتب تنسيق عمليات ملاحقة مرتكبي الجرائم السيبرانية، علاوة على مشاركة جهات الضبط القضائي في إجراءات التحقيق، ومساعدة الشرطة الوطنية وغيرها من الأجهزة<sup>(٥)</sup>، ومن تلك

(١) مشار إلى ذلك في المرجع السابق ص ١٤٥.

(٢) <http://www.ftc.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 التي تعمل في مجال الإنترنت تحرص على الأمن السيبراني إلى جانب مبادئ أخرى، كمثل: مبدأ الاختيار، ومبدأ الإخطار، ومبدأ الحق في الوصول والاطلاع.

للمزيد انظر: النظم المختلفة لحماية الخصوصية السيبرانية باعتبار أحد أركان الأمن السيبراني د/ وليد السيد سليم: ضمانات الخصوصية في الإنترنت - دار الجامعة الجديدة ٢٠١٢ ص ٦٣٥ حتى ص ٦٥٠.

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

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

(٤) للمزيد انظر: المرجع السابق، ص ٢٤٦.  
وقد أقامت بريطانيا هيئة جديدة لمكافحة الهجمات الإلكترونية، وبالفعل تصدت تلك الهيئة للهجمات في ١٨٨ مناسبة، وتعد تلك الهيئة جزءًا من وكالة الاستخبارات البريطانية.

(٥) تم إنشاء ذلك المكتب بموجب مرسوم وزاري رقم (٤٥٥ - ٢٠٠٠) المؤرخ في ١٥/٥/٢٠٠٠ على مستوى المديرية المركزية

الجهات أيضاً القسم الوطنى لقمع جرائم المساس بالأموال والأشخاص<sup>(١)</sup>.

ومن المبادئ المهمة التى تكفل الأمن السيبرانى لجهة الإدارة فى فرنسا وجود تنظيم فى معالجة البيانات الشخصية، وجاء النص عليه فى قانون السيبرانية الفرنسى من خلال حظر استخدام وسائل غير شرعية لجمع المعلومات والبيانات وتوضيح الغرض من جمع البيانات<sup>(٢)</sup>.

أما على صعيد التشريعات الفرنسية فقد تم إنشاء لجنة وزارية فى فرنسا تخصص الدعم التقنى من أجل تطوير تكنولوجيا المعلومات والاتصالات فى المرافق والرقابة الإدارية (M.T.IC) فى 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<sup>(٣)</sup>.

مؤدى ما سبق، يؤكد رفض التشريع الفرنسى انتهاج النهج الأمريكى الذى يكتفى بالرقابة القضائية فيما يخص الأمن السيبرانى، ولكن عمد التشريع إلى أسلوب الوقاية خير من العلاج، لذا عمد المشرع الفرنسى إلى إنشاء تلك اللجنة التى تقوم بالتحرى والنصح والاقتراح والرقابة، وإعلام الجمهور ومساعدة أجهزة الدولة المختلفة<sup>(٤)</sup>.

وتعد تلك اللجنة فى اعتقادنا أهم إحدى أدوات الضبط الإدارى لحماية الأمن السيبرانى فى فرنسا، حيث تعتمد على الصفة الأساسية للضبط الإدارى، وهى الطابع الوقائى والرقابة السابقة من خلال اتخاذ وسائل الحماية المسبقة، والرقابة المستمرة للتحقق من قيام الجهة القائمة على الحاسب الآلى فى تطبيق الضمانات القانونية، وما

---

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

(١) يتكون هذا القسم من «٦» محققين متخصصين فى التحقيق فى الجرائم السيبرانية، ولقد بدأ القسم مهامه عام ١٩٩٧ (مشار لذلك وللهاشم رقم ١) رسالة دكتوراه فى الجرائم السيبرانية د/ محمد أحمد عزت المرجع السابق، ص ٢٤٤.

(٢) د/ وليد السيد سليم، المرجع السابق، ص ٥٧٣.

(٣) د/ داود عبد الرازق الباز، الإدارة العامة، الحكومة الإلكترونية وأثرها على النظام القانونى للمرفق العام، مجلس النشر العلمى، جامعة الكويت، ٢٠٠٤، ص ٢٥٦.

(٤) د/ وليد السيد سليم المرجع السابق، ص ٥٨٦.

نقلا عن:

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

يؤكد ذلك سلطة اللجنة في اتخاذ القرارات التنظيمية العامة والفردية لتطبيق أحكام القانون إلى جانب تكليف أحد أعضائها بالتحقق واقعيًا من احترام الأمن السيبراني عن طريق إجراء الفحص المناسب<sup>(١)</sup>.

علاوة على ما سبق تعمل اللجنة القومية للمعلومات والحريات في فرنسا على تعزيز الأمن السيبراني للأفراد من بيانات ومعلومات بما يتفرع عن ذلك من حقوق كالحق في الأمن والسرية السيبرانية، معتمدة في ذلك على العديد من إجراءات الضبط الإداري ومنها التفتيش والمراقبة والإشراف على الأنظمة السيبرانية، بل تتلقى شكاوى الأفراد والأشخاص المعنوية العامة عند مخالفة القانون وتقوم بالترخيص والتصريح عند ممارسة نشاطات جمع البيانات والمعلومات، والتأكد من توافق النظام السيبراني مع القانون<sup>(٢)</sup>.

**مؤدى ما سبق أن اللجنة القومية للمعلومات والحريات تعمل على الدور الرقابي 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 القانون ذاته، ومنها بيانات إحصاءات الرقم القومي، وعمليات التعداد والإحصاء الوطني، وخدمات الإنترنت العامة.
- ٢- إبلاغ النائب العام فوراً بحسب ما تنص عليه المادة (٤٠) من قانون الإجراءات الجنائية الفرنسي بشأن ما يصل إلى علمها من جرائم سيبرانية.

(١) المرجع السابق ص ٥٨٦.

(٢) نصت المادة رقم (١٣) من قانون (١٧-٧٨) المعدل بموجب قانون (٢٠١١-٣٣٤) الصادر في ٢٩ مارس ٢٠١١ على أن تشكيل

اللجنة يتكون من سبعة عشر عضواً 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 تعيينهم بمرسوم من مجلس الوزراء.
- عضوان يختاران من الخبراء في مجال الحاسب والمعلوماتية.

انظر: المرجع السابق ص ٥٧٥ وما بعدها.

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. وتجدر الإشارة إلى أن التوجيه الأوروبي نص على العديد من الصلاحيات لسلطات الضبط الإداري لتعزيز الأمن السيبراني ومنها:

- صلاحيات البحث والاطلاع 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<sup>(١)</sup>.

علاوة على ما سبق قد تهدف بعض التشريعات إلى عدم إنشاء وحدات ضبط إداري مستحدثة مستقلة وتعتمد إلى الاكتفاء بوحدة 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،<sup>(٢)</sup> وإدارة مكافحة جرائم الحاسبات وشبكات المعلومات.

وفى اعتقادنا أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات من أهم وحدات الضبط الإداري التي تعزز الأمن السيبراني المصري من خلال النظر في اختصاصات تلك الإدارة وعلى رأسها بحسب القرار الوزاري رقم ١٣٥٠٦ لسنة ٢٠٠٢ ما يلي<sup>(٣)</sup>:

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

(١) للمزيد انظر: المرجع السابق، ص ٥٦٥.

(٢) فى اعتقادنا أن الإدارة العامة لمباحث الأموال العامة، والإدارة العامة للمصنفات الفنية تتعلق باختصاصات نوعية ولا تحقق تعزيز الأمن السيبراني بالمفهوم الذى يناقشه البحث، أما الإدارة العامة للتوثيق والمعلومات فإنها قد تخدم تعزيز الأمن السيبراني بصورة جزئية مكملة.

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

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

والجدير بالذكر أن القرار الوزاري رقم ١٣٥٠٧ لسنة ٢٠٠٢ نص على إنشاء أقسام إقليمية لمكافحة الجرائم السيبرانية<sup>(١)</sup>.

وبالتركيز على دور إدارة مكافحة جرائم الحاسبات وشبكات المعلومات نجد أن أهم أقسامها هو قسم التأمين حيث يقوم بما يلي<sup>(٢)</sup>.

- ١- معاونة أجهزة الوزارة في تأمين نظمها السيبرانية.
- ٢- التخطيط ووضع أساليب تعزيز الأمن السيبراني ثم التنفيذ والتنسيق مع الأجهزة المختصة.
- ٣- متابعة التراخيص التي تصدر للشركات الخاصة في 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 ٢٥١، 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 السيبراني.
  - ٥- أرشفة متكاملة لقاعدة البيانات والمعلومات لتعزيز الأمن السيبراني.
- لذا صدر القرار الوزاري رقم ٣٥٢١ لسنة ٢٠٠٤ بشأن إنشاء قسم بمديرية أمن القاهرة لمكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للبحث الجنائي.
- (٢) 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.

علاوة على ما تقدم تلعب الشراكة السيبرانية دوراً 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<sup>(١)</sup>.

ويرى الفقه المقارن أن هدف نظم الشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني يرمي إلى وجود تدابير وقائية وبرامج أمن سيبراني تقلل المخاطر السيبرانية<sup>(٢)</sup>.

ويرى البعض أن الاحتمال الأبرز بالنسبة للأمن السيبراني سيحقق من خلال لجوء جهات الإدارة على المستوى العالمي لتأسيس شبكات محلية أو إقليمية، والاستغناء عن الشبكة الموحدة للإنترنت، وذلك كي يتم الحد من تدفق البيانات والمعلومات، ولكن يعيب ذلك التدبير الاحترازي الإداري أنه يطفى على عدة أمور أولها: حرية تداول المعلومات، وثانيها: ازدياد قدرة الحكومات على مراقبة ما يُنشر على الشبكة، لصغر حجمها، وثالثها: ارتفاع تكلفة البنية التحتية لإنشاء هذه الشبكات، بسبب تكرار بنائها في كل دولة أو إقليم<sup>(٣)</sup>.

وفي اعتقادنا أنه لن تفلح جهود تعزيز الأمن السيبراني سوى بتوحيد الجهود الدولية قانونياً واحترازياً وقضائياً وذلك لوجود فقدان في المركزية الأمنية السيبرانية، وعدم وجود آليات ضابطية إدارية على المستوى الدولي تستطيع السيطرة والتحكم.

(١) من أمثلة 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".

من وحدات الإدارة المعنية بالأمن السيبراني على سبيل المثال: وزارة العدل، ووزارة الداخلية، ووزارة نظم المعلومات، والمخابرات بأنواعها.

(٣) مجلة حالة العالم، تقرير «جايسون هيلي» مدير مبادرة "cyber statecraft initiative" بمركز (Atlantic council)، ص ١٧، 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.

يؤيدنا في ذلك اختلاف القوانين الوطنية المنظمة لحماية حق من حقوق الإنسان مثلاً عن القوانين المنظمة لتعزيز الأمن السيبراني<sup>(١)</sup>.

يرى الفقه المقارن أن مسألة الأمن السيبراني أصبحت مسألة قانونية أكثر منها مسألة تقنية لتعلقها بمجالات الخصوصية Privacy وأمن المعلومات Data security، فلا بد أن تعد المنظمات حزمة القوانين المنظمة للأمن السيبراني، وأن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر<sup>(٢)</sup>.

علاوة على ما سبق يمكن الاستفادة من خبرات القطاع الخاص في مجال الأمن السيبراني، كمثال إطار "NIST" (المعهد الوطني للمعايير والتكنولوجيا)، وذلك لحماية البنية الأساسية الحيوية المحلية Domestic critical Infrastructure وذلك في الولايات المتحدة الأمريكية<sup>(٣)</sup>.

وبالمثل نجد أن الحكومة الألمانية قد اعتمدت كذلك استراتيجية أمنية سيبرانية قائمة على الشراكة بين القطاعين العام والخاص<sup>(٤)</sup>.

ويرى الفقه المقارن إمكانية لجوء جهة الإدارة إلى إجراء برامج لتطوير برامج حيافة البيانات من خلال تقنيات أكثر سرعة وبشكل قابل لتحمل التكلفة، وتسمح تلك

(١) د. أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة سنة ٢٠٠٦ ص ٥٠١. «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»

(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, PhD, 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).

(MLPS) "Multi - level protection schem" أما الصين فقد أصدرت تشريعات بغرض حماية أمنها السيبراني القومي. والتي يرمز لها بالختصر وذلك في عام 2007 "Multi - level protection schem"

التقنيات لجهة الإدارة بالتحرك فى الفترة ما بعد الجريمة بالبحث عن بيانات الأفراد المعنيين بالبحث عن البيانات<sup>(١)</sup>.

مؤدى ما سبق يجوز الاستعانة بالقطاع الخاص فى حماية الأمن السيبرانى من خلال توفير أعلى حماية تقنية لجهة الإدارة، بل ويمكن تصنيف المعلومات وفقاً لتلك الاستعانة بحسب درجة سريتها، ويمكن لجهة الإدارة دراسة كل حالة على حدة للقيام بعملية التصنيف<sup>(٢)</sup>.

فى اعتقادنا أن البنية الأساسية الحيوية هى الأولى بوضع التدابير الاحترازية، لذا سعت الولايات المتحدة إلى «حماية البنية الأساسية الحيوية» "critical infrastructure" والتي تعنى بالأساس حماية النظم "system" والأصول "assets" والتي لها تأثير على الأمن بصفة عامة، والأمن الاقتصادى القومى، والصحة العامة والسلامة العامة أو كل ما سبق<sup>(٣)</sup>.

ويساير ما سبق ما يميل إليه الفقه الأمريكى من تعزيز الأمن السيبرانى بصورة شاملة فى كل من القطاعين العام والخاص، ولكن لا بد من الأخذ فى الاعتبار أن المؤسسات العامة وشركات الطاقة أقل من حيث القدرة الوقائية فى مجال الأمن السيبرانى من الشركات التجارية التنافسية<sup>(٤)</sup>.

(1) See: task force on national security in the information Age, Markle found creating AA Trusted 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.

ساهمت تلك التقنيات خاصة بعد الهجمات الإرهابية فى ١١ سبتمبر، حيث كشفت جهة الإدارة فى الولايات المتحدة الأمريكية بيانات هائلة حول الأفراد مستمدة من القطاع الخاص، وبذلك يكون الكونجرس قد أخفق فى الموازنة بين 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

علاوة على ذلك، يمكن تحديد سبل حماية الأمن السيبراني في الولايات المتحدة من خلال حماية الأمن السيبراني 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 داخل الدولة وخارجها حول مخاطر الأمن السيبراني<sup>(1)</sup>.

ومن وجهة نظرنا، لا بد أن تأخذ جهة الإدارة في اعتبارها عند إبرام عقودها - خاصة في عقود نقل التكنولوجيا - ما يحميها من نصوص تعاقدية وتدابير احترازية، حيث إن من أهم مجالات حماية البيانات عند التعاقد جهة الإدارة مع شركة تقوم باستبدال تقنية معينة أو معالجة قواعد البيانات لديها أن تتخذ جهة 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<sup>(2)</sup>.

والجدير بالذكر أن جهة الإدارة - خاصة في حالة نقص مواردها المالية أو عدم خبرتها بأطر الضبطين التشريعي والإداري للأمن المعلوماتي - بين خيارين ليسا من السهولة بمكان، حيث يتمثل الخيار الأول في تعزيز أمنها المعلوماتي، 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

ويمكن الاستعانة في ذلك بإطار (NIST) المعهد الوطني للمعايير والتكنولوجيا الذي يقوم على تحسين الأمن السيبراني للبيئة التحتية الحيوية، وذلك الإطار لا يعد تشريعاً أو نموذجاً رسمياً.

“Critical infrastructure, the core of the NIST framework’s focus, is defined as “systems and assets whether physical or virtual, so vital to the united states that the incapacity or destruction 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.

(2) ويرتبط بذلك وجوب نقل المعرفة لموظفي جهة الإدارة لإحداث تغييرات في واجهة المستخدم عند التحديث الفني، وترحيل قاعدة البيانات.

الثانى فى شراء التكنولوجيا الأجنبية لتعزيز الأمن السيبراني<sup>(١)</sup>.

لذا يرى البعض أن التشفير يعد وسيلة مهمة لحماية الإدارة من المخاطر السيبرانية خاصة فى حالة تداول البيانات والمعلومات بين جهات إدارة مختلفة فى صورة قرارات أو أوامر أو تعاقدات إدارية<sup>(٢)</sup>.

قد يكون التشفير حلاً مؤقتاً عن طريق تأمين الشبكات السيبرانية لجهة الإدارة كتغيير طريقة التشفير والمراجعة الدورية لأساليب الحماية، ويمكننا إضافة إلى ذلك بمراعاة حصر الاختصاصات للموظفين الذين يتعاملون مع البيانات والمعلومات الحكومية وغيرها<sup>(٣)</sup>.

(1) Scott J. Shackelford, JD, PhD, 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، والتي تلجأ لها بعض الدول مبدأ استبعاد تكنولوجيا الأمن المملوكة للأجانب، وعلى سبيل المثال: الصين، وهى فى ذلك تخالف السياسة الأمريكية، والأمانية فى حماية وتعزيز الأمن السيبراني.

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

وتجدر الإشارة 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 القرصنة الإلكترونية إلى «فيروس الفدية» الذى انتشر مؤخراً من خلال استغلال الثغرات الصفرية الموجودة فى برامج تشغيل ويندوز للتجسس على الأفراد والحكومات والتي طورتها وكالة الأمن القومي الأمريكية.

(٢) د/ بشير على باز: دور الحكومة الإلكترونية فى صناعة القرار الإدارى والتصويت الإلكتروني، مجلة روح القانون، كلية الحقوق جامعة طنطا ٢٠٠٧، ص ٢٥، ٢٦.

(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 السيبراني ص ٢٧ «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 السيبرانية باعتماد كلمات سر صعبة الاختراق، وأنظمة حماية متعددة الطبقات، ومنهجية النسخ المتطابقة Mirroring، والأرشيف الاحتياطي للبيانات، وحماية شبكة السيبرانية فى الشركات والمؤسسات التجارية، والاعتماد على مواقع تكون بمثابة نسخة مطابقة للأصل خارج أراضى الدولة عند وجود بيانات عالية السرية» “ساعد ذلك جورجيا على تخطى الاختراق الروسى لبواباتها الإلكترونية حيث تم استعمال بوابات بديلة مطابقة للبوابات الأصلية تقع فى الأراضى الأمريكية.”

## المبحث الثالث

### دور الضبط الإداري الإلكتروني

#### في تهيئة البيئة السيبرانية الآمنة

هناك العديد من الآليات المعتادة لرصد وحياسة البيانات والمعلومات تركز لدور الضبط الإداري الإلكتروني في تهيئة البيئة السيبرانية الآمنة، ومن اللجان ووحدات الضبط الإداري التي تعمل على ذلك في سبيل تعزيز الأمن السيبراني 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 الثروة الطبيعية والتي تشكل محوراً من محاور الأمن السيبراني<sup>(١)</sup>.

ويأخذ التشريع المصري بأسلوب 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 الحصول على ترخيص من الجهاز وفقاً لأحكام هذا القانون وحددت المادة (٢٥) من القانون الأمن القومي -في مجمله سواء مادياً أو سيبرانياً- هدفاً، وذلك بأن تطلبت أن يحدد الترخيص الصادر من التزامات المرخص له، والتي تشمل على الأخص الالتزامات الخاصة بعدم المساس بالأمن القومي .

وهذا ما أكدت عليه المادة (٦٧) من القانون بخضوع أى مشغل أو مقدم خدمة للسلطات المختصة في الدولة ونظام إدارتها من خدمات وشبكات اتصالات، وأن تستدعى العاملين لديه القائمين على تشغيل تلك الخدمات والشبكات وصيانتها وذلك في حالة حدوث كارثة طبيعية أو بيئية، أو في الحالات التي تعلن فيها التعبئة العامة طبقاً لأحكام القانون رقم ٨٧ لسنة ١٩٦٠، وأية حالات أخرى تتعلق بالأمن القومي.

وبالنظر إلى التشريع الكويتي نجد أن هيئة تنظيم قطاع الاتصالات وتقنية المعلومات تختص بإدارة طيف الترددات الراديوية ومراقبة التداخلات وجودة الطيف الترددي

(١) 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 والتلفزيون، علاوة على ثلاثة أعضاء يرشحهم الوزير المختص.

واتخاذ الإجراءات اللازمة بهذا الخصوص بما في ذلك إعداد الجدول الوطني لتوزيع الترددات وتحديثه، وإعداد المخطط الوطني لتوزيع الترددات والسجل الوطني لتشخيص الترددات بالاشتراك مع الجهات العسكرية والأمنية<sup>(١)</sup>.

وقد أكدت المادة (٢٧) من القانون ذلك في فقرتها الأولى من خلال عدم جواز استخدام أى شخص لأية ترددات راديوية إلا إذا حصل على رخصة بذلك وفقاً للشروط التي تحددها إدارة هيئة الاتصالات وتقنية المعلومات<sup>(٢)</sup>.

فضلاً عما تقدم هناك العديد من الآليات الإدارية لرصد المخاطر السيبرانية، حيث تعتمد 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 الرأى العام).

(١) 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 «تشأ هيئة عامة ذات شخصية اعتبارية مستقلة تسمى الهيئة العامة للاتصالات وتقنية المعلومات ويشرف عليها الوزير المختص وتمتع بالشخصية الاعتبارية المستقلة وبالاستقلال المالي...».

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

(٢) انظر المادة (٢٧) من القانون، وقد اكتملت منظومة تعزيز أمن الطيف الترددي من خلال المادة (٣٠) والتي منعت اقتناء أو استعمال محطة راديوية على أراضى الدولة أو على سفينة أو على طائرة مسجلة في الدولة ما لم يتم الحصول على رخصة وفقاً 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 البرى في الأراضى أو الموانئ أو المطارات الكويتية، وكذلك السفارات الأجنبية بشروط المعاملة بالمثل، ووجود تصريح قابل للتجديد.

وتتمتع الهيئة بالاختصاصات المهمة في مجال الأمن السيبراني ومنها:

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

٢- وضع لوائح تنظيم قطاع 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 اتصالات دولية.

٤- تنظيم الربط البيني بين شبكات الاتصالات العامة المملوكة للقطاع الخاص، أو وزارة المواصلات، 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 الإداري (الدائرة الثامنة) إلى إقرار ذلك الإجراء الضبطي الإداري 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<sup>(١)</sup>.

**لذا تتعدد آليات الإدارة في 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 في كل إدارة لدراسة أفضل طرق حفظ الوثائق المعلومات.

٢- أخذ نسخ للبرامج بغرض تشغيل الدعامات القديمة عند الحاجة إليها.

٣- استخدام دعامات إلكترونية لضمان الحصول على البيانات الإلكترونية في حالة فشل تشغيل أى من الدعامات الأخرى والعمل على القيام بعملية تحويل يومي back up خارج جهاز الحاسوب<sup>(٢)</sup>.

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 الإداري - الدائرة الثامنة عقود في الدعوى رقم ٦٢٠٥٥ 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 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...».

(٢) ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية - رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١، ص ١٨١، ١٨٢.

للمزيد انظر:

- عبد العزيز السيد مصطفى - أساسيات الرقابة على نظم التبادل الإلكتروني للبيانات - بحث مقدم لمؤتمر التجارة الإلكترونية - الأفاق والتحدى - المنعقد بتجارة الإسكندرية، يوليو ٢٠٠٢، ص ٤١٩.

- /د/ هدى حامد فشقوش: جرائم الحاسب الإلكتروني في التشريع المقارن - دار النهضة العربية، القاهرة، ١٩٩٢.

بأنها: هي الشكل التقليدي لمعالجة البيانات حيث يزداد اعتماد الجهات الإدارية على البيانات 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.

ويرى الفقه المقارن أن هذا الشكل يقوم على اعتماد جهة الإدارة على موظفيها فى جمع تلك البيانات، ثم تحليلها من قبل المتخصصين الذين يقومون بالتقييم والتقدير باستقلالية تامة<sup>(١)</sup>.

ويمكن أن يقترب مصطلح "معالجة البيانات" من مصطلح "استخلاص البيانات" "Data Mining" حيث يقوم المصطلح الأخير - بمفهوم واسع - على الأنشطة التى تقوم على البيانات كأبحاث تقوم على دراسة موضوع ما أو الأبحاث 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"<sup>(٢)</sup>.

(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". =

تستخدم المؤسسات الحكومية الدراسات التى تقوم على الموضوع والدراسات العلائقية المتصلة كمثال دراسة المسئولين عن تنفيذ القانون ليصمات شخص ما فى مسرح الجريمة، أو سائق السيارة وقد يستخدم أيضاً فى مجال الضرائب... إلخ. أما دراسات الشكل أو النمط تنصل بصورة أكبر بالقانون التجارى ودراسات تقوم على المستهلك وتقديرات المخاطر التجارية بل وزاد استخدام دراسات النمط بعد هجمات الحادى عشر من سبتمبر ٢٠٠١، فقد طلب الكونجرس بموجب قانون الأمن الوطنى لسنة ٢٠٠٢ من الإدارة الجديدة للأمن الوطنى.

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:

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 عن بعد من الجو أو من الفضاء الخارجي في كثير من النواحي الفنية<sup>(1)</sup>.

أضف إلى ما سبق أن تدفق البيانات يُعد نتاجاً لعمليات الاستشعار عن بعد عبر أربع مراحل ثابتة، وهي مرحلة جمع البيانات، ثم معالجتها، وتفسيرها وأخيراً توزيعها ونشرها<sup>(2)</sup>.

وكما تؤدي أنشطة الاستشعار عن 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 اقتصادياً<sup>(3)</sup>.

فضلاً عما تقدم هناك العديد من الآليات الإدارية لرصد المخاطر السيبرانية، حيث تجدر الإشارة إلى أن الجهة الإدارية تواجه إشكاليات عند تهيئة البيئة السيبرانية تتمثل في إشكاليات حيازتها للمعلومات الشخصية خاصة الواردة من أطراف ثالثة تثير إشكاليتين، الأولى: الفعالية "efficacy" بمعنى هل تضمن عملية حيازة تلك المعلومات المصادر المالية والبشرية التي تتطلبها؟ والثانية: التأثير "Impact" بمعنى هل يؤدي

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

(2) د/ ممدوح فرجاني خطاب: النظام القانوني للاستشعار عن بعد من الفضاء الخارجي، دار النهضة العربية 1993 ص 246  
تكون تلك الآلية بإنشاء أدوات متقدمة حول الدخول للبيانات واستلامها وتحليلها لاكتشاف المخاطر الإرهابية التي تواجه الولايات المتحدة.

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

مشار إليه في د/ ممدوح فرجاني، المرجع السابق ص 248.

احتكار القطاع الخاص للمعلومات لإثارة المخاوف لدى جهة الإدارة حول سلوك مضر بالأفراد بطريقة أو بأخرى<sup>(١)</sup>.

وفيما يخص الكفاءة، يمكن أن تؤثر حيازة المعلومات أكلها بحسب المقاصد التي تحددها جهة الإدارة، وبخاصة فيما يتعلق بمسائل الأمن القومي وقانون التنفيذ، حيث لا تستطيع الإدارة وحدها مواجهة أو منع الأنشطة الإرهابية بناء على تحليل البيانات أو المعلومات وتزداد تلك الإشكالية خاصة عندما تتعارض حيازة المعلومات بفرض الحفاظ على الأمن القومي مع حيازتها لأهداف تجارية لذا يمكن تلخيص عنصر الكفاءة في ثلاثة بنود:

### 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 التحدي الأبرز في حيازة المعلومات<sup>(٢)</sup>.

وتتأثر الإشكالية الأكبر في بند جودة المعلومة كما ذكر في مجلة «computer world» في ٢٠٠٢ من أن «بيانا واحداً من معلومة سيئة» يعد إشكالية بديهية، ولكن إذا زادت أجزاء البيانات السيئة نحو آلاف أو ملايين الأخطاء؛ فإن ذلك سيؤدي إلى معلومات غير متناسقة تؤدي بدورها إلى الفوضى<sup>(٣)</sup>.

### الثاني- تناسق البيانات «Data matching»

تواجه جهة الإدارة العديد من الأخطاء في حيازة المعلومات<sup>(٤)</sup> ومنها 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 كالاتى (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.

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.<sup>(1)</sup> وذلك لكي يتم تعريف الأفراد القادمين لحدود الدولة وتقدير مدى الخطر الذي يحوم حولهم من خلال المعلومات الدقيقة عنهم.

وهذا أكثر ما تم التركيز عليه في تقرير اللجنة الاستشارية للخصوصية والتكنولوجيا (TAPAC)<sup>(2)</sup> حيث يتمثل التحدي الأكبر في كيفية ضمان أمن المعلومات خاصة في حالات مواجهة الإرهاب ورصد البيانات أو تجميعها من جهات مختلفة منفصلة عن بعضها البعض، ومنها: جهات المخابرات الذي لا يخضع لأية سيطرة.

وفي الواقع - أيضاً - يزداد الأمر صعوبة عند وجود بيانات غير متوافقة وغير منتظمة كما في حالة كاميرات المراقبة الصوتية وكاميرات الفيديو.<sup>(3)</sup>

### الثالث- أدوات استخلاص البيانات « 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 غالباً ما يعتمد مخترقو الأمن السيبراني لتضليل جهة الإدارة مقارنة بالقطاع الخاص

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

(1) تضمين رقم الضمان الاجتماعي لم يحل تلك الإشكالية في الولايات المتحدة لأن الحسابات الخاصة بكل عائلة يمكن أن يوجد بها أرقام ضمان اجتماعي مختلفة كالزوجة والمعيّل القاصر علاوة على ذلك البيانات الخاصة بالهجمات الإرهابية المحتملة أرقام الضمان الاجتماعي لا تتضمن أرقام ضمان اجتماعي .

(2) This is a substantial challenge, as stressed in the 2004 final report of Technology and privacy Advisory committee (TAPAC) the "blue ribbon" bipartisan independent committee appointed by the secretary of Defense Donald Rumsfeld 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 Information, 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 contemporary 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".

ومع ذلك، تعد المعلومات الواردة من القطاع الخاص مفتاحاً مهماً للأمن القومي من خلال توقع المسؤولين عن الأمن القومي للسلوك المعتاد لعملاء القطاع الخاص<sup>(١)</sup>.  
- "Government data mining seems similarly likely to fighting yesterday's battles".<sup>(٢)</sup>

## التوصيات:

١- يجدر بالمشروع المصري العمل على استصدار قانون للأمن السيبراني 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 للدستور المصري الصادر عام ٢٠١٤ لكنه لم يشرع لأدوات الحماية السيبرانية الكافية<sup>(٣)</sup>.

٢- نقترح أن يعمل ذلك القانون على معالجة مدى تعارض الأمن السيبراني مع الخصوصية وغيرها من الإشكاليات القانونية التي ورد ذكرها في هذا البحث.

٣- نقترح أن تعمل السلطات التنفيذية على توفير متطلبات الضبط الإداري الإلكتروني من خلال تهيئة أدوات البيئة السيبرانية الآمنة، وأولها الإدارة الإلكترونية، والحكومة الإلكترونية.

(1) Jeff Jonas & Jim Harper, cato institute, Effective counter terrorism & 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".

لذلك يعد رجال الأمن في الولايات المتحدة أكثر توقعاً للهجمات الإرهابية الخارجية من خلال توقع ضباط الاستخبارات للخطط الإرهابية بناء على النشاط الإرهابي في الماضي بخلاف الهجمات الإرهابية المحلية تتخذ شكلاً مختلفاً كل مرة في 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. 11, 2006, At A1.

(٣) . مريم عراق: دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠: مقال منشور على الموقع الإلكتروني [/https://www.mondaq.com](https://www.mondaq.com) آخر تحديث ٢٠٢١/٨/٢٠

تعد الدراسة النقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ الإصدار العلمي الأول لمركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية في مصر، والتي أعدت بإشراف الأستاذ الدكتور حسن عبد الحميد عميد كلية القانون بالجامعة البريطانية وبمشاركة كوكبة من رجال القانون في مصر، قضاة ومحامين، بالإضافة للمتخصصين في مجال تقنية المعلومات، وغيرهم ممن لهم علاقة مباشرة بقانون حماية البيانات الشخصية وبالتعاون مع مكتب - اندرسن مصر. وتأتى أهمية هذا الكتاب انه قد اجري دراسة مقارنة بين القانون واللائحة الأوروبية لحماية البيانات (GDPR) باعتبارها القواعد التي استهدى بها المشروع في إعدادة.

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 ناصرالفتال: أمن المعلومات - دار اليازورى العلمية للنشر والتوزيع .
- د/ طارق إبراهيم الدسوقي عطية: «الأمن المعلوماتي» (النظام القانوني لحماية المعلومات) دار الجامعة الجديدة، ٢٠٠٩.
- د/ ممدوح فرجاني خطاب: النظام القانوني للاستشعار عن بعد من الفضاء الخارجي، دار النهضة العربية، ١٩٩٣.
- د/ هدى حامد قشقوش: جرائم الحاسب الإلكتروني في 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 الإداري في 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 في 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 القانوني للمرفق العام، مجلس النشر العلمي، جامعة الكويت، ٢٠٠٤.
- **سامية بوقرة:** المخاطرة المعلوماتية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة ٢٠١٥ - تصدر عن الجامعة الإسلامية في لبنان.
- **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.
- **عبد العزيز السيد مصطفى:** أساسيات الرقابة على نظم التبادل الإلكتروني للبيانات - بحث مقدم لمؤتمر التجارة الإلكترونية (الآفاق والتحدى) المنعقد بكلية التجارة جامعة الإسكندرية - يوليو ٢٠٠٢.
- **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.

#### ٤- قوانين وقرارات:

- ١- القانون المصرى لتنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ .
- ٢- القانون المصرى رقم ١٠٩ لسنة ١٩٧١ فى شأن هيئة الشرطة.
- ٢- القانون الكويتى رقم ٢٧ 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 ١٠٢٢ 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 مكرراً (هـ) فى ٢٩ ديسمبر سنة ٢٠١٥.
- ٦- قرار رئيس مجلس الوزراء المصرى رقم ٢٢٢٨ لسنة ٢٠١٤ «والذى ضم بموجبه ممثل لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء إلى عضوية المجلس الأعلى للأمن السيبراني». «منشور بالجريدة الرسمية - العدد ٥٢ مكرراً (أ) فى ديسمبر سنة ٢٠١٤.
- ٧- القانون الكويتى رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية: الكويت اليوم العدد ١١٧٢، السنة الستون بتاريخ ٢٣/٢/٢٠١٤.
- 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 ١٠/٥/٢٠١١ فى القضية رقم ٢٠١/٥ جنایات عسكرية- إدارة المدعى العام العسكري- (حكم غير منشور).
- ٢- حكم محكمة القضاء الإداري، دائرة المنازعات الاقتصادية والاستثمار، الصادر فى الدعوى رقم ١٤٣٠ لسنة ٦٥ ق جلسة ٢٧/١١/٢٠١٠ (حكم غير منشور).

٤- حكم محكمة القضاء الإداري - الدائرة الثامنة عقود- الدعوى رقم ٦٣٠٥٥ لسنة ٦٨ ق بتاريخ أغسطس ٢٠١٥ (حكم غير منشور).

#### ٦- وثائق:

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

#### ٧- مواقع إلكترونية:

- موقع المكتب الفيدرالي الألماني لأمن المعلومات [www.bsi.bund.de](http://www.bsi.bund.de)

موقع ويكيديا

- <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>

#### ٨- مقالات:

- د/سمير فرج: الفضاء السيبراني-مقال منشور بالموقع الإلكتروني لجريدة الأهرام المصرية بتاريخ ٣٠ يوليو ٢٠٢٠ - آخر تحديث ٢٠/٨/٢٠٢١

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

٢- مريم عراق: دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة

٢٠٢٠: مقال منشور على الموقع الإلكتروني [/https://www.mondaq.com](https://www.mondaq.com)

آخر تحديث ٢٠/٨/٢٠٢١.

#### 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. 11, 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