التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي - دراسة مقارنة

Recent legislative developments in the field of information Comparative study-security

إعداد

د. ياسر محمد عبد السلام رجب

Dr.. Yasser Mohamed Abdel Salam Rajab

أستاذ القانون العام المشارك بكلية الحقوق جامعة القاهرة

والمستشار القانوني بوزارة العمل بدولة قطر

Doi: 10.21608/jinfo.2022.212981

استلام البحث : ٦ / ١٢ /٢٠٢١ **قبول النشر : ٢٠ / ١٢ / ٢٠٢١**

رجب ، ياسر محمد عبد السلام (٢٠٢٢). **التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي - دراسة مقارنة**. ***المجلة العربية للمعلوماتية وأمن المعلومات***، المؤسسة العربية للتربية والعلوم والآداب ، مصر، ٣ (٦) ، ١١٥ – ١٥٢.

التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي - دراسة مقارنة

المستخلص :

أصبحت قضية الأمن المعلوماتي من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما في ظل تنامي التهديدات الأمنية الإلكترونية ،ولإعتماد الإدارة والمؤسسات العامة والخاصة في الوقت الحالي على نظام الحكومة الإلكترونية، تتبدى الحاجة لتشريع منظم للأمن المعلوماتي يوازن بين اعتبارات الفاعلية من ناحية، واعتبارات المشروعية بالحفاظ على الحقوق الفردية للأفراد من ناحية أخرى . بمقارنة الوضع التشريعي الخليجي في مجال الأمن المعلوماتي نجد أن عُمان صاحبة السبق في ذلك ثم تلتها الإمارات العربية المتحدة التي تعد أول دولة عربية تصدر قانونًا مختصًا في مكافحة جرائم المعلومات. هنالك العديد من المحددات التي تجعل من تشريع الأمن المعلوماتي يحقق أهدافه يوازن بين اعتبارات الفاعلية والمشروعية كمثال الخصوصية ،وحيازة جهة الادارة للمعلومات وقواعد البيانات ،والشراكة المعلوماتية. من المحددات القانونية المهمة كأحد محددات الضبط التشريعي في مجال الأمن المعلوماتي ما يتعلق بمبدأ السرية الإلكترونية للأفراد والاتصالات، أوحماية الخصوصية ، وذلك من خلال تقنين الإدارة لأنشطتها في حيازة المعلومات، حيث تعد حيازة جهة الادارة للمعلومات وقواعد البيانات أحد محددات الضبط التشريعي حيث يفضل أن ينص التشريع المنظم للأمن المعلوماتي على عدة معالجات لاحتكار المعلومات كحيازة المعلومات على ميزان المشروعية ،وحيازة البيانات الروتينية،والآليات المعتادة لرصد وحيازة البيانات والمعلومات ،وحيازة الإدارة للمعلومات البيومترية. بناء على ما تقدم انتهى البحث لعدة توصيات تتلخص في : أولا تعديل التشريعات المعلوماتية العربية بما يؤدي لتفعيل استراتيجيات ادارية أكثر فاعلية تتيح حيازة المعلومات على نحو مشروع وخاصة فيما يتعلق بحيازة البيانات الروتينية والمعلومات البيومترية،واحترام الخصوصية كأحد محددات الضبط التشريعي ،وثانيا : تحديث الآليات المعتادة لرصد وحيازة البيانات والمعلومات والعمل على حل اشكاليات حيازة جهة الإدارة للمعلومات،وثالثا: تعديل التشريعات المعلوماتية العربية بما يساهم في ضرورة التعاون الدولي لتوفير الحلول التنسيق على مستوى التشريع القانوني والرقابي.

الكلمات المفتاحية : الأمن السيبراني-الأمن المعلوماتي - المعلومات البيومترية- البيانات الروتينية- التهديدات السيبرانية .

Abstract:

The issue of information security has become one of the major challenges at the regional and global levels, especially in light of the growing electronic security threats, and because the administration and public and private institutions depend at the present time on the e-government system, the need arises for an organized information security

legislation that balances considerations of effectiveness on the one hand, and considerations of legality by maintaining On the individual rights of individuals on the other hand. By comparing the Gulf legislative situation in the field of information security, we find that Oman took the lead in this, followed by the United Arab Emirates, which is the first Arab country to issue a law specialized in combating information crimes. There are many determinants that make information security legislation achieve its goals, balancing considerations of effectiveness and legitimacy, such as privacy, the administration's possession of information and databases, and informational partnership. One of the important legal determinants as one of the determinants of legislative control in the field of information security is related to the principle of electronic confidentiality of individuals and communications, or the protection of privacy, through the administration's legalization of its activities in the possession of information, where the administration's possession of information and databases is one of the determinants of legislative control where it is preferred that the legislation stipulates The information security regulator has several treatments to monopolize information, such as the possession of information on the balance of legitimacy, the acquisition of routine data, the usual mechanisms for monitoring and acquiring data and information, and the administration's possession of biometric information. Based on the foregoing, the research ended with several recommendations summed up in: First, amending Arab information legislation to activate more effective administrative strategies that allow legitimate possession of information, especially with regard to the possession of routine data and biometric information, and respect for privacy as one of the determinants of legislative control, and second: updating the usual mechanisms To monitor and acquire data and information and work to solve the problems of the administration's possession of information, and third: Amending Arab information legislation to contribute to the need for international cooperation to provide solutions for coordination at the level of legal and regulatory legislation.

key words : Cyber security - information security - biometric information - routine data - cyber threats - data and information - Arab information legislations.

مقدمة

أصبحت قضية الأمن المعلوماتي من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما في ظل تنامي التهديدات الأمنية الإلكترونية على مستوى الدول والمؤسسات العامة والحكومية والخاصة سواء بالنظر لعدد الهجمات أو الأضرار الناجمة عنها، غير إن مسألة الأمن المعلوماتي مسألة قانونية أكثر منها مسألة تقنية لتعلقها بمجالات الخصوصية Privacy وأمن المعلومات Data security، فلا بد أن تعد الجهات الادارية حزمة قوانين منظمة للأمن المعلوماتي، وأن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر السيبرية[١].

لذا إن لم يكن الفضاء الإلكتروني والمعلوماتي وسيلة موثوقة بها للاتصال أو التجارة فسيعرض الأفراد كما الشركات عن الاستثمار ، ويزيد من احتمالية ذلك الفرض التقاعس الحكومي في دول العالم - خاصة العالم الثالث - عن توفير وتطبيق الإجراءات الدفاعية اللازمة[٢].

ويتهدد الأمن المعلوماتي للإدارة بصورة كبيرة لإعتماد الإدارة في الوقت الحالي في إدارتها لمرافقها على نظام الحكومة الإلكترونية، وقد يصل الأمر لإنتهاك أمن الدولة الوطني، كالإطلاع على معلومات تمس أمن الدولة، أو الوصول إلى أنظمة التحكم في محطات المفاعلات النووية.[٣]

علاوة على ماتقدم هنالك العديد من المحددات التي تجعل من تشريع الأمن المعلوماتي عاملا ناجعا يحقق أهدافه كمثال الخصوصية ،وحيازة جهة الادارة للمعلومات وقواعد البيانات ،والشراكة المعلوماتية،ومن المهم دراسة تلك المحددات في العديد من التشريعات المقارنة.

([1]) The Emergence of cyber security law, prepared for the Indiana university Maurer school of law by Hanover Research, February, 2015. P,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".

(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 لذلك لا يمكن ضمان حماية الأمن السيبراني من خلال نشر أحدث وسائل التكنولوجيا فقط ، بل يجب أن يؤخذ في الاعتبار أيضا الأشخاص والعمليات التي تتفاعل مع النظم فالأمن السيبراني منظومة تتركز حول عناصر أساسية منها : نشر الوعي بين الأفراد، وإبراز أفضل الممارسات، ومعرفة أفضل الوسائل لمشاركة المعلومات.

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

- **إشكالية البحث:**

تثور اشكالية البحث الأساسية حول كيفية إعمال التشريع المنظم للأمن المعلوماتي للتوازن بين اعتبارات الفاعلية من ناحية (تحقيق دور الجهات الادارية في حفظ أمن الفضاء المعلوماتي والشراكة المعلوماتية)،واعتبارات الحفاظ على الحقوق الفردية للأفراد من ناحية أخرى(الحفاظ على الخصوصية المعلوماتية كمثال)

- **الأهداف المبتغاة من دراسة هذا الموضوع:**

١-بحث موقف التشريعات من إعمال التوازن بين الاعتبارات المنظمة للأمن المعلوماتي،وترسيخ الحفاظ على الخصوصية المعلوماتية ،وتوضيح بعض أدوار الجهات الادارية من خلال الضبط الاداري في إعمال ذلك التوازن والحفاظ المشار اليهما.

٢- الوقوف على الاشكاليات الناتجة عن حيازة جهة الادارة للمعلومات وقواعد البيانات كأحد محددات الضبط التشريعي.

٣-الوقوف على جدوى شراكة معلوماتية بين القطاع الخاص والجهات الادارية،أو بين الدول لتحقيق تكاملية أمنية معلوماتية .

أهمية البحث:

[١] على الصعيد العلمى

تمثل الكتابة في مجال الأمن المعلوماتي من المجالات المستحدثة لتعلقها بتشريعات الحاسب الآلي ،والتشريعات الالكترونية ،ولذلك تتركز معظم الكتابات عنها في مجال القانون الخاص ،ولذلك تتبدى أهمية البحث لوجود قصور فنى وقانونى في الكتابة عن الأمن التعاقدي وتحقيقه في القانون العام،وخاصة القانون الاداري.

[٢] على الصعيد العملى:

-تتبدى أهمية البحث لتعرضه لمحددات الضبط التشريعي للأمن المعلوماتي في النظم القانونية المقارنة،وخاصة بدول مجلس التعاون الخليجي ،ولتعرضه لاشكاليات الخصوصية المعلوماتية كأحد محددات الضبط التشريعي

- تتبدى كذلك أهمية البحث لتعرضه لحيازة جهة الادارة للمعلومات وقواعد البيانات كأحد محددات الضبط التشريعي بين اعتبارات القاعلية والمشروعية.

- تتبدى كذلك أهمية البحث لتعرضه لفكرة الشراكة المعلوماتية كأحد محددات الضبط التشريعي .

- **صعوبات البحث:**

١- ندرة المؤلفات الفقهية التى تناولت الأمن المعلوماتي فى القانون الاداري خاصة أن الأمن المعلوماتي يقع على تخوم العديد من القوانين كالقانون العام والقانون الخاص، فضلاً عن قانون التجارة الدولية، بل وقوعها بين فرعين من العلوم وهما القانون والحاسبات الآلية .

٢- غموض بعض المصطلحات التقنية في مجال الأمن المعلوماتي كمثال الطيف الترددي ،ومثال "أتمتة الملفات"

منهج البحث:

يقوم على منهجين أحدهما استقرائي عن طريق رد الفروع إلى أصولها، والآخر استباطي بتحليل نصوص القوانين المقارنة بالإضافة لتحليل بعض الفقرات بالإضافة إلى عرض الآراء الفقهية.

بالإضافة إلى المنهج المقارن بتناول العديد من القوانين كالقانون الأمريكي والانجليزي وقوانين دول مجلس التعاون الخليجي كالقانون القطري و الكويتي والاماراتي والسعودي والعماني.

المبحث الأول

التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي في النظم القانونية المقارنة.

تعتمد بعض الأنظمة القانونية على تشريعات أمن معلوماتي فعالة موضوعيا واجرائيا على العكس من البعض الآخر يعتمد على قوانين غير فعالة. (٤)

لذلك يمكن أن يتحدد الضبط التشريعي للأمن المعلوماتي في اتجاهين:

الأول – تناسب العقوبة مع تأثير الجريمة فالعقوبة تكون بسيطة في حالة انتهاك الأمن المعلوماتي بقصد التسلية والعبث، وتكون شديدة في حالات سرقة الأموال أو سرقة المعلومات.

الثاني – توقيع عقوبة مشددة على أية حالة من حالات الانتهاك الأمني المعلوماتي بغض النظر عن تأثير الانتهاك ودوافع الجاني. (٥)

---

(4)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): Jona than clough, principles of cyber crime (2010). p. 6

(2) Richard Clarke, threats to U.S. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, 12 Depaul Bus, L. J. (1999 – 2000). p. 8

(٥) تنقسم شخصيات الجناة الإلكترونيين إلى:

١) المتطفلون: "Hackers" وهم مجموعة من الناس يقصدون التسلية لغرض إثبات قدرتهم على الاختراق أو تحديهم أو لمجرد المزاح.

٢) محبو المال: وهم مبرمجون موهوبون يقومون بالاحتيال لسرقة الأموال من المصارف أو مؤسسات الأعمال.

٣) المحترفون: وهم مجموعة من الناس، يقصدوا سرقة معلومات هامة وحساسة وسرية والهدف المقصود غالبًا لذلك النوع هي الدوائر الحكومية والعسكرية.

ويرى الفقه المقارن أن المعالجة التشريعية للأمن المعلوماتي تكون بطريقتين أولهما قوانين التجسس وثانيهما قوانين الاتصالات. (٦)

غير أنه تجدر الإشارة إلى أن بعض التشريعات تعاني قصورًا تشريعيًا في الأمن المعلوماتي ويتمثل ذلك القصور التشريعي أحيانًا في حداثة الفعل المؤدى لانتهاك الأمن المعلوماتي، أو عدم الفهم المتكامل لعناصر الفعل الإجرامي ومثال ذلك جريمة الدخول غير المصرح للنظام المعلوماتي، فالمتتبع لتلك الجريمة يجد أنها من الصعوبة بمكان كي تتم معالجتها تشريعيًا بموجب النصوص العقابية التقليدية. (٧)

ومن أحد أهم أدوات الضبط التشريعي تشديد العقوبات إذا تعلق انتهاك الأمن المعلوماتي بالأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية. (٨)

---

(٦) Abraham D. Safaer, National security and leaks, the Government's Autority to Discipline itself. International studies in Human Rights volume 16, p. 69.

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

(٨) نص المشرع القطري في القانون رقم ١٤ لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية (منشور على شبكة المعلومات الدولية على الرابط http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar آخرتحديث ٢٠٢١/١٠/٦)في المادة "٢" على أن "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها."

"وتضاعف العقوبة المنصوص عليها في الفقرة السابقة إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك. أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة" .

وحسنا نص المشرع في الفصل الثالث: (التزامات أجهزة الدولة) في المادة ٢٢

على أن "تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

١- اتخاذ التدابير الأمينة الوقائية اللازمة لحماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكاتها المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها.

٢- سرعة إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القانون فور اكتشافها أو اكتشاف أي محاولة للالتقاط أو الاعتراض أو التنصت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات اللازمة لكشف الحقيقة.

علاوة على ماسبق تتعدد تشريعات الأمن المعلوماتي فيما يتعلق بقوانين الكمبيوتر كالتالي:
١) تشريعات حماية برامج الكمبيوتر وهي تعكس الاتجاهات العالمية "في إدراج الملكية الفكرية ضمن تنظيمات التجارة الدولية نتيجة للاقتصاد الرقمي والاقتصاد المؤسسي على المعرفة.
٢) تشريعات الأصول الإجرائية الجزائية وهي في الواقع تطوير لقواعد الإثبات في الإجراءات لكنها تتصل بالحقوق الجديدة المعترف بها في الميدان التقني المعلوماتي.
٣) تشريعات المحتوى الضار وهي تهدف في المقام الأول للحماية من محتوى المعلوماتية على الأمنية.
٤) تشريعات معايير الأمن المعلوماتي وهي تهدف إلى تبادل البيانات والتشفير ويستهدف البعض دراستها ضمن محتوى التجارة الإلكترونية. [٩]

٣- الاحتفاظ ببيانات تقنية المعلومات ومعلومات المشترك لمدة لا تقل عن (١٢٠) يوماً، وتزويد الجهة المختصة بتلك البيانات.
٤- التعاون مع الجهة المختصة لتنفيذ اختصاصاتها.".
ونص المشرع الإماراتي كمثال في المادة ٢٢ من القانون الاتحادي الإماراتي لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات (منشور على شبكة المعلومات الدولية على الرابط -http://www.gcc legal.org/BrowseLawOption.aspx?country=2&LawID=3168 آخرتحديث ٢٠٢١/١٠/٦)على أن "يعاقب بالسجن كل من دخل بغير وجه حق موقعًا أو نظامًا مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك... ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والتجارية والاقتصادية".
(٩) هناك العديد من تشريعات الأمن المعلوماتي على مستوى العالم نذكر منها على سبيل المثال في الولايات المتحدة الأمريكية قانون خصوصية الاتصالات الإلكترونية لعام ١٩٨٦، وقانون خصوصية الاتصالات لعام ١٩٩٧، وقانون خصوصية المعطيات لعام ١٩٩٧ – أما في ألمانيا نجد قانون حماية المعطيات ومشروع قانون حماية البيانات عام ٢٠٠٠ المتوافق مع القانون الأوروبي لعام ١٩٩٥، وفي فرنسا قانون معالجة الآلية للمعطيات والمعدل في عام ٢٠٠٠، وفي النرويج قانون تسجيل البيانات الشخصية لعام ٢٠٠٠، وفي بلجيكا قانون حماية الحياة الخاصة في ما يتعلق بالتعامل مع المعطيات الشخصية المعدل عام ٢٠٠٠، وفي هذا قانون حماية البيانات الشخصية والوثائق الإلكترونية لعام ٢٠٠٠، وفي بريطانيا قانون حماية المعطيات لعام ١٩٨٤ وقانون حماية البيانات لعام ١٩٩٨ المعدل لقانون ١٩٨٤، وقانون حرية المعلومات لعام ٢٠٠٠، وفي اليابان قانون حماية المعلومات في الشخصية رقم ٩٥ الصادر في ١٩٩٨/١٢/١٦ وفي التشيك قانون حماية البيانات الشخصية في نظم المعلومات لعام ١٩٩٢ وقانون حماية البيانات لعام ٢٠٠٠، وفي هنجاريا قانون حماية البيانات الشخصية ونشر البيانات للمصالح العامة لعام ١٩٩٢، وفي رومانيا قانون حماية البيانات لعام ١٩٩٢، وفي كوريا الجنوبية قانون حرية المعلومات لعام ١٩٩٦، وفي روسيا قانون حماية المعلومات لعام ١٩٩٥، وفي إيطاليا قانون حماية البيانات لعام ١٩٩٦، وفي ليتوانيا قانون الحماية القانونية للبيانات الشخصية لعام ١٩٩٦، وفي الصين نظم حماية وإدارة الشبكات لعام ١٩٩٧، وفي تايلند قانون حماية البيانات في القطاع العام لعام ١٩٩٨، وفي الهند مشروع قانون حماية البيانات الموصى بإصداره من الفريق الوطني لتقنية

والجدير بالذكر أن المشرع القطري قد انتهج في القانون رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية سبيلين مختلفين لحماية الأمن المعلوماتي وذلك من خلال تبنيه لمنهج استثناء بعض البيانات الشخصية من الحماية التشريعية المعلوماتية اذا ارتبطت بالنظام العام كمثال مانصت عليه المادة ١٨ من الفصل الخامس (الاعفاءات)بأن "للجهة المختصة أن تقرر معالجة بعض البيانات الشخصية دون التقيد بأحكام المواد(4) ، (9)، (15)، (17) من هذا القانون، وذلك لتحقيق أي من الأغراض الآتية:

١- حماية الأمن الوطني والأمن العام.

٢- حماية العلاقات الدولية للدولة.

٣- حماية المصالح الاقتصادية أو المالية للدولة.

٤- منع أي جريمة جنائية، أو جمع معلومات عنها، أو التحقيق فيها.

وتحتفظ الجهة المختصة بسجل خاص تقيد به البيانات التي تحقق الأغراض المشار إليها، ويصدر بتحديد شروط وضوابط وأحوال القيد في هذا السجل قرار من الوزير."

أما المنهج الآخر فهو اسباغ مزيد من الحماية التشريعية لبعض البيانات كمثال مانصت عليه المادة16 من الفصل الرابع(البيانات الشخصية ذات الطبيعة الخاصة)حيث نصت على أنه"تعد بيانات شخصية ذات طبيعة خاصة، البيانات المتعلقة بالأصل العرقي، والأطفال، والصحة أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية، والجرائم الجنائية،وللوزير أن يضيف أصنافاً أخرى من البيانات الشخصية ذات الطبيعة الخاصة، إذا كان من شأن سوء استخدامها أو إفشائها إلحاق ضرر جسيم بالفرد.ولا يجوز معالجة البيانات الشخصية ذات الطبيعة الخاصة، إلا بعد الحصول على تصريح بذلك من الإدارة المختصة، وفقاً للإجراءات والضوابط التي يصدر بتحديدها قرار من الوزير للوزير، بقرار منه، فرض احتياطات إضافية لغرض حماية البيانات الشخصية ذات الطبيعة الخاصة."

التجربة الأمريكية في تعزيز الأمن المعلوماتي

تنقسم التجربة الأمريكية في تعزيز الأمن المعلوماتي إلى شقين أولهما المعايير الفنية Technical standatds والتشريعات والرقابة Legislation and Moitoring ونتناولهما كالتالي:- (١٠)

المعلومات وتطوير البرمجيات وفي جنوب أفريقيا قانون الوصول إلى المعلومات لعام ٢٠٠٠، وفي تركيا مشروع قانون حماية البيانات الشخصية لعام ٢٠٠٠.

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

وانظر أيضا في التجربة الفرنسية في حماية الحق في الخصوصية المعلوماتية مرجع د/شريف يوسف خاطر: حماية الحق في الخصوصية المعلوماتية -دراسة تحليلية لحق الاطلاع على البيانات الشخصية –دراسة مقارنة-دار الفكر والقانون ٢٠١٥،وقد آثرنا عدم التطرق لتلك التجربة كي نلقي الضوء على تجارب أخرى لم تطرقها طرق البحث.

١- المعايير الفنية

تم إنشاء المعهد القومي للمعايير القياسية والتكنولوجيا كباكورة أولية في عام ١٩٠١ يتبع وزارة التجارة الأمريكية، علاوة على وحدة المعلومات التابعة لمعمل تكنولوجيا المعلومات حيث تضع سياسات ومعايير تبادل المعلومات. (١١)

ومن أهم اللجان لجنة الحاسب والاتصالات التابعة للمجلس القومي للبحوث، وترجع أهمية تلك اللجنة إلى أنها تشفر المعلومات والبيانات "cryptography". (١٢)

٢- التشريعات والرقابة

لن تكتمل منظومة الأمن المعلوماتي سوى بوجود إطار تشريعي لذا صدرت في الولايات المتحدة الأمريكية قوانين تعزز ذلك كقانون حرية المعلومات في عام ١٩٦٦ ،ويأتي القانون الفيدرالي لأمن المعلومات الصادر في عام ٢٠٠٢ كأهم التشريعات التي تعزز الأمن المعلوماتي لجهة الإدارة في الولايات المتحدة الأمريكية من خلال إلزام المؤسسات والهيئات بالإجراءات القياسية التي أصدرها المعهد القومي للمعايير القياسية والتكنولوجيا. (١٣)

ويوفر القانون الفيدرالي لأمن المعلومات الصادر في عام ٢٠٠٢ إطارًا لتأكيد فعالية السيطرة الإدارية على مصادر المعلومات بما فيها حماية المعلومات الفيدرالية ونظم المعلومات مع تحديد اختصاصات لكن رئيس وكالة فيدرالية(١٤)

---

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

(١٢) المرجع السابق ص١٨٢ في إشارة إلى المرجع:

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

(١٣)وإذا كان غرض قانون حرية المعلومات في عام ١٩٦٦ هو تعزيز الحق في تداول المعلومات إلا أن التعديلات اللاحقة على ذلك القانون كانت تهدف إلى تعزيز السرية والأمن المعلوماتي والدليل صدور التعديل الذي يقضي مجموعة المعلومات الإلكترونية Electronic freedom of Information Act)) (EFIA) لتعزيز الأمن المعلوماتي حيث يطالب جميع جهات الإدارة (بأتمتة الملفات) أي جعل الملفات الورقية في صورة إلكترونية وإعداد فرنسا خاصة لإطلاع المواطنين عليها.

لمزيد من الإيضاح أنظر د/ راشد محمد المري، المرجع السابق ص١٨٣.

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

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

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

٣) تنفيذ السياسات والإجراءات التي تقلل المخاطر لأدنى حد ممكن

٤) القيام باختبارات دورية وتقييم لأدوات أمن المعلومات.

- أما على صعيد الرقابة تم إنشاء فريق الإستعداد في عام ٢٠٠٣ كجزء رئيسي من وحدة الأمن القومي الافتراضي (National cyper security Division). [١٥]
علاوة على ماسبق كان الفقه القانوني الأمريكي يرى أن الكونجرس عليه أن يقوم برسم استراتيجية واضحة[١٦] لدور جهة الإدارة في تعزيز الأمن المعلوماتي من خلال الضبط الإداري ويرتكز ذلك على إصلاح قانون إدارة أمن المعلومات الاتحادية لعام ٢٠٠٢.
Federal Information security Management Act of 2002 (FISAAA)
والعديد من المحاور الهامة الأخرى. [١٧]

ويهدف القانون الفيدرالي لأمن المعلومات الصادر في عام ٢٠٠٢ إلى ثلاثة أهداف وهي:-
أولاً: السرية: الاحتفاظ بالقيود المرخص بها على الوصول إلى المعلومات وكشفها بما في ذلك الوسائل الخاصة بحماية الخصوصية الشخصية والمعلومات المملوكة لجهة ما.
ثانيًا: السلامة: منع دخول معلومات غير صحيحة أو إتلاف المعلومات.
ثالثًا: التوفر (الإتاحة): ضمان الوصول الفوري والموثوق به للمعلومات واستخدامها.

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

(16) See office of TECH: Assessment, Electronic Record system anti individual privacy 57 (1986).

(17) The Emergence of cypersecurity law op .cit., p.12

ومن تلك المحاور التي أوردها الفقه القانوني الأمريكي:-
١) حماية البنية التحتية الحيوية (وخاصة شبكة الكهرباء والصناعات الكيماوية).
٢) تبادل المعلومات والتنسيق بين القطاعات.
٣) مراعاة انتهاكات السرقة أو التعرض للبيانات الشخصية كالمعلومات المالية.
٤) مراعاة السياسة العقابية لجرائم الإنترنت.
٥) مراعاة الخصوصية في مجال التجارة الإلكترونية.
٦) الجهود الدولية في الأمن المعلوماتي.
٧) البحث والتطوير.
٨) تطوير القوى العاملة في مجال الأمن السيبري.

والجدير بالذكر أن هناك عدة تشريعات تم إدخالها إلى الكونجرس مؤخرًا تمس الأمن السيبري ومن تلك القوانين قانون خصوصية المعلومات الشخصية وأمنها لعام ٢٠١٤ من شأن ذلك القانون حفاظ الشركات على المعلومات الاستهلاكية في مأمن من قراصنة الكمبيوتر.
وهناك أيضًا قانون أمن البيانات لعام ٢٠١٤ (Data security Act 2014) ويلزم ذلك القانون الكيانات بما في ذلك المؤسسات المالية والوكالات الاتحادية بحماية أفضل للمعلومات الحساسة، والتحقق من الخروقات الأمنية المعلوماتية وإخطار المستهلكين بذلك عند وجود خطر كبير من سرقة الهوية والاحتيال.
وثالثًا هناك القانون الوطني للأمن السيبراني وحماية البنية التحتية الحيوية لعام ٢٠١٣.
"The Natioal cybersecurity and infrastructure protection 2013 Act".

أضف إلى ماسبق تقوم النظم القانونية الأوروبية بتغليب الأمن المعلوماتي في حالة تهديد الأمن العام. (١٨)

التجربة الخليجية في تعزيز الأمن المعلوماتي

بمقارنة الوضع التشريعي الخليجي في مجال الأمن المعلوماتي نجد أنه يسايرتعزيز الأمن المعلوماتي حيث كانت عُمان صاحبة السبق في ذلك (١٩) ثم تلتها الإمارات العربية المتحدة. (٢٠)

حيث إن سلطنة عُمان من الدول سابقت في الحفاظ على أمنها المعلوماتي من خلال قطاع الاتصالات حيث تم إقرار قانون الاتصالات رقم ٣٠ لسنة ٢٠٠٣ لتعزيز بيئة معلوماتية آمنة للقطاع الاستثماري. (٢١)

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

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

كمثال ما نصت عليه المادة الثالثة من القانون الفرنسي الصادر في ١٠ يوليو ١٩٩١ على الأسباب القانونية التي يمكن الاستناد إليها لإجراء المراقبة أو التصنت الإداري والتي جاء فيها (يجوز الإذن أو التصريح ... بالتصنت الذي يكون موضوعه أو محله البحث عن المعلومات التي تهم الأمن القومي، المحافظة على المصالح الاقتصادية والعلمية للمجتمع الفرنسي، منع الإرهاب والمجموعات الإجرامية المنظمة وكذلك منع تكوين أو إعادة تكوين المجموعات التي تم حلها وفقًا لقانون ١٠ يناير ١٩٦٣"

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

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

(١٩) ثم ذلك من خلال تعديل قانون الجزاء العماني رقم ٧ والذي صدر عام ١٩٧٤ بموجب المرسوم السلطاني رقم ٢٠٠١/٧٢م،والجدير بالذكر صدور قانون الجزاء العماني بموجب المرسوم السلطاني رقم ٧ لسنة ٢٠١٨ باصدار قانون الجزاء العماني-الجريدة الرسمية التي تصدرها وزارة الشؤون القانونية بسلطنة عمان-السنة السابعة والأربعون بتاريخ ١٤ يناير ٢٠١٨ مرددا ذات الأحكام في الباب الأول من الكتاب الثاني.

(٢٠) تعد الإمارات العربية المتحدة أول دولة عربية تصدر قانونًا مختصًا في مكافحة جرائم المعلومات وذلك بموجب القانون الاتحادي رقم (٢) لسنة ٢٠٠٦.

أما المملكة العربية السعودية عززت أمنها المعلوماتي بالمرسوم الملكي رقم ١٧ بتاريخ ١٤٢٨/٣/٧هـ بنظام مكافحة جرائم المعلوماتية (منشور على شبكة المعلومات الدولية على الرابط www.mof.gov.sa/docslibrary/RegulationsInstructions/Documents آخرتحديث ٢٠٢١/١٠/٦) من خلال وضع آلية نظامية للحد من انتهاك الأمن المعلوماتي كي تتحقق استخدامات الحاسب بزيادة تحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات والشبكات وحماية النظام العام الخلقي (الأخلاق والآداب العامة).

(٢١) د/ حسين بن سعيد الغافري، المرجع السابق ص٦٥.

وذهبت المادة ٦١ من هذا التشريع على العقاب بالسجن مدة لا تزيد على سنة، وبغرامة لا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين للعديد من الأفعال [٢٢]
وقد احتوى التشريع العماني على العديد من المصطلحات التي تركز على أمن الفضاء المعلوماتي[٢٣]. وقد ركزت المادة السادسة من القانون على حماية البيانات والمعلومات الإلكترونية الحكومية السرية واعتبر أن البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة. [٢٤]

في إشارة إلى العقيد/ محسن بن علوي آل حفيظ: موجز عن قانون تنظيم الاتصالات ٣٠ لسنة ٢٠٠٢ – الندوة التعريفية بأحكام قانون الاتصالات - مسقط ٢٠٠٩.

"رغبة من المشرع العماني في إيجاد إطار قانوني فعال لتنظيم قطاع الاتصالات بالسلطنة ولتشجيع المنافسة الشريفة وخلق بيئة مستقرة تتسم بالشفافية وتعزيز ثقة المستثمرين في هذا المجال" حيث خضع القانون ومنذ صدوره في عام ٢٠٠٢ للعديد من التعديلات آخرها ٢٠٠٨.

(٢٢)منها كل من أرسل بواسطة نظام أو أجهزة أو وسائل الاتصالات رسالة مخالفة للنظام العام أو الآداب العامة مع علمه بذلك، بما يعني تعزيز الضبط التشريعي العماني للأمن الفضاء المعلوماتي ورؤيته المبكرة، للنظام العام المعلوماتي على الصعيد المادي والأخلاقي.. لم ينتهي الأمر عند هذا الحد بل جاء المشرع العُماني بقانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١(منشور على شبكة المعلومات الدولية على الرابط http://www.gcc-legal.org/BrowseLaws.aspx?country=1- آخرتحديث ٢٠٢١/١٠/٦) للرغبة في سد الفراغ التشريعي في ذلك المجال أتت فكرة هذا القانون من خلال رغبة المشرع العماني في سد الفراغ التشريعي حيث بدأت صياغة هذا القانون في الربع الأخير من ٢٠٠٨ وتم الانتهاء من إعداد المسودة الأولى منه في الربع الثالث من ٢٠٠٩ وإحالته للجهات المختصة لإبداء ملاحظاتها عليه، ثم صدر في الربع الأول من ٢٠١١ بموجب المرسوم السلطاني ٢٠١١/١٢، وانقسم القانون إلى ٣٠ مادة موزعة على ٦ فصول.

(٢٣) احتوى القانون على العديد من المصطلحات كالتالي:

- تقنية المعلومات: الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات.
- البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات.
- البيانات والمعلومات الحكومية: البيانات والمعلومات الإلكترونية الخاصة بوحدات الجهاز الإداري للدول.
- الشبكة المعلوماتية: ارتباط من أكثر وسيلة لتقنية المعلومات للحصول على البيانات والمعلومات الإلكترونية وبناء لها.
- الالتقاط: مشاهدة البيانات والمعلومات الإلكترونية أو الحصول عليها.

(٢٤) نصت المادة السادسة على أن "يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدًا ودون وه حق موقعًا إلكترونيًا أو نظامًا معلوماتيًا بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك، وتكون العقوبة السجن مدى لا تقل عن ثلاث

وذهب التشريع العماني كذلك في المادة الثالثة منه إلى تجريم الدخول العمدي بدون وجه حق إلى المواقع الإلكترونية أو الأنظمة المعلوماتية أو وسائل التقنية المعلوماتية [٢٥] ،وهناك العديد من النصوص التي لا يتسع المقام لذكرها حافظت على النظام العام العماني وأمن الفضاء المعلوماتي هناك من خلال تجريم الجرائم الإلكترونية للإتجار في البشر[٢٦]، والجرائم الإلكترونية لغسل الأموال[٢٧]، والجرائم الإلكترونية للإتجار في الأعضاء البشرية[٢٨]، والجرائم الإلكترونية لتجارة الأسلحة[٢٩]، والجرائم الإلكترونية لتجارة

سنوات ولا تزيد على عشر سنوات غرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشر آلاف ريال عماني إذا ترتب على الفعل المجرم إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر البيانات أو المعلومات الإلكترونية. وتعد البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة."

(٢٥)وشدد العقوبة في حال إلغائه أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية أو إلحاق الضرر بالمستخدمين أو المستفيدين.حيث رفعت تلك المادة الحد الأدنى للسجن إلى سنة والحد الأقصى إلى ثلاث سنوات، ورفعت الحد الأدنى للغرامة على ألف ريال عماني، والحد الأقصى إلى ثلاثة آلاف ريال عماني في حالة إذا ما تم إرتكاب الجرائم الواردة في المادة الثالثة أثناء أو بمناسبة تأدية العمل. بل وإمعانًا في الحماية غلظت المادة الرابعة العقوبة على المتعاملين مع الفضاء المعلوماتي لافتراض الثقة في أشخاصهم، خاصة إذا كانوا في اعتقادنا من موظفي جهة الإدارة

(٢٦) أنظر المادة ٢٢ من قانون ١٢/ لسنة ٢٠١١ العماني.

أما المادة الثامنة من قانون ٢٠١١/١٢ العماني الخاص بمكافحة جرائم تقنية المعلومات جرمت الاعتراض العمدي ودون وجه حق لاستخدام وسائل تقنية المعلومات من خلال خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو التصنت عليها.

أما المادة العاشرة من ذات القانون جرمت الإعاقة أو التعطيل العمدي للوصول إلى حدمات الدخول إلى نظام معلوماتي أو وسائل تقنية المعلومات، وذلك باستخدام وسائل تقنية المعلومات.

وتطرقت المادة التاسعة عشر لحماية النظام العام والقيم الدينية حيث جرمت استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو نشر أو توزيع أو شراء أو حيازة كل ما من شأنه أن ينطوي على المساس بالقيم الدينية أو النظام العام.

وجاءت المادة عشرون لتكمل منظومة حماية النظام العام من خلال عنصر الأمن العام بتجريم إنشاء المواقع الإلكترونية لتنظيم إرهابي أو استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات لأغراض إرهابية أو نشر المبادئ الإرهابية والدعوة لها في تمويل العمليات الإرهابية أو تسهيل الاتصالات بين تنظيماتها أو بين أعضائها وقياداتها.

(٢٧) أنظر المادة ٢١ من قانون ١٢/ لسنة ٢٠١١ العماني.

(٢٨) أنظر المادة ٢٣ من قانون ١٢/ لسنة ٢٠١١ العماني.

(٢٩) أنظر المادة ٢٤ من قانون ١٢/ لسنة ٢٠١١ العماني.

المخدرات[٣٠]، والجرائم الإلكترونية لانتهاك الملكية الفكرية[٣١]، والجرائم الإلكترونية لتجارة الآثار[٣٢].

وكما أسلفنا بأن الإمارات العربية المتحدة تعد أول دولة عربية تصدر قانونًا مختصًا في مكافحة جرائم المعلومات وذلك بموجب القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ ،حيث كان لصدور قانوني التوقيع الإلكتروني في ٢٠٠٢، وقانون التجارة الإلكترونية صدى واسعًا في مجال الأمن المعلوماتي للأفراد، ولكن على المستوى القومي لم يتطرق إلى حماية البيانات الحكومية، لذا كانت الحاجة إلى صدور قانون مستقل وهو قانون مكافحة الجرائم المعلوماتية والذي صدر في يناير ٢٠٠٦ وقد تضمن الحفاظ على النظام العام في المعلوماتي بكافة عناصره سواء النظام العام العادي أو الأخلاقي وهو ما يتأكد في المادة ٢٠ من القانون ،ومن ناحية أخرى عمد المشرع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات إلى السير على درب المشرع الإماراتي في تقسيم مسارات تعزيز الضبط التشريعي للأمن المعلوماتي [٣٣]

وفى اعتقادنا أنه يجب الاعتماد على تقسيمات النظام العام بشقيه المادى والأخلاقى عند تحديد الأطر الحاكمة للضبط التشريعى ، ويؤكد على رأينا تبنى عدة تشريعات عربية لذلك عند تقسيم مسارات أوجه الإخلال بالأمن المعلوماتى كمثال ماجاء به القانون الكويتى رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات وذلك كالتالي: [٣٤]

(٣٠) أنظر المادة ٢٥ من قانون ١٢/ لسنة ٢٠١١ العماني.
(٣١) أنظر المادة ٢٦ من قانون ١٢/ لسنة ٢٠١١ العماني.
(٣٢) أنظر المادة ٢٧ من قانون ١٢/ لسنة ٢٠١١ العماني.
(٣٣) أنظر تفصيلاً قانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات – الكويت اليوم العدد ١٢٤٤ السنة الحادية والستون منشور بتاريخ ٢٠١٥/٧/١٢.

ومن الجرائم الإضرار بالأمن العام المعلوماتي خاصة، والأمن العام بصفة عامة عن طريق تجارة الرقيق الأبيض والمخدرات (المادة ٨ من القانون) وكذلك (المادة ٤ من القانون) ،والإضرار بالأمن العام عن طريق التهديدات الإرهابية الإلكترونية (المادة ١٠ من القانون).

(٣٤) أنظر تفصيلاً المرجع السابق :قانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات

حيث يررت المذكرة الإيضاحية لذلك القانون أن اتساع دائرة استخدام شبكة المعلومات الدولية أدى لتعدد المعلومات في كافة المجالات واستخدامها المتزايد مما ولد مخاطر جديدة وجرائم يطلق عليها "الجرائم المعلوماتية" منها الجرائم الماسة بالأخلاق والآداب العامة، وسرقة المعلومات، واختراق النظم السرية مما تطلب استحداث قوانين غير تقليدية لمواجهة ذلك.

١) تغليظ العقاب على تزوير مستندات رسمية أو بنكية أو بيانات حكومية أو بنكية إلكترونية (المادة ٣ فقرة ٢) ، والإضرار بالبيانات أو المعلومات الحكومية السرية عن طريق الدخول غير المشروع لها وتغليظ العقوبة في حالة إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها وذلك في (المادة ٣ فقرة ١) وهو مايتعلق بالأمن المعلوماتى لجهة الإدارة بمفهوم أشد تركيزا.

المبحث الثاني

دور الخصوصية في التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي

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

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

٢) معاقبة أي شخص يراقب تلك الاتصالات مع الأخذ في الاعتبار وجود بعض الاستثناءات في بعض التشريعات الأوروبية، ومنها جواز تدخل مقدم الخدمة المعلوماتية لانتهاك السرية إذا كان تدخله تبرره الضرورة الفنية، ومنها كذلك مراقبة صاحب العمل لمن يعمل معه استنادًا لرضائهم المفترض عن سياسة الرقابة الخاصة بمصلحة المشروع. (٣٥)

---

٢) الإضرار بالقطاع الطبي (المادة ٣ فقرة ٣) وهو مايتعلق بالنظام العام وخاصة فى أحد عناصره وهوالصحة العامة.

٣) الإضرار بالآداب العامة والأخلاق (المادة ٣ فقرة ٤) وهو مايتعلق بالنظام العام الأخلاقى.

والجدير بالذكر أن المشرع القطري قد عمد في القانون رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية لحماية النظام العام الخلقي كما نص في المادة ١٧ بأنه"مع مراعاة الالتزامات المنصوص عليها في هذا القانون، يجب على مالك أو مشغل أي موقع إلكتروني موجه للأطفال، مراعاة ما يلي:

١- وضع إخطار على الموقع حول ماهية بيانات الأطفال، وكيفية استخدامها، والسياسات التي يتبعها في الإفصاح عنها.

٢- الحصول على موافقة صريحة من ولي أمر الطفل الذي تتم معالجة بيانات شخصية عنه، وذلك عن طريق اتصال إلكتروني أو أي وسيلة أخرى مناسبة.

٣- تزويد ولي أمر الطفل، بناءً على طلبه، وبعد التحقق من هويته، بوصف لنوع البيانات الشخصية التي تتم معالجتها، مع بيان الغرض من المعالجة، ونسخة من البيانات التي تمت معالجتها أو جمعها عن الطفل.

٤- حذف أو محو أو وقف معالجة أية بيانات شخصية تم جمعها من الطفل أو عنه، إذا طلب ولي الأمر ذلك."

٥- ألا تكون مشاركة الطفل في لعبة، أو عرض جائزة، أو أي نشاط آخر، مشروطة بتقديم الطفل بيانات شخصية تزيد على ما هو ضروري للمشاركة في ذلك النشاط."

٤) الإضرار بالأمن العام المعلوماتي خاصة، والأمن العام بصفة عامة عن طريق تجارة الرقيق الأبيض والمخدرات (المادة ٨ من القانون) وكذلك (المادة ٤ من القانون)، والتهديدات الإرهابية الإلكترونية (المادة ١٠ من القانون).

(٣٥)د/أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة سنة ٢٠٠٦ص٤٨٨.

وتتعلق السرية الإلكترونية للأفراد بمدى وجود بنوك معلومات وبيانات، وتثور إشكالية بنوك المعلومات والبيانات على صعيدين أولهما: كمي، والثاني: كيفي [٣٦]
وفي ذات الاتجاه يؤكد بعضهم على أنه إذا كانت قوانين المعلومات تفضل احترام الخصوصية ومنح الأمن المعلوماتي للأفراد العاديين إلا أنه لا بد من إقامة توازن بين حق الفرد في الأمن المعلوماتي وبين حق المجتمع في المعرفة من خلال عدم حجب المعلومات التي تضر ضررًا بالغًا بالآخرين أو المجتمع ككل. [٣٧] فقد قررت المادة ٢٨ من قانون حماية البيانات لعام ١٩٩٨ في المملكة المتحدة استثناء حماية المعلومات الشخصية من الحماية في الخصوصية طالما تعلق الأمر بأغراض حماية الأمن القومي[٣٨].
ولكن من ناحية أخرى نصت الفقرة الثانية من ذات المادة من الجدول الأول من مبادئ حماية البيانات The Data protection principles على أن تكون طريقة الحصول على البيانات الشخصية لغرض أو للأغراض المحددة قانونًا وألا يتم معالجتها بطريقة غير متوافقة مع تلك الأغراض، وأكدت الفقرة الثالثة ذلك بأن تكون ذات تلك البيانات متوافقة وذات صلة مع الأغراض التي من أجلها تمت المعالجة[٣٩].
لذا مؤدى ما سبق يجب اتخاذ جهة الإدارة التدابير التنظيمية اللازمة والإجراءات التقنية ضد عمليات المعالجة غير المشروعة وغير المرخص بها ضد الفقد الفجائي، أو التدمير، أو خسارة تلك البيانات وهذا ما أكدته الفقرة السابعة، بل واتخاذ التدابير اللازمة لعدم نقل تلك المعلومات الشخصية لأي بلد خارج بلدان المنطقة الاقتصادية الأوروبية EEA ما لم تضمن تلك البلد حماية لتلك البيانات.
وعلى الصعيد الأمريكى يرى الفقه أن حماية الخصوصية تؤدي غالبًا إلى تعزيز الأمن المعلوماتي، وذلك من خلال تقنين الإدارة لأنشطتها في حيازة المعلومات، أو على الأقل تبرير قيامها بنشاط تجميع البيانات والمعلومات على مستوى المسئولين الأعلى، أو من خلال

(٣٦) د/ هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ١٩٩٢ ص٨٠. إذ على الصعيد الكمي هناك عدد هائل من البيانات والمعلومات تخزنها المؤسسات الكبرى في الشركات الحكومية، وكذلك جهة الإدارة، ومن تلك البيانات ما يتعلق بالوضع المادي، أو التعليمي أو العائلي، أو المهني، أو الصحي، وتعد الحاسبات وشبكات الاتصال هي الوعاء الذي يقوم بتخزين ومعالجة وتحليل تلك البيانات والمعلومات ،أما على الصعيد الكيفي يعد شيوع النقل الرقمي للبيانات مشكلة أمنية معلوماتية لسهولة استراق السمع والتجسس الإلكتروني.
(٣٧) عمر محمد سلامة العليوي، حق الحصول على المعلومات في ضوء القانون الأردني رقم ٤٧ لسنة ٢٠٠٧ – دراسة مقارنة – رسالة دكتوراه، كلية الحقوق، جامعة عين شمس سنة ٢٠١١، ص١٨١.
([38]) Data Protection Act 1998 Published by TSO, the stationery office p. 50 – Data pretention & Investigatory powers Act 2014 chapter 27.
([39])"Personal data shall be a dequate, relvant and not excessive in relation to the purpose or purposes for which they are processed".

لجنة من الكونجرس أو قضاة فيدراليين أو بمتطلبات الإذن القضائي أو أية إجراءات لحماية الخصوصية وجهود الأمن القومي[٤٠].

عامة تكمن الإشكالية في عدم وضوح الرؤية قانونًا عن المدى الذى يمكن أن يمد القطاع الخاص الحكومة بالبيانات الهائلة، وإلى أي مدى يمكن أن تقلق الادارة من البرامج الخاصة بحيازة المعلومات والبيانات لدى القطاع الخاص[٤١].

علاوة على ما سبق يمكن التخلي عن فكرة الخصوصية المعلوماتية إذا تعلق الأمر بالنظام العام للدولة وفقًا لقانون الأمن ومكافحة الإرهاب والجريمة ٢٠٠١ في المملكة المتحدة (الفصل ٢٤) حيث نصت الفقرة الثانية من المادة ١٧ على أن تلك البنود الواردة في ذلك القسم تطبق للكشف عن المعلومات بواسطة أو لمصلحة السلطة العامة. إذا كانت أغراض الكشف تلك المعلومات مصرح به بموجب البنود التالية:-

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

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

استطرادا لما سبق يمكن لبعض الدول أن تلجأ إلى قانون العقوبات لتعزيز الأمن المعلوماتي كمثال قانون العقوبات الأسترالي. [٤٢]

ويتضمن دليل حماية البيانات الأوروبي لعام ١٩٩٥ حماية فاعلة ضد استخدام البيانات الشخصية الحساسة. [٤٣]

([40]) Fred H. Cate, Government Data Mining:- The need for a legal framework, Hienonline – 43 Harv. C. R. C.L.L. Rev. 2008 p. 51.

([41]) Ibid, p. 51.

(42)Jonathan clough: principles of cybercrime-second edition -Cambridge press 2010., p. 124.

(٤٣) منير محمد الجنيهي، ممدوح محمد الجنيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي ٢٠٠٦ ص٨٤.

مثال تلك البيانات البيانات المتعلقة بالصحة والأمور المالية وإن كانت ظهرت العديد من الإشكاليات بشأنها جراء قدرة الجهات الخاصة والحكومية على الوصول للبيانات لذا ظهر التوجه الأوروبي نحو إيجاد جهة رقابة تعمل على تنفيذ القانون فيما يعرف في بعض الدول باسم (المفوض) وفي دول أخرى (المراقب) وفي دول ثالثة (مسجل البيانات)، ويفرض دليل حماية البيانات على الدول الأعضاء التزامات فيما يخص التأكد من أمنية البيانات الشخصية التي ترتبط بالمواطنين الأوروبيين تحظى بنفس المستوى من الحماية إذا نقلت إلى خارج الحدود أهمية معالجتها بأنظمة معلومات خارجها، ويحظر نقل البيانات إلى الدول التي لا توفر قوانينها حماية للخصوصية

علاوة على ما سبق أصدرت المفوضية الأوروبية في عام ٢٠٠٠ نموذجًا جديدًا لدليل معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية، وقد وسع ذلك الدليل من نطاق الحماية للأفراد عن طريق حماية البيانات المنقولة عبر الإنترنت ومنع السلوكيات الاتصالية الضارة في السوق التجاري الإلكتروني مثل (SPAM) البريد الإلكتروني. (٤٤)

يرى الفقه أن حماية الخصوصية تؤدي غالبًا إلى تعزيز الأمن المعلوماتي، وذلك من خلال تقنين الإدارة لأنشطتها في حيازة المعلومات، أو على الأقل تبرير قيامها بنشاط تجميع البيانات والمعلومات على مستوى المسئولين الأعلى، أو من خلال لجنة من الكونجرس أو قضاة فيدراليين أو بمتطلبات الإذن القضائي أو أية إجراءات لحماية الخصوصية وجهود الأمن القومي(٤٥).

في اعتقادنا أن مسألة التوازن بين الخصوصية والأمن المعلوماتي تحتاج إلى وضوح في فهم المقاصد وضبط الصياغات التشريعية المرتبطة، حيث قد تثير مسألة غموض المصطلحات عبئًا إضافيًا على الجهة القائمة بالتشريع والجهة القائمة بالضبط في مسائل الأمن المعلوماتي، ومثال ذلك: أن الدخول Access برز في العام ١٩٩٦ أمام محكمة كانساس العليا في قضية الولاية ضد Allen. (٤٦) وقد اعتمدت الحكومة الأمريكية على التعريف التشريعي الواسع لعبارة Access وذلك لعموميته بين التشريعات الولائية المبكرة لجرائم الحاسوب، ولكن المحكمة رفضت تفسير عبارة الدخول بأنها مجرد الاقتراب "To approach".

ومن القوانين الأمريكية التي تعالج إشكاليات الخصوصية والأمن المعلوماتي قانون "مشاركة وحماية المعلومات الرقمية (Cyper Intelligence Sharing and Protection Act) إذ

---

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

(45) Fred H. Cate, Government Data Mining:- The need for a legal framework, Hienonline – 43 Harv. C. R. C.L.L. Rev. 2008 p. 51.

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

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

يسمح ذلك القانون بمشاركة المعلومات ما بين الحكومة الأمريكية وشركات التقنية والتصنيع.[٤٧]

ومن القضايا التي أثيرت في فرنسا والتي تخص الأمن المعلوماتي ما قامت به شركة جوجل الأمريكية عندما استخدمت برنامج التصوير الحي للشوارع (street view) إذ انتهكت حينها أحكام قانون حماية المعلوماتية والحريات الفرنسي رقم (١٧-٧٨) وقد اعتبرتها اللجنة القومية للمعلوماتية في فرنسا منتهكة لأحكام القانون العام لعدم إخطارها لأن الخدمة تقدم معلومات تعريفية عن أفراد يمكن تحديدهم بالدمج مع بيانات الموقع ومعالجتها. [٤٨]

بالإضافة إلى ما سبق صدرت العديد من قوانين الخصوصية الأمريكية على مستوى القطاعات sectoral privacy laws كمثال تبنى قسم الصحة والخدمات الإنسانية The department of Health Human Services فى العام ٢٠٠١ قواعد - مصرح بها من الكونجرس – لا تجيز الإفصاح عن المعلومات الشخصية الصحية ما لم يكن ذلك في إطار من القانون[٤٩].

وعلى صعيد التشريعات العربية التي وازنت بين الأمن المعلوماتي وتعزيزه، وحماية الخصوصية والبيانات الشخصية من الانتهاك أو التدمير نص القانون الكويتي رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملا ت الإلكترونية في المادة ٣٥ منه على التزام الإدارة عند حيازتها وجمعها للمعلومات والبيانات أن تكون في وظيفتها تقوم بذلك في إطار مشروع، وفي الغرض الذي تم جمع المعلومات من أجله بل وألزمها في الفقرة الثانية من التحقق من دقة البيانات والمعلومات المسجلة، وأن تتخذ تدابير حمايتها من القضاء والتلف أو الإفشاء أو الاستبدال ببيانات غير صحيحة أو إدخال معلومات عليها على خلاف الحقيقة. [٥٠]

ولكن على الصعيد العملي تذهب بعض الآراء في دولة الكويت إلى إغلاق تويتر (الموقع الإلكتروني الاجتماعي الأكثر شهرة هناك)، ويلقي البعض بالعبء على وسائل الضبط الإداري – وخاصة وزارة الداخلية – في مواجهة اختراقات أمن الفضاء المعلوماتي والأدهى

---

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

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

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

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

من ذلك الوقوع في فخ المطالبة بإنشاء محكمة دولية إلكترونية لعلاج الجرائم المعلوماتية المهددة للنظام العام. (٥١)

أما الرأي الذي نميل إليه هو أن تلك المواقع أصبحت واقعًا لا بد من التعامل معه،فلا بد من الوصول إلى صيغة تجبر كل من يدخل إلى تلك المواقع بتسجيل بياناته الصحيحة والرسمية لإنهاء الحسابات المزيفة أو الحد منها على أقل تقدير. (٥٢)

و نصت المادة ٣٧ من قانون المعاملات الإلكترونية الكويتي رقم٢٠ لسنة ٢٠١٤ على أنه "فيما عدا ما تختزنه الجهات الحكومية الأمنية بسجلاتها وأنظمتها المعالجة الإلكترونية من بيانات أو معلومات تتعلق بالأشخاص – لاعتبارات تتعلق بالأمن الوطني للبلاد – يجوز للشخص أن يطلب من أي من الجهات المذكورة بالمادة السابقة بإطلاق على البيانات أو المعلومات الشخصية المسجلة لديها....". (٥٣)

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

(٥١) جريدة الشاهد الكويتية الورقية – العدد ٢٧١٦ صدرت الأربعاء ١٣ يوليو ٢٠١٧ الصفحة الثالثة.
انقسمت الآراء التشريعية والبرلمانية هناك إلى أربعة آراء:- الرأي الأول يرى تفعيل القانون الكويتي للجرائم الإلكترونية واللائحة التنفيذية، والرأي الثاني يرى سن تشريعات جديدة بها عقوبات رادعة لمن يضر بالنظام العام المعلوماتي، حيث يجب تنظيم التواصل الاجتماعي بما يتماشى مع الأمن العام والوحدة الوطنية، والرأي الثالث يرى إغلاق تويتر نهائيًا، أما الرأي الرابع والأخير فيرى وجوب التواؤم مع القضاء المعلوماتي بمتطلباته الحديثة. وهو الرأي الوسط الذي يمثل إليه.

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

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

الإداري لحماية النظام العام بمفهومه المثلث الأمن العام والصحة العامة والسكينة العامة للمواطنين".(٥٤)

المبحث الثالث

دور حيازة جهة الادارة للمعلومات وقواعد البيانات في التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي

تعد حيازة جهة الادارة للمعلومات وقواعد البيانات أحد محددات الضبط التشريعي حيث يفضل أن ينص التشريع المنظم للأمن المعلوماتي على عدة نصوص أهمها احتكار المعلومات، وان كان ذلك من الصعوبة بمكان لاعتبارات(المشروعية) أو حرية تداول المعلومات من ناحية،وللصعوبة التكنولوجية ، أو الآليات المعتادة لرصد وحيازة تلك المعلومات من ناحية ثانية،ولإشكاليات تحديد المقصود بالمعلومات والبيانات محل الحيازة من ناحية ثالثة، لذا ستكون معالجة ذلك المبحث فى النقاط الآتية:

أولا- حيازة المعلومات على ميزان المشروعية

بالنظر لحيازة المعلومات على ميزان المشروعية يرى الفقه المقارن أننا في عصر التقارير التي تعتبر أداة من أدوات تحصيل البيانات والمعلومات، ولا يقتصر الأمر على شبكة الإنترنت بل على الحواسب الآلية التي تسجل كل دقائق الأمور(٥٥).

وإذا تطرقنا الى التشريع الأمريكي نجد أن جهة الإدارة هناك تحوز رصيدا هائلا من البيانات حول الأفراد لأغراض عامة ومهمة، وعادة ما تكون عملية جمع المعلومات باهظة التكاليف لما تحتويه من صعوبة التجميع أو التكوين، وقد وصفت المحكمة العليا ذلك التأثير كصعوبة عملية أكثر من كونه خصوصية حيث إنه بقدر بساطته يعد أمرا مكلفا وباهظ الثمن(٥٦).

---

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

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

(55) Professor Daniel solovie writes, “We are becoming a society of records, and these records are not held by us, but by third parties”.

See:- Daniel solove, Digital Dossiers ad the Dissipation of fourth Amendment privacy, 75 S. CAL, L. REV. 1083, 1089 (2002).

(56) Fred H. Cate: - Government Data Mining: - The need for a legal framework, Hienonline – 43 Harv. C. R. C.L.L. Rev. 2008., p. 1

For more: see:- Kathleen M. Sullivan, under a watchful Eye:

كما قد يلزم المشرع جهة الإدارة بتدابير معينة يتم النص عليها في القانون كاتخاذ التدابير الوقائية اللازمة أمنيًا لحماية أنظمتها المعلوماتية وشبكاتها والبيانات والمعلومات الإلكترونية الخاصة بها. (٥٧) بل وقد يذهب في صورة أكثر تفصيلاً لإلزام الجهة المختصة باتخاذ االتدابير والإجراءات الكفيلة بالحفاظ على الأدوات والأنظمة المعلوماتية. (٥٨)

وعادة قد يكون جمع الحكومات للبيانات والمعلومات الشخصية حول الأفراد استجابة لظروف معينة تتعلق بالأمن القومي كمخاوف الحكومة الأمريكية من الهجمات الإرهابية(٥٩).

ثانيا-حيازة البيانات الروتينية.

Incursions on personal privacy, in the war on our freedoms: civil liberties in An AGE of TERRORISM 128, 131 (Richard leone & Greg Anrig, Jr. eds, 2003).

(٥٧) نص المشرع القطري في المادة ٢٢ من قانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية (منشور على شبكة المعلومات الدولية على الرابط http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar آخرتحديث ٢٠٢١/١٠/٦) على أن: "تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

١) اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكاتها المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها.

٢) سرعة إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القانون فور اكتشافها أو اكتشاف أي محاولة للالتقاط الاعتراض أو التصنت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات اللازمة لكشف الحقيقة.

٣) الاحتفاظ ببيانات تقنية المعلومات ومعلومات المشترك لمدة لا تقل عن ١٢٠ يومًا وتزويد الجهة المختصة بتلك البيانات.

٤) التعاون مع الجهة المختصة لتنفيذ اختصاصاتها."

(٥٨) نص المشرع القطري في المادة ١٩ من القانون سالف الذكر أنه "على الجهة المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأجهزة أو الأدوات أو وسائل تقنية المعلومات، أو الأنظمة المعلوماتية أو البيانات أو المعلومات الإلكترونية محل التحفظ لحين صدور قرار من الجهات القضائية المعنية بشأنها". ويعد القانون القطري رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية (منشور على شبكة المعلومات الدولية على الرابط http://www.almeezan.qa/LawPage.aspx?id=7121&language=ar آخرتحديث ٢٠٢١/١٠/٦) من التشريعات العربية التي نجحت في إقامة التوازن بين الخصوصية المعلوماتية للأفراد وبين تحقيق الأمن المعلوماتي من خلال منظومة التشريعات التي يعد أبرزها القانون ١٤ لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية.

([59]) federal support for Home land saurity information sharing: Role subcomm. On intelligence Information sharing and Risk Assessment of the H. comm. on Home land security, 109 th cong. 23 (2005) (statement of lee Humilton, vice chairmanm 9/11 public Discourse project).

هناك نوع من البيانات يطلق عليه "البيانات الروتينية" تحصل عليه المؤسسات العامة والخاصة من العملاء يوميًا في قطاعات العمل، والتسوق، والسفر، والاستثمار والدراسة والاتصالات وبالتالي يمكن لجهة الإدارة أن تحصل على تلك البيانات بدون أي قيد دستوري، ولا شك أن طلب جهة الإدارة بالكشف عن بيانات تتعلق بالصحة والأمور المالية، أو الأذواق سيكون من الخصوصية بخلاف أن تطلب الحصول على تلك البيانات لن يكون بدون ضمانة أو تصريح قضائي(٦٠).

لذا يثير جمع البيانات لأغراض الأمن القومي العديد من الإشكاليات لوقوعها على تخوم العلاقة بين الفرد (وحقه في الخصوصية) والدولة (وحقها في الأمن القومي)، "فقد طالبت الحكومة الأمريكية المؤسسات المالية بتقارير بيانات واسعة المدى في إطار جهودها في محاربة الإرهاب وذلك من خلال تعديل قانون سرية البنوك The Bank secrecy act في ٢٠٠١ بل طالبت الحكومة بموجب قانون "الباتريوت" "A PATRIOT act" المؤسسات المالية أن تمدها بتقارير حول الصفقات المؤكدة التي قد تفيد في المسائل الجنائية والاستخباراتية والضريبية وفي مجال محاربة الإرهاب، بل وتعدى ذلك إلزام الأفراد المتعاملين مع البنوك بملء تقارير النشاطات المشتبه بها "suspiciais Activity Reports" وتقارير تحويل العملة "Currency Transaction Reports" (٦١).

ثالثا-الآليات المعتادة لرصد وحيازة البيانات والمعلومات

بالنظر للآليات المعتادة لرصد وحيازة البيانات والمعلومات تعمد جهة الإدارة إلى اللجوء إلى آليات أمنية لرصد بعض المخاطر على شبكات التواصل الاجتماعي وقد ذهبت محكمة القضاء الإداري المصرية (الدائرة الثامنة) إلى إقرار تلك الآليات كونها اجراءات ضبط اداري تمكن وزارة الداخلية من القيام بدورها المنوط بها، واعتبرت أن قيام جهة الإدارة بإنشاء تلك الآلية يعد من قبيل الرقابة والتنظيم وليس التقييد. (٦٢)

---

(60) H. cate, op. cit., p. 26.

يلاحظ أن أغلب البيانات والمعلومات التي تحصل عليها الإدارة يتم من خلال طرف ثالث -غالبًا يكون قطاعاً خاصاً – ويتم تجميع تلك البيانات عن طريق ذلك الطرف لأغراض إدارية.

(61) Fred H. Cate, op. cit., p. 11

:The USA PAIRIOT act also mandates new rules requiring all financial institutins to: (1) verify the Identity of any person seeking to open an account, (2) maintain records of the information used to verify the person's identity and (3) provide the information to the government of matching with terrorist watch lists".

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

"...فكل من الدستور والقانون قد أوجب على وزارة الداخلية الحفاظ على النظام العام والأمن العام والأرواح والأعراض والأموال ومنع الجرائم وضبطها والبرنامج ليس إلا وسيلة لتمكين وزارة الداخلية من

لذلك تتعدد آليات الإدارة فى رصد المخاطر المعلوماتية لكننا سنقتصر على أهم آليتين وهما كالتالى:

أولا: نظام الأرشفة الإلكترونية:

يعد نظام الأرشفة الإلكترونية أحد أقدم الوسائل التقليدية لحفظ الأمن المعلوماتي ،ويرى البعض امكانية تفعيله كالتالي:-

١) تشكيل لجان حكومية في كل إدارة لدراسة أفضل طرق حفظ الوثائق المعلومات.

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

٣) استخدم دعامات إلكترونية لضمان الحصول على البيانات الإلكترونية في حالة فشل تشغيل أي من الدعامات الأخرى والعمل على القيام بعملية تحويل يومي back up خارج جهاز الحاسوب. (٦٣)

ثانيا: الاستشعار عن بعد:

يعد الاستشعار عن بعد من أدوات جهة الإدارة في استخلاص البيانات ، ويمكن تعريفه بأنه طريقة للحصول على معلومات عن شيء ما من مسافة بعيدة، ويستخدم هذا التعبير في الوقت الحاضر لوصف الطرق التي تُجمع بها البيانات عن الأهداف أو الظواهر الطبيعية ".(٦٤)

رابعا-اشكاليات حيازة جهة الإدارة للمعلومات وطرق حلها.

على صعيد اشكاليات حيازة جهة الإدارة للمعلومات وطرق حلها نجد أنه قد تثير حيازة جهة الإدارة للمعلومات الشخصية -خاصة الواردة من أطراف ثالثة- إشكاليتين، الأولى: الكفاءة "efficacy" بمعنى هل تضمن عملية حيازة تلك المعلومات المصادر المالية والبشرية التي تتطلبها؟ والثانية: التأثير "Impact" بمعنى هل يؤدي احتكار القطاع الخاص للمعلومات لإثارة المخاوف لدى جهة الإدارة حول سلوك مضر بالأفراد أو بطريقة أو بأخرى(٦٥).

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...".

(٦٣)د/ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية -رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١ ص١٨١، ١٨٢.

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

(65) 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".

For more:

لذا يمكن تلخيص عنصر الكفاءة في البنود الآتية:-
البند الأول: جودة البيانات Data Quality
في محاولة لتقييم مصطلح حيازة المعلومات لحماية الأمن القومي، قام المركز البحثي التابع للكونجرس (CRS) بتعريفه على أنه مسألة متعددة الوجوه ويشكل ذلك التحدي الأبرز في حيازة المعلومات. (٦٦)
وتتأتى الإشكالية الأكبر في بند جودة المعلومة كما ذكر في مجلة "computer world" في ٢٠٠٣ من أن "بياناً واحداً من معلومة سيئة" يعد إشكالية بديهية ، ولكن إذا زادت أجزاء البيانات السيئة لنحو آلاف أو ملايين الأخطاء فإن ذلك سيؤدي لمعلومات غير متناسقة تؤدي إلى الفوضى(٦٧).
البند الثاني :تناسق البيانات "Data matching"
تواجه جهة الإدارة العديد من الأخطاء في حيازة المعلومات(٦٨) ومنها تناسق البيانات، وقد يستعان في الولايات المتحدة الأمريكية للتغلب على تلك الأخطاء برقم الضمان الاجتماعي

-Tommy Peters on, Data scrubbing, computer world, Feb. 10, 2003, at 32.

(٦٦) 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".

([67]) 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"

(٦٨) مثال تلك الأخطاء كالآتي (طريقة كتابة الأسماء، تغيير النساء لأسمائهن خاصة بعد الزواج، العديد من الأشخاص لهم نفس الأسماء، العديد من الأشخاص يشتركون في نفس العنوان سواء عمل أو مسكن أو صندوق بريدي.
في اعتقادنا أن اللجنة الوطنية لأمن المعلومات في دولة قطر من الجهات التي تتولى مهمة التناسق في البيانات حيث تم النص على تلك اللجنة بموجب القرار الأميري رقم (١٩) لسنة ٢٠١٦ بإنشاء اللجنة الوطنية لأمن المعلومات (منشور على شبكة المعلومات الدولية على الرابط http://www.almeezan.qa/LawPage.aspx?id=6920&language=ar آخرتحديث ٢٠٢١/١٠/٦)حيث نصت المادة ٣ من القرار"تهدف اللجنة إلى تعزيز أمن المعلومات في الدولة بما يحقق خطط التنمية الشاملة في جميع المجالات، وذلك من خلال التوجيه الاستراتيجي للجهود الوطنية اللازمة لتنفيذ الأهداف المحددة في الاستراتيجية الوطنية لأمن المعلومات، وتحقيق التعاون مع الجهات المختصة أو المعنية في هذا المجال."
ونصت المادة ٤ من القرار"للجنة في سبيل تحقيق أهدافها، ممارسة جميع الاختصاصات والصلاحيات اللازمة لذلك، وبوجه خاص ما يلي:

"social security Numbers" وقد واجهت الإدارة في الولايات المتحدة نفس الإشكالية خاصة عند مواجهة الإرهاب.(٦٩) ويكون ذلك لكي يتم تعريف الأفراد القادمين لحدود الدولة وتقدير مدى الخطر الذي يحوم حولهم من خلال المعلومات الدقيقة عنهم،

البند الثالث: حيازة أدوات حيازة المعلومات Data Mining Tools

تواجه مسألة حيازة المعلومات بغرض الحفاظ على الأمن القومي تحديات أكبر من مسألة حيازتها بغرض الأهداف التجارية للعديد من الأسباب، علاوة على ذلك غالبًا ما يعمد مخترقو الأمن المعلوماتى لتضليل جهة الإدارة مقارنة بالقطاع الخاص "Government data mining often is searching for needle not in a haystach, but among millions of other needles.

ومع ذلك تعد المعلومات الواردة من القطاع الخاص مفتاحًا مهمًا للأمن القومي من خلال توقع المسئولين عن الأمن القومي للسلوك المعتاد لعملاء القطاع الخاص(٧٠).

١- اعتماد الاستراتيجية الوطنية لأمن المعلومات، والإشراف على تنفيذها وتحديثها في ضوء ما يستجد من متغيرات، وتنسيق السياسات والأنشطة المتعلقة بالتخطيط الاستراتيجي لمنظومة أمن المعلومات واعتماد الآليات والمعايير الخاصة بها.

٢- التوجيه الاستراتيجي للجهات المعنية بشأن أمن المعلومات في ضوء الاستراتيجية الوطنية لأمن المعلومات، وإنشاء قنوات الاتصال مع المؤسسات الدولية والجهات الخارجية المختصة ووضع أطر التعاون معها ومتابعة التطورات والمستجدات في هذا المجال.

٣- اعتماد خطط إدارة المخاطر المتعلقة بأمن المعلومات وتبادل المعلومات المتعلقة بها."

٤- دعم المشاريع الخاصة بتأمين البنية التحتية المعلوماتية بالدولة.

٥- وضع الآليات التي تكفل التعاون وسرعة تبادل المعلومات بين الجهات المعنية بأمن المعلومات للاستفادة من المعلومات المتوافرة لدى القطاعات المختلفة بالدولة في حماية البنية التحتية للمعلومات من الهجمات الإلكترونية.

٦- توجيه الجهات المعنية لوضع الخطط والبرامج الوطنية للبحوث والتطوير في مجال أمن المعلومات، بالتعاون مع المؤسسات الأكاديمية والبحثية داخل الدولة وخارجها.

٧- دعم مبادرات التعليم والتدريب والتوعية في مجال أمن المعلومات."

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

(70) 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".

لذلك يعد رجال الأمن في الولايات المتحدة أكثر توقعًا للهجمات الإرهابية الخارجية من خلال توقع ضباط الاستخبارات للخطط الإرهابية بناء على النشاط الإرهابي في الماضي بخلاف الهجمات

"Government data mining seems similarly likely to fighting yesterday's battles".[71]

وفي اعتقادنا يمكن حماية النظام العام والأمن القومي من خلال إعداد جهة الإدارة لبرامج واضحة مسبقة تحدد الأهداف التي من أجلها يتم جمع تلك المعلومات مع مراعاة الدقة والنفقات[٧٢].

البند الرابع: تقدير الكفاءة Assessing Efficacy

الإرهابية المحلية تتخذ شكلاً مختلفًا كل مرة في التخطيط والتنفيذ بحيث تكون مواجهتها أقل وفرص كشفها غير متوقعة.

([71]) 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,

([72]) Jones & Harper, op. cit., p.2

One of the bluntest assessments comes from Jeff Jonas, Chief scientist of IBM's Entity Analytic solutions Group, and Jim Harper, director of information policy studies at "the cato institute".

من أدوات التشريع القطري في ذلك اللجنة الوطنية القطرية لتنسيق الطيف الترددي حيث نص قرار وزير الاتصالات وتكنولوجيا المعلومات رقم (٥) لسنة ٢٠١٣ بتشكيل "اللجنة الوطنية القطرية لتنسيق الطيف الترددي(منشور على شبكة المعلومات الدولية على الرابط http://www.almeezan.qa/LawPage.aspx?id=6113&language=a آخرتحديث ٢٠٢١/١٠/٦)وجاء في " المادة ٢منه "تعمل اللجنة الوطنية القطرية لتنسيق الطيف الترددي كلجنة استشارية لتقديم التوصيات بشأن أمور الطيف الترددي في دولة قطر. وتقع المسؤولية النهائية في تنفيذ القرارات على عاتق وزارة الاتصالات وتكنولوجيا المعلومات. وتتمثل الاختصاصات الرئيسية للجنة الوطنية القطرية لتنسيق الطيف الترددي فيما يلي:

١- مناقشة القضايا المحلية والاقليمية والدولية المتعلقة بالاتصالات الراديوية.

٢- تقديم التوصيات بشأن بعض تخصيصات التردد والتي تتعلق بالخطة الوطنية لتخصيص التردد، والقضايا التي تتطلب التنسيق بين مختلف مستخدمي الاتصالات اللاسلكية في البلاد.

٣- إعداد مقترحات للمؤتمرات والاجتماعات الإقليمية أو الدولية وتنسيق كافة الأنشطة المتعلقة بالاتحاد الدولي للاتصالات والطيف الترددي على المستوى الوطني.

٤- إعداد التوصيات لتعزيز الإرشادات الخاصة بالانبعاثات والاشعاعات الكهرومغناطيسية من محطات الاتصالات الراديوية المنصبة على أبراج وصواري الاتصالات.

٥- تقديم التوصيات عند الضرورة للجهات ذات العلاقة فيما يتعلق بمشاركة الابراج وصواري الهوائيات من قبل أكثر من مستخدم للاتصالات اللاسلكية.

٦- تسهيل المناقشات بين مختلف الأطراف عندما يتعذر وصولها إلى اتفاقيات متبادلة.

٧- معالجة القضايا الأخرى التي تتطلب التنسيق بين عدة مستخدمين للطيف الترددي.

ويجوز لوزير الاتصالات وتكنولوجيا المعلومات إضافة اختصاصات إضافية للجنة حسب ما تتطلبه الحاجة لتنفيذ أعمالها"

يذهب الفقه المقارن إلى القول بأهمية تقدير كفاءة نظم حيازة المعلومات، ومن المحاولات الأولى في ذلك ما تتطلبه التشريع الأمريكى عند أية محاولة لحيازة المعلومات من أن يكون هناك إذنًا مكتوبًا من الرئيس الإداري الأعلى للجهة الإدارية حائزة المعلومات(٧٣).

مؤدى ماسبق يرى البعض وجود حرج في مساءلة جهات الإدارة التي تقوم على حيازة البيانات الشخصية للأفراد على اعتبار أن قراراتها غالبًا ما تكون مدروسة وبناء على ضمير مهني(٧٤)، وفى اعتقادنا أن صعوبة إثبات المسئولية الإدارية عن الخطأ فى حيازة الإدارة للمعلومات لاتعنى القول بنفى المسئولية عنها.

خامسا-حيازة الإدارة للمعلومات البيومترية

يمكن أن نتناول في نقطة أخيرة اشكالية حيازة الإدارة للمعلومات البيومترية كونها من مكونات نظم حيازة المعلومات لتفعيل آليات الضبط الإداري،حيث يمكن أن يمتد الأمن المعلوماتي إلى التسجيلات الإلكترونية للمعلومات البيومترية كالحامض النووي DNA ، ووفقا لذلك نص قانون حماية المعلومات لعام ٢٠١٢ الصادر في المملكة المتحدة فى المادة ٢٣ منه على ما يلي: "بالاستناد إلى القسم (٦٣ أ) من لائحة الإثبات الجنائية والشرطية لعام ١٩٨٤ لا بد أن تضم قاعدة البيانات القومية الملفات الشخصية للحامض النووي DNA" وأشارت الفقرة الثانية من المادة على وجوب تسجيل الملفات الشخصية للحامض النووي على قاعدة البيانات القومية"(٧٥).

(73) TECH, AND PRIVACY ADVISORY COMM, U.S. DEPT of DEL Safeguarding privacy in the fight Against terrorism (2004) TAPAC, safeguarding privacy.

(74) Privacy and civil liberties in the Hands of Government post-september 22, 2001: Recommendations of the 9/11 commission and the US. Department of Defense Technology and privacy Advisory committee. Hearing Before the subcomm. On commercial and Administrative law ad subcomm-on the constitution of the H. comm. On the Judiciary, 108th cong. 5(2004) (Statement of John O. Marsh, Jr. TAPAC).

(75) Protection of freedoms Act 2012 Chapter 9- United Kingdom, p. 18 clause 23.
وحماية لتلك البيانات الشخصية أشارت المادة ٢٤ من ذات القانون إلى المجلس الخاص باستراتيجيات البيانات القومية للحامض النووي

(National DNA Datebase strategy Board)
وأشارت المواد اللاحقة إلى التزام ذلك المجلس بوضع دليل استرشادي لكيفية تدمير تلك البيانات، بل وأشارت إلى وجوب التزام الرئيس التنفيذي في الشرطة بذلك الدليل الاسترشادي.

أضف إلى ذلك أن القوانين المقارنة تعمل على حفظ الأمن العام كأحد أركان النظام العام في الدولة عن طريق حيازة "المعلومات البيومترية"(٧٦).

(76) "Biometric Information" means information about a person's physical or behavioural characteristics or features which:-

a) is capable of being used in order to establish or verify the identity of the person, and

b) Is obtained or recorded the intention that it be used for purposes of biometric recognition system.

See clause 28, protection of freedoms Act 2012 (C9) part 1- Regulation of biometric data.

وفي اعتقادنا أن تلك المعلومات تتعاظم أهميتها في الآونة الأخيرة خاصة بعد العمليات الإرهابية المتزايدة.

وتجدر الاشارة إلى إختصاصات إدارة الأمن السيبراني بوزارة المواصلات والاتصالات في قطر وفقا للقرار الأميري رقم (٨) لسنة ٢٠١٦ بالهيكل التنظيمي لوزارة المواصلات والاتصالات(منشور على شبكة المعلومات الدولية على الرابط http://www.almeezan.qa/LawPage.aspx?id=6895&language=ar آخرتحديث ٢٠٢١/١٠/٦)بحسب مانصت عليه المادة22

حيث نصت على أن"تختص إدارة الأمن السيبراني بما يلي:

١- وضع استراتيجية وطنية لأمن المعلومات ومتابعة تنفيذها، بالتنسيق مع الجهات المختصة.

٢- وضع السياسات والمعايير لرفع كفاءة وسائل الحماية لأنظمة تشغيل البنية التحتية الوطنية للمعلومات الحيوية في كافة القطاعات، والإجراءات اللازمة لضمان الامتثال لها.

٣- إعداد برامج تدريبية وتوعوية مصاحبة لدعم الجهات المعنية لتطبيق السياسات الموضوعة وذلك بالتنسيق مع الجهات المختصة.

٤- التنسيق مع المنظمات العالمية والأجهزة الحكومية وغير الحكومية والهيئات والجهات المماثلة لضمان أمن البنى التحتية الحيوية وحماية شبكات ونظم المهمات الحيوية وتقييم أدائها وحماية الأنظمة المعلوماتية من الاختراقات والهجمات الإلكترونية.

٥- تطبيق قواعد أمن أنظمة التطبيقات الحيوية، لمنع تسريب أو نشر البيانات السرية، واتخاذ الإجراءات اللازمة لمنع الاختراقات لضمان الاستمرارية في العمل.

٦- وضع ضوابط وإجراءات الاتصال وحفظ أمن المعلومات، وحماية خصوصية البيانات المتداولة عبر الأنظمة والشبكات الإلكترونية ومتابعة تطبيقها والتصديق على التزام الجهات المعنية بها.

٧- اقتراح مشروعات الأدوات التشريعية الخاصة بأمن المعلومات والبنية التحتية للمعلومات الحيوية وإبداء الرأي في المنازعات.

٨- ضع نطاق المراقبة والإنذار المبكر لتفعيل قدرات الاستجابة للحوادث من خلال تطوير وسائل تقنية الرصد الإلكتروني وتطبيقات تحليل البرامج الخبيثة.

٩- اتخاذ الإجراءات اللازمة لتنفيذ إطار الاستجابة لحوادث الفضاء الإلكتروني.

١٠- تحليل المخاطر السيبرانية ودراسة أفضل السبل لتجنبها والقدرة على مواجهة الأزمات السيبرانية بمرونة وتطويرها من خلال المشاركة مع المؤسسات الأكاديمية ومراكز البحث العلمي.

خاتمة للبحث

- لإعتماد الإدارة والمؤسسات العامة والخاصة في الوقت الحالي على نظام الحكومة الإلكترونية، تتبدى الحاجة لتشريع منظم للأمن المعلوماتي يوازن بين اعتبارات الفاعلية من ناحية (تحقيق دور الجهات الادارية في حفظ أمن الفضاء المعلوماتي والشراكة المعلوماتية)،واعتبارات المشروعية بالحفاظ على الحقوق الفردية للأفراد من ناحية أخرى(الحفاظ على الخصوصية كمثال)وتعرضنا بالفحص والدراسة-في ضوء ذلك- لبعض النظم القانونية المقارنة،وخاصة بدول مجلس التعاون الخليجي.

- هنالك العديد من المحددات التي تجعل من تشريع الأمن المعلوماتي عاملا ناجعا يحقق أهدافه يوازن بين اعتبارات الفاعلية والمشروعية كمثال الخصوصية ،وحيازة جهة الادارة للمعلومات وقواعد البيانات ،والشراكة المعلوماتية،ومن المهم دراسة تلك المحددات في العديد من التشريعات المقارنة ،وتوضيح بعض أدوار الجهات الادارية من خلال الضبط الاداري في إعمال ذلك التوازن والحفاظ المشار اليهما.

التوصيات:

١- تعديل التشريعات المعلوماتية العربية عامة وبدول مجلس التعاون الخليجي خاصة بما يؤدي لتفعيل استراتيجيات ادارية أكثر فاعلية تتيح حيازة المعلومات على نحو مشروع وخاصة فيما يتعلق بحيازة البيانات الروتينية والمعلومات البيومترية،واحترام الخصوصية كأحد محددات الضبط التشريعي.

٢- على الجهات الادارية بدول مجلس التعاون الخليجي تحديث الآليات المعتادة لرصد وحيازة البيانات والمعلومات والعمل على حل اشكاليات حيازة جهة الإدارة للمعلومات.

٣- تعديل التشريعات المعلوماتية العربية عامة وبدول مجلس التعاون الخليجي خاصة بما يساهم في ضرورة التعاون الدولي لتوفير الحلول التنسيق بين العديد من القطاعات على مستوى التشريع القانوني والرقابي.

١١- وضع المعايير والآليات لفحص واعتماد أجهزة الاتصالات وتكنولوجيا المعلومات لضمان خلوها من آليات تسريب قبل تركيبها واستخدامها على شبكات الاتصال الحيوية مثل الشبكات الوطنية.

١٢- وضع آليات تنظيم عمل مزوّدي خدمات التصديق الإلكتروني ووضع آليات العمل اللازمة لتقديم خدماتهم بجودة.

١٣- وضع آليات ضبط التعامل بالهوية الرقمية لتفادي تسرب المعلومات السرية"

المراجع العربية

- المؤلفات العامة والمتخصصة

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

- د/شريف يوسف خاطر: حماية الحق في الخصوصية المعلوماتية -دراسة تحليلية لحق الاطلاع على البيانات الشخصية –دراسة مقارنة-دار الفكر والقانون ٢٠١٥.

- منير محمد الجنيهي، ممدوح محمد الجنيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي ٢٠٠٦.

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

- د/ هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ١٩٩٢.

- د/ وليد السيد سليم، ضمانات الخصوصية فى الإنترنت – دار الجامعة الجديدة ٢٠١٢ .

رسائل علمية:

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

- راشد محمد المري: "الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١٣

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

- نشوى رأفت إبراهيم أحمد: حماية الحقوق والحريات الشخصية في مواجهة التقنية الحديثة "البيانات الشخصية، المراسلات والمحداثات الشخصية، الحق في الصورة) رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة ٢٠١٢.

دوريات:

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

- جريدة الشاهد الكويتية الورقية – العدد ٢٧١٦ صدرت الأربعاء ١٣ يوليو ٢٠١٧ الصفحة الثالثة.

-تشريعات:
- القانون القطري رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية. منشور على شبكة المعلومات الدولية على الرابط
http://www.almeezan.qa/LawPage.aspx?id=7121&language=ar
آخرتحديث ٢٠٢١/١٠/٦
- القانون القطري رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية منشور على شبكة المعلومات الدولية على الرابط
http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar
آخرتحديث ٢٠٢١/١٠/٦
- القانون الاتحادي الإماراتي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات منشور على شبكة المعلومات الدولية على الرابط -http://www.gcc legal.org/BrowseLawOption.aspx?country=2&LawID=3168 آخرتحديث ٢٠٢١/١٠/٦
- القانون الكويتي رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية منشور الكويت اليوم العدد ١١٧٢ السنة الستون ٦٩ بتاريخ ٢٠١٤/٢/٢٣.
- قرار وزير الاتصالات وتكنولوجيا المعلومات القطري رقم (٥) لسنة ٢٠١٣ بإنشاء اللجنة الوطنية القطرية لتنسيق الطيف الترددي منشور على شبكة المعلومات الدولية على الرابط
http://www.almeezan.qa/LawPage.aspx?id=6113&language=a
آخرتحديث ٢٠٢١/١٠/٦
- قانون الجزاء العماني رقم ٧ الصادر عام ١٩٧٤ بموجب المرسوم السلطاني رقم ٢٠٠١/٧٢م. منشور على شبكة المعلومات الدولية على الرابط -http://www.gcc legal.org/BrowseLaws.aspx?country=1 آخرتحديث ٢٠٢١/١٠/٦
- القانون الفيدرالي الأمريكي لأمن المعلومات الصادر في عام ٢٠٠٢
- المرسوم الملكي السعودي رقم ١٧ بتاريخ ١٤٢٨/٣/٧هـ بنظام مكافحة جرائم المعلوماتية منشور على شبكة المعلومات الدولية على الرابط
www.mof.gov.sa/docslibrary/RegulationsInstructions/Documents
آخرتحديث ٢٠٢١/١٠/٦
- قانون تنظيم الاتصالات العماني رقم ٣٠ لسنة ٢٠٠٣ منشور على شبكة المعلومات الدولية على الرابط http://www.gcc-legal.org/BrowseLaws.aspx?country=1 -
آخرتحديث ٢٠٢١/١٠/٦

- القانون العماني رقم ٢٠١١/١٢ الخاص بمكافحة جرائم تقنية المعلومات منشور على شبكة المعلومات الدولية على الرابط -http://www.gcc-legal.org/BrowseLaws.aspx?country=1 آخرتحديث ٢٠٢١/١٠/٦
- القانون الكويتي رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات -الكويت اليوم العدد ١٢٤٤ السنة الحادية والستون منشور بتاريخ ٢٠١٥/٧/١٢.
- القرار الأميري القطري رقم (١٩) لسنة ٢٠١٦ بإنشاء اللجنة الوطنية لأمن المعلومات منشور على شبكة المعلومات الدولية على الرابط
http://www.almeezan.qa/LawPage.aspx?id=6920&language=ar
آخرتحديث ٢٠٢١/١٠/٦
- القرار الأميري القطري رقم (٨) لسنة ٢٠١٦ بالهيكل التنظيمي لوزارة المواصلات والاتصالات منشور على شبكة المعلومات الدولية على الرابط
http://www.almeezan.qa/LawPage.aspx?id=6895&language=ar
آخرتحديث ٢٠٢١/١٠/٦

أحكام قضائية:

- حكم محكمة القضاء الإداري المصرية – الدائرة الثامنة عقود في الدعوى رقم ٦٣٠٥٥ لسنة ٦٨ ق بتاريخ أغسطس ٢٠١٥ (حكم غير منشور).
- الطعن رقم ١٠١٧١ لسنة ٥٤ ق. عليا المحكمة الإدارية العليا المصرية – الدائرة الثانية - حكم غير منشور.

مؤتمرات:

- المؤتمر السنوي الثالث لأمن المعلومات المنعقد بالدوحة في نوفمبر ٢٠١٦

المراجع الأجنبية:

-Abraham D. Safaer, National security and leaks, the Government's Autority to Discipline itself. International studies in Human Rights volume 16,.

- Amanda N. Craigetal. Proactive cybersecurity: 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
- Daniel solove, Digital Dossiers ad the Dissipation of fourth Amendment privacy, 75 S. CAL, L. REV. 1083, 1089 (2002).
- David weissbrodt, cyber – conflict, cyber – crime, and cyber Espionage, Minnesota Journal of Internatinal. Law's 2013 symposium.
- Fred H. Cate: - Government Data Mining:- The need for a legal framework, Hienonline – 43 Harv. C. R. C.L.L. Rev. 2008-
- Federal support for Home land saurity information sharing: Role subcomm. On intelligence Information sharing and Risk Assessment of the H. comm. on Home land security, 109 th cong. 23 (2005) (statement of lee Humilton, vice chairmanm 9/11 public Discourse project).
-Hector Becerra, Jennifer Oldham & Mitchell landsberg, Airline Terrorism Alert: winging it one Again, L.A. Times, Aug. I1, 2006.
- Jonathan Clough: principles of cybercrime-second edition - Cambridge press 2010.
- Jeff Jonas & Jim Harper, cato institute, Effective counter terrorism and the limited role of predictive Data mining (2006).
- Kathleen M. Sullivan, under a watchful Eye:
Incursions on personal privacy, in the war on our freedoms: civil liberties in An AGE of TERRORISM 128, 131 (Richard leone & Greg Anrig, Jr. eds, 2003).
- Kasperson (W. K. Henrik) computer crimes and other crimes Against Information Technology in U. S. A., R. I. D. P. 2001
- Marietta Benko, and others, space law in the united nations, Martinus Nijhoff, Netherlands, 1985,
- Markle found, Mobilizing information to prevent terrorism protecting America's freedom in the information age(2006);.
- Nathan Alexander sales: Regulating cyper security – Northwestern university law Review 2013 vol., 107, No 4,

- Nathan Alexander sales: Regulating cyper security – Northwestern university law Review 2013 vol., 107
- Office of TECH: Assessment, Electronic Record system anti individual privacy 57 (1986).
- Privacy and civil liberties in the Hands of Government post-september 22, 2001: Recommendations of the 9/11 commission and the US. Department of Defense Technology and privacy Advisory committee.
- Richard Clarke, threats to U.S. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, 12 Depaul Bus, L. J. (1999 – 2000).
- Susan W. Brenner, cyber crime:- criminal threats for cyberspace (2010): Jona than clough, principles of cyber crime (2010).
- The Emergence of cyber security law, prepared for the Indiana University Maurer School of law by Hanover Research, February, 2015.
- TECH, AND PRIVACY ADVISORY COMM, U.S. DEPT of DEL Safeguarding privacy in the fight Against terrorism (2004) TAPAC, safeguarding privacy.
- Tommy Peters on, Data scrubbing, computer world, Feb. 10, 2003.
- Todd A. Brown, legal propriety of protecting Defense Industrial Base Information Infrastructure GAA.F.L.Rev. 2011, 220 (2009)

Legislations:

- The Natioal cybersecurity and infrastructure protection 2013 Act"
- Data Protection Act 1998 Published by TSO, the stationery office – Data pretention & Investigatory powers Act 2014 chapter 27.
- Protection of freedoms Act 2012 Chapter 9- United Kingdom.
- Federal Information security Management Act of 2002 (FISAAA)
- Data security Act 2014(القانون الأمريكي لأمن البيانات لعام ٢٠١٤)

Conferences

- The Cantigny principles on technology terrorism, and privacy, National security law Report, feb. 2005,

- "The Cantigny" conference on counter terrorism technology and privacy organized by the standing committee on law and Nation security of the American Bar Association".