

محددات الضبط التشريعي للأمن المعلوماتي «دراسة مقارنة»

الدكتور/ ياسر محمد عبد السلام رجب *

* مدرس القانون العام - كلية الحقوق - جامعة القاهرة، مستشار قانوني بوزارة التنمية الإدارية والعمل والشؤون الاجتماعية - دولة قطر.



المقدمة

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 الإدارية حزمة قوانين منظمة للأمن المعلوماتي، وأن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقدير المخاطر السيبرية⁽¹⁾.

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⁽²⁾.

ويتهدد الأمن المعلوماتي للإدارة بصورة كبيرة اعتماد الإدارة في الوقت الحالي في إدارتها لمرافقها على نظام الحكومة الإلكترونية، وقد يصل الأمر لانتهاك أمن الدولة الوطني، كالاطلاع على معلومات تمس أمن الدولة، أو الوصول إلى أنظمة التحكم في محطات المفاعلات النووية⁽³⁾.

علاوة على ما تقدم هنالك العديد من المحددات التي تجعل من تشريع الأمن المعلوماتي عاملاً ناجحاً يحقق أهدافه كمثال الخصوصية، وحيازة جهة الإدارة 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".

(2) تمكن المنتهكون الإلكترونيون من سرقة أسماء العملاء، وكلمات المرور المشفرة، وعناوين البريد الإلكتروني، والحسابات الإلكترونية، وبلغ عددها في «ياهو» فقط أكثر من 500 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 أيضاً 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 إشكالية البحث الأساسية حول كيفية إعمال التشريع المنظم للأمن المعلوماتي للتوازن بين اعتبارات الفاعلية من ناحية (تحقيق دور الجهات الإدارية 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

1 - بحث موقف التشريعات من إعمال التوازن بين الاعتبارات المنظمة للأمن المعلوماتي، وترسيخ الحفاظ على الخصوصية المعلوماتية، وتوضيح بعض أدوار الجهات الإدارية من خلال الضبط الإداري في إعمال ذلك التوازن والحفاظ المشار إليهما.

2 - الوقوف على الإشكاليات الناتجة عن حيازة جهة الإدارة للمعلومات وقواعد البيانات كأحد محددات الضبط التشريعي.

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

أهمية البحث

على الصعيد العلمي

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

على الصعيد العملي

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

- تتبدى كذلك أهمية البحث لتعرضه لحيازة جهة الإدارة 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

1 - ندرة المؤلفات الفقهية التي تناولت الأمن المعلوماتي في القانون الإداري؛ خاصة أن الأمن المعلوماتي يقع على تخوم العديد من القوانين كالقانون العام والقانون الخاص، فضلا عن قانون التجارة الدولية، بل وقوعها بين فرعين من العلوم وهما القانون والحاسبات الآلية.

2 - 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 استنباطي بتحليل نصوص القوانين المقارنة بالإضافة لتحليل بعض الفقرات وكذلك عرض الآراء الفقهية. بالإضافة إلى المنهج المقارن

بتناول العديد من القوانين كالقانون الأمريكي والإنجليزي وقوانين دول مجلس التعاون الخليجي كالقانون القطري والكويتي والإماراتي والسعودي والعماني.

خطة البحث

في ضوء ما تقدم سوف تكون معالجة ذلك البحث كالتالي:

المبحث الأول: محددات الضبط التشريعي للأمن المعلوماتي في النظم القانونية المقارنة

المبحث الثاني: الخصوصية كأحد محددات الضبط التشريعي

المبحث الثالث: حيازة جهة الإدارة للمعلومات وقواعد البيانات كأحد محددات الضبط التشريعي

المبحث الرابع: الشراكة المعلوماتية كأحد محددات الضبط التشريعي

المبحث الأول

محددات الضبط التشريعي للأمن المعلوماتي في النظم القانونية المقارنة

تعتمد بعض الأنظمة القانونية على تشريعات أمن معلوماتي فعالة موضوعيا وإجرائيا، على العكس من البعض الآخر يعتمد على قوانين غير فعالة.⁽¹⁾ 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.⁽²⁾

ويرى الفقه المقارن أن المعالجة التشريعية للأمن المعلوماتي تكون بطريقتين: الأولى قوانين التجسس، والثانية قوانين الاتصالات.⁽³⁾ غير أنه تجدر الإشارة إلى أن بعض التشريعات تعاني قصورا تشريعا في الأمن المعلوماتي ويتمثل ذلك القصور التشريعي أحيانا في حادثة الفعل المؤدي 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 تشريعا بموجب النصوص العقابية التقليدية.⁽⁴⁾

(1) 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

(2) تنقسم شخصيات الجناة الإلكترونيين إلى:

(1) المتطفلون: "Hackers" وهم مجموعة من الناس يقصدون التسلية لغرض إثبات قدرتهم على الاختراق أو تحديهم أو لمجرد المزاح.
(2) محبو المال: وهم مبرمجون موهوبون يقومون بالاحتيال لسرقة الأموال من المصارف أو مؤسسات الأعمال.
(3) المحترفون: وهم مجموعة من الناس، يقصدون سرقة معلومات هامة وحساسة وسرية والهدف المقصود – غالبا – لذلك النوع هي الدوائر الحكومية والعسكرية.

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

(4) 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 2016م ص10، 11.

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.⁽¹⁾

علاوة على ماسبق تتعدد تشريعات الأمن المعلوماتي فيما يتعلق بقوانين الكمبيوتر كالتالي:

- 1 - تشريعات حماية برامج الكمبيوتر، وهي تعكس الاتجاهات العالمية «في إدراج الملكية الفكرية ضمن تنظيمات التجارة الدولية نتيجة للاقتصاد الرقمي والاقتصاد المؤسس على المعرفة.
- 2 - تشريعات الأصول الإجرائية الجزائية، وهي في الواقع تطوير لقواعد الإثبات في الإجراءات لكنها تتصل بالحقوق الجديدة المعترف بها في الميدان التقني المعلوماتي.
- 3 - تشريعات المحتوى الضار، وهي تهدف في المقام الأول للحماية من محتوى المعلوماتية على الأمانة.

(1) نص المشرع القطري في القانون رقم 14 لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar>

(آخر تحديث 2018/10/6)

في المادة 2 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 22 على أن: «تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

- 1 - اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكتها المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها.
- 2 - سرعة إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القانون فور اكتشافها أو اكتشاف أي محاولة للاتقاط أو الاعتراض أو التنصت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات اللازمة لكشف الحقيقة.
- 3 - الاحتفاظ ببيانات تقنية المعلومات ومعلومات المشترك لمدة لا تقل عن (120) يوما، وتزويد الجهة المختصة بتلك البيانات.
- 4 - التعاون مع الجهة المختصة لتنفيذ اختصاصاتها».

ونص المشرع الإماراتي كمثل في المادة 22 من القانون الاتحادي الإماراتي لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.gcc-legal.org/BrowseLawOption.aspx?country=2&LawID=3168>

(آخر تحديث 2018/10/6)

على أن: «يعاقب بالسجن كل من دخل بغير وجه حق موقعا أو نظاما 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».

4 - تشريعات معايير الأمن المعلوماتي، وهي تهدف إلى تبادل البيانات والتشفير ويستهدف البعض دراستها ضمن محتوى التجارة الإلكترونية⁽¹⁾.

والجدير بالذكر أن المشرع القطري قد انتهج في القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية سبيلين مختلفين لحماية الأمن المعلوماتي وذلك من خلال تبنيه لمنهج استثناء بعض البيانات الشخصية من الحماية التشريعية المعلوماتية إذا ارتبطت بالنظام العام، كمثال مانصت عليه المادة 18 من الفصل الخامس (الإعفاءات) 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:

1 - حماية الأمن الوطني والأمن العام.

2 - حماية العلاقات الدولية للدولة.

3 - حماية المصالح الاقتصادية أو المالية للدولة.

4 - 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 إسباغ مزيد من الحماية التشريعية لبعض البيانات مثال ما نصت عليه المادة 16

(1) هناك العديد من تشريعات الأمن المعلوماتي على مستوى العالم، نذكر منها على سبيل المثال في الولايات المتحدة الأمريكية قانون خصوصية الاتصالات الإلكترونية لعام 1986، وقانون خصوصية الاتصالات لعام 1997، وقانون خصوصية المعطيات لعام 1997، أما في ألمانيا نجد قانون حماية المعطيات ومشروع قانون حماية البيانات عام 2000 المتوافق مع القانون الأوروبي لعام 1995، وفي فرنسا قانون معالجة الآلية للمعطيات والمعدل في عام 2000، وفي النرويج قانون تسجيل البيانات الشخصية لعام 2000، وفي بلجيكا قانون حماية الحياة الخاصة فيما يتعلق بالتعامل مع المعطيات الشخصية المعدل عام 2000، وفي هذا قانون حماية البيانات الشخصية والوثائق الإلكترونية لعام 2000، وفي بريطانيا قانون حماية المعطيات لعام 1984 وقانون حماية البيانات لعام 1998 المعدل لقانون 1984، وقانون حرية المعلومات لعام 2000، وفي اليابان قانون حماية المعلومات في الشخصية رقم 95 الصادر في 1998/12/16، وفي التشيك قانون حماية البيانات الشخصية في نظم المعلومات لعام 1992 وقانون حماية البيانات لعام 2000، وفي هنغاريا قانون حماية البيانات الشخصية ونشر البيانات للمصالح العامة لعام 1992، وفي رومانيا قانون حماية البيانات لعام 1992، وفي كوريا الجنوبية قانون حرية المعلومات لعام 1996، وفي روسيا قانون حماية المعلومات لعام 1995، وفي إيطاليا قانون حماية البيانات لعام 1996، وفي ليتوانيا قانون الحماية القانونية للبيانات الشخصية لعام 1996، وفي الصين نظم حماية وإدارة الشبكات لعام 1997، وفي تايلاند قانون حماية البيانات في القطاع العام لعام 1998، وفي الهند مشروع قانون حماية البيانات الموصى بإصداره من الفريق الوطني لتقنية المعلومات وتطوير البرمجيات، وفي جنوب أفريقيا قانون الوصول إلى المعلومات لعام 2000، وفي تركيا مشروع قانون حماية البيانات الشخصية لعام 2000.

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 بتحديدتها قرار من الوزير. وللوزير 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 standards، وثانيهما التشريعات والرقابة Legislation and Monitoring، ونتناولهما كالتالي:⁽¹⁾

1 - المعايير الفنية

تم إنشاء المعهد القومي للمعايير القياسية والتكنولوجيا كباكورة أولية في عام 1901 تتبع وزارة التجارة الأمريكية، علاوة على وحدة المعلومات التابعة لمعمل تكنولوجيا المعلومات؛ حيث تضع سياسات ومعايير تبادل المعلومات.⁽²⁾ ومن أهم اللجان لجنة الحاسب والاتصالات التابعة للمجلس القومي للبحوث، وترجع أهمية تلك اللجنة إلى أنها تشفر المعلومات والبيانات «cryptography»⁽³⁾.

(1) انظر للمزيد د/ راشد محمد المري: رسالة دكتوراه بعنوان «الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر»، رسالة مقدمة لكلية الحقوق جامعة القاهرة 2013، ص 182.

وانظر أيضاً: 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 2015، وقد أثرتنا عدم التطرق لتلك التجربة كي نلقي الضوء على تجارب أخرى لم تطرقها طرق البحث.

(2) يقوم ذلك المعهد بإصدار القواعد والمعايير الفنية لتصنيف نظم المعلومات على أنها نظم قومية من وجهة نظر أمن المعلومات انظر: د/ راشد محمد المري، الجرائم الإلكترونية مرجع سابق ص 182.

(3) راجع:

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

مشار إليه د/ راشد محمد المري، الجرائم الإلكترونية مرجع سابق ص 182.

2 - 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 1966، ويأتي القانون الفيدرالي لأمن المعلومات الصادر في عام 2002 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⁽¹⁾ ويوفر القانون الفيدرالي لأمن المعلومات الصادر في عام 2002 إطاراً لتأكيد فعالية السيطرة الإدارية على مصادر المعلومات بما فيها حماية المعلومات الفيدرالية ونظم المعلومات مع تحديد اختصاصات كل رئيس وكالة فيدرالية⁽²⁾، أما على صعيد الرقابة تم إنشاء فريق الاستعداد في عام 2003 كجزء رئيس من وحدة الأمن القومي الافتراضي (National cyper security Division)⁽³⁾.

علاوة على ماسبق كان الفقه القانوني الأمريكي يرى أن الكونجرس عليه أن يقوم برسم استراتيجية

(1) وإذا كان غرض قانون حرية المعلومات في عام 1966 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) (EFIA) (freedom of Information Act) لتعزيز الأمن المعلوماتي؛ حيث يطالب جميع جهات الإدارة (بأتمتة الملفات)؛ أي جعل الملفات الورقية في صورة إلكترونية وإعداد فهرس خاصة لإطلاع المواطنين عليها. لمزيد من الإيضاح انظر: د/ راشد محمد المري، المرجع السابق ص183. وتتخلص 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. (2) «على كل رئيس وكالة فيدرالية»:

- (1) تقييم المخاطر واتجاهات الضرر الذي قد يحدث من عمليات الوصول والاستخدام والإفصاح والتوزيع والتعديل والتدمير غير المرخص به للمعلومات أو لنظم المعلومات.
 - (2) تحديد مستويات أمن المعلومات المناسبة لحماية كل المعلومات ونظم المعلومات بوكالته.
 - (3) تنفيذ السياسات والإجراءات التي تقلل المخاطر لأدنى حد ممكن.
 - (4) القيام باختبارات دورية وتقييم لأدوات أمن المعلومات.
- ويهدف القانون الفيدرالي لأمن المعلومات الصادر في عام 2002 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.
- ثانياً: السلامة، منع دخول معلومات غير صحيحة أو إتلاف المعلومات.
- ثالثاً: التوفر (الإتاحة)، ضمان الوصول الفوري والموثوق به للمعلومات واستخدامها.
- (3) 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 الاختراقات المحتملة.

واضحة⁽¹⁾ لدور جهة الإدارة في تعزيز الأمن المعلوماتي من خلال الضبط الإداري ويرتكز ذلك على إصلاح قانون إدارة أمن المعلومات الاتحادية لعام 2002.

Federal Information security Management Act of 2002 (FISAAA)

والعديد من المحاور الهامة الأخرى.⁽²⁾

أضف إلى ما سبق، تقوم النظم القانونية الأوروبية بتغليب الأمن المعلوماتي في حالة تهديد الأمن العام⁽³⁾.

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

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

ومن تلك المحاور التي أوردتها الفقه القانوني الأمريكي:

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

(2) تبادل المعلومات والتنسيق بين القطاعات.

(3) مراعاة انتهاكات السرقة أو التعرض للبيانات الشخصية كالمعلومات المالية.

(4) مراعاة السياسة العقابية لجرائم الإنترنت.

(5) مراعاة الخصوصية في مجال التجارة الإلكترونية.

(6) الجهود الدولية في الأمن المعلوماتي.

(7) البحث والتطوير.

(8) تطوير القوى العاملة في مجال الأمن السيبري.

والجدير بالذكر أن هناك عدة تشريعات تم إدخالها إلى الكونجرس مؤخرا تمس الأمن السيبري، ومن تلك القوانين قانون خصوصية المعلومات الشخصية وأمنها لعام 2014، من شأن ذلك القانون حفاظ الشركات على المعلومات الاستهلاكية في مأمن من قرصنة الكمبيوتر.

وهناك أيضا قانون أمن البيانات لعام 2014 (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.

وثالثا هناك القانون الوطني للأمن السيبراني وحماية البنية التحتية الحيوية لعام 2013.

“The Natioal cybersecurity and infrastructure protection 2013 Act”.

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

(3) د/ نشوى رأفت إبراهيم أحمد، مرجع سابق ص277.

كمثال، ما نصت عليه المادة الثالثة من القانون الفرنسي الصادر في 10 يوليو 1991 على الأسباب القانونية التي يمكن الاستناد إليها لإجراء المراقبة أو التنصت الإداري والتي جاء فيها: (يجوز الإذن أو التصريح ... بالتنصت الذي يكون موضوعه أو محله البحث عن المعلومات التي تهتم الأمن القومي، المحافظة على المصالح الاقتصادية والعلمية للمجتمع الفرنسي، منع الإرهاب والمجموعات الإجرامية المنظمة وكذلك منع تكوين أو إعادة تكوين المجموعات التي تم حلها وفقا لقانون 10 يناير 1963).

واشترطت المادة الرابعة من القانون أن يتم الإذن بالمراقبة بإذن مكتوب ومسبب يصدر من رئيس الوزراء أو من يقوم بتفويضه تفويضا خاصا، 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 للمراقبة.

انظر بالتفصيل: ص 278 من المرجع السابق فيما يخص اللجنة القومية للمراقبة وتشكيلها وآليات عملها.

التجربة الخليجية في تعزيز الأمن المعلوماتي

بمقارنة الوضع التشريعي الخليجي في مجال الأمن المعلوماتي نجد أنه يساير تعزيز الأمن المعلوماتي؛ حيث كانت عمان صاحبة السبق في ذلك⁽¹⁾، ثم تلتها الإمارات العربية المتحدة.⁽²⁾

حيث إن سلطنة عمان من الدول السابقة في الحفاظ على أمنها المعلوماتي من خلال قطاع الاتصالات؛ حيث تم إقرار قانون الاتصالات رقم 30 لسنة 2003 لتعزيز بيئة معلوماتية آمنة للقطاع الاستثماري.⁽³⁾ وذهبت المادة 61 من هذا التشريع إلى العقاب بالسجن مدة لا تزيد على سنة، وبغرامة لا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين للعديد من الأفعال.⁽⁴⁾

(1) تم ذلك من خلال تعديل قانون الجزاء العماني رقم 7 والذي صدر عام 1974 بموجب المرسوم السلطاني رقم 2001/72م، والجدير بالذكر صدور قانون الجزاء العماني بموجب المرسوم السلطاني رقم 7 لسنة 2018 باصدار قانون الجزاء العماني- الجريدة الرسمية التي تصدرها وزارة الشؤون القانونية بسلطنة عمان - السنة السابعة والأربعون بتاريخ 14 يناير 2018، مرددا ذات الأحكام في الباب الأول من الكتاب الثاني.

(2) تعد الإمارات العربية المتحدة أول دولة عربية تصدر قانونا مختصا في مكافحة جرائم المعلومات وذلك بموجب القانون الاتحادي رقم (2) لسنة 2006.

أما المملكة العربية السعودية عززت أمنها المعلوماتي بالمرسوم الملكي رقم 17 بتاريخ 1428/3/7هـ بنظام مكافحة جرائم المعلوماتية، منشور على شبكة المعلومات الدولية على الرابط:

www.mof.gov.sa/docslibrary/RegulationsInstructions/Documents

(آخر تحديث 2018/10/6)

من خلال وضع آلية نظامية للحد من انتهاك الأمن المعلوماتي كي تتحقق استخدامات الحاسب بزيادة تحفظ الحقوق المترتبة على الاستخدام المشروع للحسابات والشبكات وحماية النظام العام الخلقي (الأخلاق والآداب العامة).

(3) د/ حسين بن سعيد الغافري، مرجع سابق ص65.

في إشارة إلى العقيد/ محسن بن علوي آل حفيظ: موجز عن قانون تنظيم الاتصالات 30 لسنة 2002 - النودة التعريفية بأحكام قانون الاتصالات - مسقط 2009.

"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 2002 للعديد من التعديلات آخرها 2008.

(4) 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 ينته الأمر عند هذا الحد، بل جاء المشرع العماني بقانون مكافحة جرائم تقنية المعلومات رقم 12 لسنة 2011، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.gcc-legal.org/BrowseLaws.aspx?country=1->

(آخر تحديث 2018/10/6)

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 2008 وتم الانتهاء من إعداد المسودة الأولى منه في الربع الثالث من 2009 وإحالتها للجهات

وقد احتوى التشريع العماني على العديد من المصطلحات التي تركز على أمن الفضاء المعلوماتي⁽¹⁾. 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.⁽²⁾

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⁽³⁾، وهناك العديد من النصوص التي لا يتسع المقام لذكرها حافظت على النظام العام العماني وأمن الفضاء المعلوماتي هناك من خلال تجريم

المختصة لإبداء ملاحظاتها عليه، ثم صدر في الربع الأول من 2011 بموجب المرسوم السلطاني 2011/12، وانقسم القانون إلى 30 مادة موزعة على 6 فصول.

(1) 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 ب وحدات الجهاز الإداري للدولة.
الشبكة المعلوماتية: ارتباط أكثر من وسيلة لتقنية المعلومات للحصول على البيانات والمعلومات الإلكترونية وبناء لها.
الالتقاط: مشاهدة البيانات والمعلومات الإلكترونية أو الحصول عليها.

(2) 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 عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك، وتكون العقوبة السجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة 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».

(3) وشددت 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 إلى ألف ريال عماني، والحد الأقصى إلى ثلاثة آلاف ريال عماني في حالة إذا ما تم ارتكاب الجرائم الواردة في المادة الثالثة أثناء أو بمناسبة تأدية العمل. بل وإمعانا في الحماية غلظت المادة الرابعة العقوبة على المتعاملين مع الفضاء المعلوماتي لافتراض الثقة في أشخاصهم، خاصة إذا كانوا في اعتقادنا من موظفي جهة الإدارة.

الجرائم الإلكترونية للإتجار في البشر⁽¹⁾، والجرائم الإلكترونية لغسل الأموال⁽²⁾، والجرائم الإلكترونية للإتجار في الأعضاء البشرية⁽³⁾، والجرائم الإلكترونية لتجارة الأسلحة⁽⁴⁾، والجرائم الإلكترونية لتجارة المخدرات⁽⁵⁾، والجرائم الإلكترونية لانتهاك الملكية الفكرية⁽⁶⁾، والجرائم الإلكترونية لتجارة الآثار⁽⁷⁾.

وكما أسلفنا بأن الإمارات العربية المتحدة تعد أول دولة عربية تصدر قانوناً مختصاً في مكافحة جرائم المعلومات وذلك بموجب القانون الاتحادي رقم (2) لسنة 2006؛ حيث كان لصدور قانوني التوقيع الإلكتروني في 2002، وقانون التجارة الإلكترونية صدى واسع 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 2006، وقد تضمن الحفاظ على النظام العام المعلوماتي بكافة عناصره سواء النظام العام العادي أو الأخلاقي وهو ما يتأكد في المادة 20 من القانون، ومن ناحية أخرى عمد المشرع الكويتي في القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات إلى السير على درب المشرع الإماراتي في تقسيم مسارات تعزيز الضبط التشريعي للأمن المعلوماتي⁽⁸⁾.

(1) انظر: المادة 22 من قانون 12/ لسنة 2011 العماني.

أما المادة الثامنة من قانون 2011/12 العماني الخاص بمكافحة جرائم تقنية المعلومات جرمت الاعتراض العمدي ودون وجه حق لاستخدام وسائل تقنية المعلومات من خلال خط سير البيانات أو المعلومات الإلكترونية المرسله عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو التنصت عليها.

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

وتطرقت المادة التاسعة عشرة 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 العشرون 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.

(2) انظر: المادة 21 من قانون 12/ لسنة 2011 العماني.

(3) انظر: المادة 23 من قانون 12/ لسنة 2011 العماني.

(4) انظر: المادة 24 من قانون 12/ لسنة 2011 العماني.

(5) انظر: المادة 25 من قانون 12/ لسنة 2011 العماني.

(6) انظر: المادة 26 من قانون 12/ لسنة 2011 العماني.

(7) انظر: المادة 27 من قانون 12/ لسنة 2011 العماني.

(8) انظر تفصيلاً: قانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات - الكويت اليوم العدد 1244، السنة الحادية والستون، منشور بتاريخ 2015/7/12.

ومن الجرائم الإضرار بالأمن العام المعلوماتي خاصة، والأمن العام بصفة عامة عن طريق تجارة الرقيق الأبيض والمخدرات (المادة 8 من القانون)، وكذلك (المادة 4 من القانون)، والإضرار بالأمن العام عن طريق التهديدات الإرهابية الإلكترونية (المادة 10 من القانون).

وفى اعتقادنا أنه يجب الاعتماد على تقسيمات النظام العام بشقيه المادي والأخلاقي عند تحديد الأطر الحاكمة للضبط التشريعي، ويؤكد على رأينا تبني عدة تشريعات عربية لذلك عند تقسيم مسارات أوجه الإخلال بالأمن المعلوماتي كمثال ما جاء به القانون الكويتي رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات وذلك كالتالي⁽¹⁾:

- (1) انظر تفصيلاً: المرجع السابق، قانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات.
- حيث بررت 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.
- أ (تغليظ العقاب على تزوير مستندات رسمية أو بنكية أو بيانات حكومية أو بنكية إلكترونية (المادة 3 فقرة 2)، 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 3 فقرة 1)، وهو ما يتعلق بالأمن المعلوماتي لجهة الإدارة بمفهوم أشد تركيزاً.
- ب (الإضرار بالقطاع الطبي (المادة 3 فقرة 3)، وهو ما يتعلق بالنظام العام وخاصة في أحد عناصره وهو الصحة العامة.
- ج (الإضرار بالآداب العامة والأخلاق (المادة 3 فقرة 4) وهو ما يتعلق بالنظام العام الأخلاقي.
- والجدير بالذكر أن المشرع القطري قد عمد في القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية لحماية النظام العام الخلقي كما نص في المادة 17 بأنه: «مع مراعاة الالتزامات المنصوص عليها في هذا القانون، يجب على مالك أو مشغل أي موقع إلكتروني موجه للأطفال، مراعاة ما يلي:
- 1 - وضع إخطار على الموقع حول ماهية بيانات الأطفال، وكيفية استخدامها، والسياسات التي يتبعها في الإفصاح عنها.
 - 2 - الحصول على موافقة صريحة من ولي أمر الطفل الذي تتم معالجة بيانات شخصية عنه، وذلك عن طريق اتصال إلكتروني أو أي وسيلة أخرى مناسبة.
 - 3 - تزويد ولي أمر الطفل، بناء 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.
 - 4 - حذف أو محو أو وقف معالجة أية بيانات شخصية تم جمعها من الطفل أو عنه، إذا طلب ولي الأمر ذلك.
 - 5 - 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»
- د (الإضرار بالأمن العام المعلوماتي خاصة، والأمن العام بصفة عامة عن طريق تجارة الرقيق الأبيض والمخدرات (المادة 8 من القانون) وكذلك (المادة 4 من القانون)، والتهديدات الإرهابية الإلكترونية (المادة 10 من القانون).

المبحث الثاني

الخصوصية كأحد محددات الضبط التشريعي

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:

1 - 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 قانوناً.

2 - 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 استناداً لرضائهم المفترض عن سياسة الرقابة الخاصة بمصلحة المشروع⁽¹⁾.

وتتعلق السرية الإلكترونية للأفراد بمدى وجود بنوك معلومات وبيانات، وتثور إشكالية بنوك المعلومات والبيانات على صعيدين أولهما: كمي، والثاني: كيفي.⁽²⁾ 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 ضرراً بالغاً بالآخرين أو المجتمع ككل.⁽³⁾ فقد قررت المادة 28 من قانون حماية البيانات لعام 1998 في

(1) د/ أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق، جامعة المنصورة، سنة 2006، ص488.

(2) د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة 1992، ص80. 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.

(3) عمر محمد سلامة العليوي، حق الحصول على المعلومات في ضوء القانون الأردني رقم 47 لسنة 2007 - دراسة مقارنة - رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، سنة 2011، ص181.

المملكة المتحدة استثناء حماية المعلومات الشخصية من الحماية في الخصوصية طالما تعلق الأمر بأغراض حماية الأمن القومي⁽¹⁾.

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 قانوناً 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⁽²⁾.

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 الأمريكي يرى الفقه أن حماية الخصوصية تؤدي غالباً إلى تعزيز الأمن المعلوماتي، وذلك من خلال تقنين الإدارة لأنشطتها في حيازة المعلومات، أو على الأقل تبرير قيامها بنشاط تجميع البيانات والمعلومات على مستوى المسؤولين الأعلى، أو من خلال لجنة من الكونجرس أو قضاة فيدراليين أو بمتطلبات الإذن القضائي أو أية إجراءات لحماية الخصوصية وجهود الأمن القومي⁽³⁾.

عامة تكمن الإشكالية في عدم وضوح الرؤية قانوناً عن المدى الذي يمكن أن يمد القطاع الخاص الحكومة بالبيانات الهائلة، وإلى أي مدى يمكن أن تقلق الإدارة من البرامج الخاصة بحيازة المعلومات والبيانات لدى القطاع الخاص⁽⁴⁾. علاوة على ما سبق يمكن التخلي عن فكرة الخصوصية المعلوماتية إذا تعلق الأمر بالنظام العام للدولة وفقاً لقانون الأمن ومكافحة الإرهاب والجريمة 2001 في المملكة المتحدة (الفصل 24)؛ حيث نصت الفقرة الثانية من المادة 17 على أن تلك البنود الواردة في ذلك القسم تطبق للكشف عن المعلومات بواسطة أو لمصلحة السلطة العامة. إذا كانت أغراض الكشف عن تلك المعلومات مصرح به بموجب البنود التالية:

(1) Data Protection Act 1998 Published by TSO, the stationery office p. 50 – Data retention & Investigatory powers Act 2014 chapter 27.

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

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

(4) Ibid, p. 51.

أ - أغراض أي تحقيق جنائي سواء يجرى بالفعل أو سيتم لاحقا سواء بالمملكة المتحدة أو أي مكان.
 ب- لأغراض أي إجراءات جنائية سواء تتم بالفعل أو ستبدأ لاحقا 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.⁽¹⁾ ويتضمن دليل حماية البيانات الأوروبي لعام 1995 حماية فاعلة ضد استخدام
 البيانات الشخصية الحساسة⁽²⁾.

علاوة على ما سبق أصدرت المفوضية الأوروبية في عام 2000 نموذجا جديدا 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⁽³⁾.

يرى الفقه أن حماية الخصوصية تؤدي – غالبا – إلى تعزيز الأمن المعلوماتي، وذلك من خلال تقنين
 الإدارة لأنشطتها في حيازة المعلومات، أو على الأقل تبرير قيامها بنشاط تجميع البيانات والمعلومات على
 مستوى المسؤولين الأعلى، أو من خلال لجنة من الكونجرس أو قضاة فيدراليين أو بمتطلبات الإذن القضائي
 أو أية إجراءات لحماية الخصوصية وجهود الأمن القومي⁽⁴⁾.

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 عبئا إضافيا على الجهة
 القائمة بالتشريع والجهة القائمة بالضبط في مسائل الأمن المعلوماتي، ومثال ذلك: أن الدخول Access

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

(2) منير محمد الجنيهي، ممدوح محمد الجنيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي 2006 ص84.
 مثال: تلك 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.

(3) المرجع السابق ص85 «تجدر أن التوجيهات الصادرة عن الاتحاد الأوروبي عموما 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».

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

برز في العام 1996 أمام محكمة كانساس العليا في قضية الولاية ضد Allen⁽¹⁾. 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» (Cyber Intelligence Sharing and Protection Act)؛ إذ يسمح ذلك القانون بمشاركة المعلومات ما بين الحكومة الأمريكية وشركات التقنية والتصنيع⁽²⁾. ومن القضايا التي أثرت 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 (17-78)، 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⁽³⁾.

بالإضافة إلى ما سبق صدرت العديد من قوانين الخصوصية الأمريكية على مستوى القطاعات sectoral privacy laws كمثال: تبني قسم الصحة والخدمات الإنسانية The department of Health Human Services في العام 2001 قواعد - مصرح بها من الكونجرس - لا تجيز الإفصاح عن المعلومات الشخصية الصحية ما لم يكن ذلك في إطار من القانون⁽⁴⁾.

وعلى صعيد التشريعات العربية التي وازنت بين الأمن المعلوماتي وتعزيزه، وحماية الخصوصية والبيانات الشخصية من الانتهاك أو التدمير نص القانون الكويتي رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية في

(1) نطاق الجريمة الافتراضية (تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب): - أورين كير: بحث منشور في مجلة القانون - جامعة نيويورك - العدد 78 / نوفمبر 2003، ترجمة د/ عمر محمد بن يونس، الأكاديمية الدولية للتجارة الدولية 2008 ص74. «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 مجاناً، وعندما اتصل Allen بحواسيب الشركة المذكورة واجهته شاشة تطلب منه اسم المستخدم وكلمة العبور. ولقد اتضح للمحققين أن Allen ضمن كلمة العبور بدقة وقام لاحقاً بإزالة الدليل على نشاطه بإلغائه للسجلات Logs، ولقد تمت إدانة Allen بدخوله إلى حواسيب الشركة بدون تصريح انتهاكاً لتشريع جرائم الحاسوب بولاية كانساس.

(2) 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».

(3) د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت - دار الجامعة الجديدة 2012 ص600.

(4) 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".

المادة 35 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 القضاة والتلف أو الإفشاء أو الاستبدال ببيانات غير صحيحة أو إدخال معلومات عليها على خلاف الحقيقة⁽¹⁾.

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 من ذلك الوقوع في فخ المطالبة بإنشاء محكمة دولية إلكترونية لعلاج الجرائم المعلوماتية المهددة للنظام العام⁽²⁾.

أما الرأي الذي نميل إليه هو أن تلك المواقع أصبحت واقعا 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⁽³⁾.

وقد نصت المادة 37 من قانون المعاملات الإلكترونية الكويتي رقم 20 لسنة 2014 على أنه: «فيما عدا ما تحتفظ به 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...»⁽⁴⁾ وبالنظر إلى الواقع 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

(1) انظر: القانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية: الكويت اليوم، العدد 1172، السنة الستون، بتاريخ 2014/2/23.

(2) جريدة الشاهد الكويتية الورقية - العدد 2716 صدرت الأربعاء 13 يوليو 2017 الصفحة الثالثة. انقسمت الآراء التشريعية والبرلمانية هناك إلى أربعة آراء: - الرأي الأول يرى تفعيل القانون الكويتي للجرائم الإلكترونية واللجنة 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 نهائيا، أما الرأي الرابع والأخير فيرى وجوب التوافق مع القضاء المعلوماتي بمتطلباته الحديثة. وهو الرأي الوسط الذي نميل إليه.

(3) تثار تلك المشكلة في دولة الكويت خاصة؛ لأن النسيج الاجتماعي هناك يحتوي على فئات مختلفة اجتماعيا، 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 يخلون بالأمن العام.

(4) انظر: قانون المعاملات الإلكترونية الكويتي رقم 20 لسنة 2014، منشور بجريدة الكويت اليوم العدد 1172، السنة الستون، بتاريخ 2014/2/23.

تشريعي ينظم دواعي الحجب وحدود ذلك الحجب وتوقيتاته؛ حيث قضت المحكمة الإدارية العليا في أحد أحكامها بأن: «الحريات والحقوق العامة التي كفلها الدستور ليست طليقة من كل قيد وإنما يجوز تنظيمها تشريعيا بما لا ينال من محتواها، ومن ثم فإن القيود التي يفرضها المشرع على تلك الحرية تمثل استثناء من الأصل الدستوري المقرر بكفالة وضمان حرية التعبير، ومن ثم يجب أن تكون في أضيق الحدود، ولما كانت التشريعات المصرية لم تحدد الحالات التي تستدعي حجب المواقع الإلكترونية إلا أن هذا الفراغ التشريعي لا يخل بحق جهة الإدارة في الحجب حينما يكون هناك مساس بالأمن القومي أو المصالح العليا بما لتلك الأجهزة من سلطة في مجال الضبط الإداري لحماية النظام العام بمفهومه المثلث الأمن العام والصحة العامة والسكينة العامة للمواطنين»⁽¹⁾.

(1) انظر: الطعن رقم 10171 لسنة 54 ق. عليا المحكمة الإدارية العليا - الدائرة الثانية - حكم غير منشور - وكانت الدعوى تطالب بحجب المواقع الإلكترونية لارتكابها جرائم جنائية ضد الدولة. "ويتعين التفرقة في هذا الصدد بين التعدي على الحق الفردي للأشخاص وبين التعدي على المجتمع وأمنه وأمانه، وإن كانا كلاهما ممقوتا وممجوجا تلفظه الشرائع ونصوص الدستور والقانون، أما حال المساس بأمن المجتمع وأمانه فلا يدرأه إلا أن يوصد منبع هذا الخطر موقعا على شبكة الإنترنت أو غيره".

المبحث الثالث

حيازة جهة الإدارة للمعلومات وقواعد البيانات كأحد محددات الضبط التشريعي

تعد حيازة جهة الإدارة للمعلومات وقواعد البيانات أحد محددات الضبط التشريعي؛ حيث يفضل أن ينص التشريع المنظم للأمن المعلوماتي على عدة نصوص أهمها احتكار المعلومات، وإن 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 في النقاط الآتية:

أولاً: حيازة المعلومات على ميزان المشروعية

ثانياً: حيازة البيانات الروتينية

ثالثاً: الآليات المعتادة لرصد وحيازة البيانات والمعلومات

رابعاً: إشكاليات حيازة جهة الإدارة للمعلومات وطرق حلها

خامساً: حيازة الإدارة للمعلومات البيومترية

أولاً: 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 الحواسيب الآلية التي تسجل كل دقائق الأمور⁽¹⁾. وإذا تطرقنا إلى التشريع الأمريكي نجد أن جهة الإدارة هناك تحوز رصيда هائلًا 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 أمراً مكلفاً وباهظ الثمن⁽²⁾.

(1) 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).

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

كما قد يلزم المشرع جهة الإدارة بتدابير معينة يتم النص عليها في القانون كاتخاذ التدابير الوقائية اللازمة أمنياً لحماية أنظمتها المعلوماتية وشبكاتها والبيانات والمعلومات الإلكترونية الخاصة بها.⁽¹⁾ بل وقد يذهب في صورة أكثر تفصيلاً لإلزام الجهة المختصة باتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأدوات والأنظمة المعلوماتية.⁽²⁾ وعادة قد يكون جمع الحكومات للبيانات والمعلومات الشخصية حول الأفراد استجابة لظروف معينة تتعلق بالأمن القومي كمخاوف الحكومة الأمريكية من الهجمات الإرهابية.⁽³⁾

ثانياً: حياة البيانات الروتينية

هناك نوع من البيانات يطلق عليه «البيانات الروتينية» تحصل عليه المؤسسات العامة والخاصة من العملاء يومياً 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

2008., p. 1

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

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

(1) نص المشرع القطري في المادة 22 من قانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية الإلكترونية، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6366&language=a>

(آخر تحديث 2018/10/6)

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

(1) اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكات المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها.

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

(3) الاحتفاظ ببيانات تقنية المعلومات ومعلومات المشترك لمدة لا تقل عن 120 يوماً وتزويد الجهة المختصة بتلك البيانات.

(4) التعاون مع الجهة المختصة لتنفيذ اختصاصاتها.

(2) نص المشرع القطري في المادة 19 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 (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=7121&language=ar>

(آخر تحديث 2018/10/6)

من التشريعات العربية التي نجحت في إقامة التوازن بين الخصوصية المعلوماتية للأفراد وبين تحقيق الأمن المعلوماتي من خلال منظومة التشريعات التي يعد أبرزها القانون 14 لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية.

(3) 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 chairmann 9/11 public Discourse project).

تتعلق بالصحة والأمور المالية، أو الأذواق سيكون من الخصوصية بخلاف أن تطلب الحصول على تلك البيانات لن يكون بدون ضمانة أو تصريح قضائي⁽¹⁾.

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 2001، 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 «suspicious Activity Reports»، وتقارير تحويل العملة «Currency Transaction Reports»⁽²⁾.

ثالثاً: الآليات المعتادة لرصد وحيازة البيانات والمعلومات

بالنظر للآليات المعتادة لرصد وحيازة البيانات والمعلومات تعتمد 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 إجراءات ضبط إداري تمكن وزارة الداخلية من القيام بدورها المنوط بها، واعتبرت أن قيام جهة الإدارة بإنشاء تلك الآلية يعد من قبيل الرقابة والتنظيم وليس التقييد⁽³⁾. لذلك تتعدد آليات الإدارة في رصد المخاطر المعلوماتية لكننا سنقتصر على أهم آليتين، وهما كالتالي:

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

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

(2) 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".

(3) حكم محكمة القضاء الإداري - الدائرة الثامنة عقود في الدعوى رقم 63055 لسنة 68 ق، بتاريخ أغسطس 2015 (حكم غير منشور).
«... فكل من الدستور والقانون قد أوجب على وزارة الداخلية الحفاظ على النظام العام والأمن العام والأرواح والأعراض والأموال ومنع الجرائم وضبطها والبرنامج ليس إلا وسيلة لتمكين وزارة الداخلية من القيام بدورها المنوط بها، فضلاً عن أن هذا البرنامج من شأنه فقط الاطلاع على محتوى متاح للكافة يمكن لأي شخص الاطلاع عليه بمجرد دخوله على شبكة الإنترنت، وليس من شأنه اختراق حسابات الأشخاص، أو الاطلاع على بياناتكم الشخصية...».

أولاً: نظام الأرشفة الإلكترونية

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

- 1 - تشكيل لجان حكومية في كل إدارة لدراسة أفضل طرق حفظ الوثائق المعلوماتية.
- 2 - أخذ نسخ للبرامج بغرض تشغيل الدعامات القديمة عند الحاجة إليها.
- 3 - استخدام 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⁽¹⁾.

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 تجمع بها البيانات عن الأهداف أو الظواهر الطبيعية⁽²⁾.

رابعا: إشكاليات حيافة جهة الإدارة للمعلومات وطرق حلها

على صعيد إشكاليات حيافة جهة الإدارة للمعلومات وطرق حلها نجد أنه قد تثير حيافة جهة الإدارة للمعلومات الشخصية - خاصة الواردة من أطراف ثالثة - إشكاليتين، الأولى: الكفاءة «efficacy»؛ بمعنى هل تضمن عملية حيافة 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⁽³⁾. لذا يمكن تلخيص عنصر الكفاءة في البنود الآتية:

البند الأول: جودة البيانات Data Quality

في محاولة لتقييم مصطلح حيافة المعلومات لحماية الأمن القومي، قام المركز البحثي التابع للكونجرس

(1) د/ ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية - رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة - 2011، ص181، 182.

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

(3) 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:

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

(CRS) بتعريفه على أنه مسألة متعددة الوجوه ويشكل ذلك التحدي الأبرز في حيازة المعلومات⁽¹⁾. وتتأتى الإشكالية الأكبر في بند جودة المعلومة كما ذكر في مجلة «computer world» في 2003 من أن «بيانا واحدا 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⁽²⁾.

البند الثاني: تناسق البيانات Data matching

تواجه جهة الإدارة العديد من الأخطاء في حيازة المعلومات⁽³⁾ ومنها تناسق البيانات، وقد يستعان في الولايات المتحدة الأمريكية للتغلب على تلك الأخطاء برقم الضمان الاجتماعي «social security Numbers»

- (1) 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».
- (2) 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”
- (3) 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 (19) لسنة 2016 بإنشاء اللجنة الوطنية لأمن المعلومات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6920&language=ar>

(آخر تحديث 2018/10/6)

- حيث نصت المادة 3 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 4 من القرار: «لجنة في سبيل تحقيق أهدافها، ممارسة جميع الاختصاصات والصلاحيات اللازمة لذلك، وبوجه خاص ما يلي:
- 1 - 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.
 - 2 - 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.
 - 3 - اعتماد خطط إدارة المخاطر المتعلقة بأمن المعلومات وتبادل المعلومات المتعلقة بها.
 - 4 - دعم المشاريع الخاصة بتأمين البنية التحتية المعلوماتية بالدولة.
 - 5 - 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.
 - 6 - توجيه الجهات المعنية لوضع الخطط والبرامج الوطنية للبحوث والتطوير في مجال أمن المعلومات، بالتعاون مع المؤسسات الأكاديمية والبحثية داخل الدولة وخارجها.
 - 7 - دعم مبادرات التعليم والتدريب والتوعية في مجال أمن المعلومات.

وقد واجهت الإدارة في الولايات المتحدة نفس الإشكالية خاصة عند مواجهة الإرهاب.⁽¹⁾ 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 – غالبا – ما يعتمد مخترقو الأمن المعلوماتي لتضليل جهة الإدارة مقارنة بالقطاع الخاص «Government data mining often is searching for needle not in a haystack, but among millions of other needles». ومع ذلك تعد المعلومات الواردة من القطاع الخاص مفتاحا مهما للأمن القومي من خلال توقع المسؤولين عن الأمن القومي للسلوك المعتاد لعملاء القطاع الخاص⁽²⁾.

«Government data mining seems similarly likely to fighting yesterday's battles»⁽³⁾.

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⁽⁴⁾.

(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) 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 توقعا للهجمات الإرهابية الخارجية من خلال توقع ضباط الاستخبارات للخطط الإرهابية بناء على النشاط الإرهابي في الماضي، بخلاف الهجمات الإرهابية المحلية التي تتخذ شكلا مختلفا كل مرة في التخطيط والتنفيذ؛ بحيث تكون مواجهتها أقل وفرص كشفها غير متوقعة.

(3) 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.

(4) 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 (5) لسنة 2013 بتشكيل «اللجنة الوطنية القطرية لتنسيق الطيف الترددي، منشور على شبكة المعلومات الدولية على الرابط:

البند الرابع: تقدير الكفاءة Assessing Efficacy

يذهب الفقه المقارن إلى القول بأهمية تقدير كفاءة نظم حيازة المعلومات، ومن المحاولات الأولى في ذلك ما تتطلبه التشريع الأمريكي عند أية محاولة لحيازة المعلومات من أن يكون هناك إذن مكتوب من الرئيس الإداري الأعلى للجهة الإدارية حائزة المعلومات⁽¹⁾. مؤدى ما سبق يرى البعض وجود حرج في مساءلة جهات الإدارة التي تقوم على حيازة البيانات الشخصية للأفراد على اعتبار أن قراراتها – غالبا – ما تكون مدروسة وبناء على ضمير مهني⁽²⁾، وفي اعتقادنا أن صعوبة إثبات المسؤولية الإدارية عن الخطأ في حيازة الإدارة للمعلومات لاتعني القول بنفي المسؤولية عنها.

خامسا: حيازة الإدارة للمعلومات البيومترية

يمكن أن نتناول في نقطة أخيرة إشكالية حيازة الإدارة للمعلومات البيومترية كونها من مكونات نظم حيازة المعلومات لتفعيل آليات الضبط الإداري؛ حيث يمكن أن يمتد الأمن المعلوماتي إلى التسجيلات

<http://www.almeezan.qa/LawPage.aspx?id=6113&language=a>

(آخر تحديث 2018/10/6)

- وجاء في «المادة 2 منه» 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 الرئيسة للجنة الوطنية القطرية لتنسيق الطيف الترددي فيما يلي:
- 1 - مناقشة القضايا المحلية والإقليمية والدولية المتعلقة بالاتصالات الراديوية.
 - 2 - تقديم التوصيات بشأن بعض تخصيصات التردد والتي تتعلق بالخطة الوطنية لتخصيص التردد، والقضايا التي تتطلب التنسيق بين مختلف مستخدمي الاتصالات اللاسلكية في البلاد.
 - 3 - إعداد مقترحات للمؤتمرات والاجتماعات الإقليمية أو الدولية وتنسيق كافة الأنشطة المتعلقة بالاتحاد الدولي للاتصالات والطيف الترددي على المستوى الوطني.
 - 4 - إعداد التوصيات لتعزيز الإرشادات الخاصة بالانبعاثات والإشعاعات الكهرومغناطيسية من محطات الاتصالات الراديوية المنصبة على أبراج وصواري الاتصالات.
 - 5 - تقديم التوصيات عند الضرورة للجهات ذات العلاقة فيما يتعلق بمشاركة الأبراج وصواري الهوائيات من قبل أكثر من مستخدم للاتصالات اللاسلكية.

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

7 - 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⁽¹⁾.

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

(2) 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).

الإلكترونية للمعلومات البيومترية كالحامض النووي DNA، ووفقا لذلك نص قانون حماية المعلومات لعام 2012 الصادر في المملكة المتحدة في المادة 23 منه على ما يلي: «بالاستناد إلى القسم (63 أ) من لائحة الإثبات الجنائية والشرطية لعام 1984 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⁽¹⁾.

أضف إلى ذلك أن القوانين المقارنة تعمل على حفظ الأمن العام كأحد أركان النظام العام في الدولة عن طريق حيابة «المعلومات البيومترية»⁽²⁾.

(1) Protection of freedoms Act 2012 Chapter 9- United Kingdom, p. 18 clause 23.

وحماية لتلك البيانات الشخصية أشارت المادة 24 من ذات القانون إلى المجلس الخاص باستراتيجيات البيانات القومية للحامض النووي (National DNA Database 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.

(2) "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 تتعاضد أهميتها في الآونة الأخيرة خاصة بعد العمليات الإرهابية المتزايدة. وتجدر الإشارة إلى اختصاصات إدارة الأمن السيبراني بوزارة المواصلات والاتصالات في قطر وفقا للقرار الأميري رقم (8) لسنة 2016 بالهيكل التنظيمي لوزارة المواصلات والاتصالات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6895&language=ar>

(آخر تحديث 2018/10/6)

- بحسب مانصت عليه المادة 22؛ حيث نصت على أن: "تختص إدارة الأمن السيبراني بما يلي:
- 1 - وضع استراتيجية وطنية لأمن المعلومات ومتابعة تنفيذها، بالتنسيق مع الجهات المختصة.
 - 2 - وضع السياسات والمعايير لرفع كفاءة وسائل الحماية لأنظمة تشغيل البنية التحتية الوطنية للمعلومات الحيوية في كافة القطاعات، والإجراءات اللازمة لضمان الامتثال لها.
 - 3 - إعداد برامج تدريبية وتوعوية مصاحبة لدعم الجهات المعنية لتطبيق السياسات الموضوعية وذلك بالتنسيق مع الجهات المختصة.
 - 4 - التنسيق مع المنظمات العالمية والأجهزة الحكومية وغير الحكومية والهيئات والجهات المماثلة لضمان أمن البنى التحتية الحيوية وحماية شبكات ونظم المهمات الحيوية وتقييم أداؤها وحماية الأنظمة المعلوماتية من الاختراقات والهجمات الإلكترونية.
 - 5 - تطبيق قواعد أمن أنظمة التطبيقات الحيوية، لمنع تسريب أو نشر البيانات السرية، واتخاذ الإجراءات اللازمة لمنع الاختراقات لضمان الاستمرارية في العمل.
 - 6 - وضع ضوابط وإجراءات الاتصال وحفظ أمن المعلومات، وحماية خصوصية البيانات المتداولة عبر الأنظمة والشبكات الإلكترونية ومتابعة تطبيقها والتصديق على التزام الجهات المعنية بها.
 - 7 - اقتراح مشروعات الأدوات التشريعية الخاصة بأمن المعلومات والبنية التحتية للمعلومات الحيوية وإبداء الرأي في المنازعات.

-
- 8 - وضع نطاق المراقبة والإنذار المبكر لتفعيل قدرات الاستجابة للحوادث من خلال تطوير وسائل تقنية الرصد الإلكتروني وتطبيقات تحليل البرامج الخبيثة.
- 9 - اتخاذ الإجراءات اللازمة لتنفيذ إطار الاستجابة لحوادث الفضاء الإلكتروني.
- 10 - تحليل المخاطر السيبرانية ودراسة أفضل السبل لتجنبها والقدرة على مواجهة الأزمات السيبرانية بمرونة وتطويرها من خلال المشاركة مع المؤسسات الأكاديمية ومراكز البحث العلمي.
- 11 - وضع المعايير والآليات لفحص واعتماد أجهزة الاتصالات وتكنولوجيا المعلومات لضمان خلوها من آليات تسريب قبل تركيبها واستخدامها على شبكات الاتصال الحيوية مثل الشبكات الوطنية.
- 12 - وضع آليات تنظيم عمل مزودي خدمات التصديق الإلكتروني ووضع آليات العمل اللازمة لتقديم خدماتهم بجودة.
- 13 - وضع آليات ضبط التعامل بالهوية الرقمية لتفادي تسرب المعلومات السرية».

المبحث الرابع

الشراكة المعلوماتية كأحد محددات الضبط التشريعي

تعد الشراكة المعلوماتية بين القطاعين العام والخاص أحد أهم وسائل تعزيز الأمن المعلوماتي، فضلا على ضرورة التعاون الدولي لتوفير الحلول⁽¹⁾. فالتقنيات المستعملة في الاختراقات المعلوماتية لا بد أن تواجه بطرق جديدة للتعامل لإدارة تلك الاختراقات من خلال وجود قواعد معلوماتية واستخباراتية تحدد نوع التهديدات فضلا عن التنسيق بين العديد من القطاعات على مستوى التشريع القانوني والرقابي⁽²⁾. ومن أهم المنظمات التي تولت الاهتمام بالأمن المعلوماتي دوليا الاتحاد الأوروبي، وحلف الناتو الذي اعتمد في ذلك على الشراكات بين مختلف الأجهزة الحكومية وغير الحكومية⁽³⁾.

ويرى الفقه المقارن أن هدف نظم الشراكة بين القطاعين العام والخاص في مجال الأمن المعلوماتي يرمي إلى وجود تدابير وقائية وبرامج أمن معلوماتي تقلل المخاطر المعلوماتية⁽⁴⁾.

(1) تطرق المؤتمر السنوي الثالث لأمن المعلومات المنعقد بالدوحة في نوفمبر 2016 إلى ذلك وأعرب الرئيس السابق لاسكوتلانديارد «اللورد ستيفنز» إلى أن جميع القطاعات أصبحت معنية بتأمين معطياتها وبياناتها؛ حيث عمد بعض القراصنة إلى الاستحواذ على بيانات وملفات اللاعبين المشاركين في الأولمبياد.

ساير المشرع القطري ذلك بالنص في الباب الرابع: التعاون الدولي المادة 23 من قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية نصت على أنه: «يتعين على الجهة المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القانون، وفقا للقواعد التي يقررها قانون الإجراءات الجنائية المشار إليه والاتفاقيات الثنائية أو متعددة الأطراف التي تكون الدولة طرفا فيها، أو مبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القانون أو أي قانون آخر.

ولا ينفذ طلب المساعدة القانونية أو طلب تسليم المجرمين، استنادا إلى أحكام هذا القانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تدرج الجريمة في فئة الجرائم ذاتها أو تستخدم في تسمية الجريمة ذات المصطلح المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرما بمقتضى قوانين الدولة الطالبة.

(2) من أمثلة قطاعات البنية التحتية المعلوماتية القطاعات المالية والطاقة والرعاية الصحية والاتصالات والاستخبارات ووزارة الداخلية... إلخ. (3) Cezar PETA: cyber security – current topic of National security Public security studies, volume II, Issue 3 (7) / 2013, p. 67 “cyber security is challenge that must be tackled through cooperation between various national actors, and institutions, private companies and non-governmental organizations, and international level through cooperation among states, regional and global organizations.

في اعتقادنا أن الاتفاقيات الدولية ومذكرات التفاهم أحد أنجع الوسائل لتبادل الخبرات، ومثال ذلك: ما نادى به البعض من عقد اتفاقيات دولية رقمية كمثال دعوة شركة MICROSOFT إلى عقد “اتفاقية جنيف الرقمية” التي تتطلب من الحكومات الإبلاغ عن ثغرات الأجهزة الحاسوبية للبائعين بدلا من تخزينها أو بيعها أو استغلالها.

(4) Ibid, p. 70

- “Dan Tofan, Technical director of CERT – RO stated that, there are situations in which the entity can not manage

أما الفقه الأمريكي فهو يفضل الأساليب العملية في تحقيق الأمن المعلوماتي، وذلك عن طريق التعاون الدولي قانونيا وقضائيا كالاتفاق في مجال الاختصاص القضائي، والقانون الواجب التطبيق في بيئة منازعات الإنترنت⁽¹⁾. علاوة على ما سبق يمكن الاستفادة من خبرات القطاع الخاص في مجال الأمن السيبري، كمثال إطار «NIST» (المعهد الوطني للمعايير والتكنولوجيا)، وذلك لحماية البنية الأساسية الحيوية المحلية Domestic critical Infrastructure، وذلك في الولايات المتحدة الأمريكية⁽²⁾.

ويرى الفقه الأمريكي إمكانية لجوء جهة الإدارة إلى إجراء برامج لتطوير برامج حيازة البيانات من خلال تقنيات أكثر سرعة وبشكل قابل لتحمل التكلفة، وتسمح تلك التقنيات لجهة الإدارة بالتحرك في الفترة ما بعد الجريمة بالبحث عن بيانات الأفراد موضوعي البحث عن البيانات.⁽³⁾

لذا يؤكد الفقه الأمريكي على أن الولايات المتحدة الأمريكية في مجال تعزيز الأمن المعلوماتي تستعين بالقطاع الخاص واستثماراته في الوقاية ووضع تدابير احترازية للأمن المعلوماتي، وتستعين بالقطاع العام واستثماراته في العلاج وتلافي آثار الانتهاكات المعلوماتية⁽⁴⁾. في اعتقادنا أن البنية الأساسية الحيوية هي الأولى بوضع التدابير الاحترازية؛ لذا سعت الولايات المتحدة إلى «حماية البنية الأساسية الحيوية» critical

incident alone, and in this case the cooperation between both entities becomes very important".

من وحدات الإدارة المعنية بالأمن المعلوماتي على سبيل المثال: وزارة العدل، ووزارة الداخلية، ووزارة نظم المعلومات، والمخابرات بأنواعها أما الوسائل الافتراضية فلن تفيد، ومثالها: دعوات إنشاء حكومة الإنترنت أو بوليس الإنترنت، أو معايير الاستخدام الموحد، أو سياسات التنظيم الذاتي للالتزامات؛ وذلك لأن الإنترنت يتصف (باللامركزية) وغياب السلطة التحكيمية.

(2) 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>

(3) 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 في 11 سبتمبر؛ حيث كشفت جهة الإدارة في الولايات المتحدة الأمريكية بيانات هائلة حول الأفراد مستمدة من القطاع الخاص، وبذلك يكون الكونجرس قد أخفق في الموازنة بين الخصوصية "privacy" والأمن القومي "National security"

- For more – the Cantigny principles on technology terrorism, and privacy, National security law Report, feb. 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".

(4) Nathan Alexander sales: Regulating cyper security – Northwestern university law Review 2013 vol., 107, No 4, p. 1506

«infrastructure» والتي تعني بالأساس حماية النظم «system» والأصول «assets» والتي لها تأثير على الأمن بصفة عامة، والأمن الاقتصادي القومي، والصحة العامة والسلامة العامة أو كل ما سبق⁽¹⁾.

ويساير ما سبق ما يميل إليه الفقه الأمريكي من تعزيز الأمن المعلوماتي بصورة شاملة في كل من القطاعين العام والخاص، ولكن لابد من الأخذ في الاعتبار أن المؤسسات العامة وشركات الطاقة أقل في القدرة الوقائية في مجال الأمن المعلوماتي من الشركات التجارية التنافسية⁽²⁾. علاوة على ما سبق يمكن تحديد سبل حماية الأمن المعلوماتي في الولايات المتحدة من خلال حماية الأمن المعلوماتي للبنية الأساسية الحيوية عن طريق وصف الموقف الأمني السيبراني لجهة الإدارة، وتحديد وترتيب أولويات فرص التحسين في إطار عملية مستمرة ومتكررة، والتواصل بين الجهات المعنية بالأمن السيبراني في داخل الدولة وخارجها حول مخاطر الأمن السيبراني⁽³⁾.

في اعتقادنا أن جهة الإدارة لا بد أن تأخذ 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 تعاقد جهة الإدارة مع شركة تقوم باستبدال تقنية معينة لديها 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⁽⁴⁾.

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

(2) Bruce P. smith, Hacking, Poaching, and counterattacking: Digital counterstrikes and the contours of self-Help, 1 J.L Econ, & Pol'y 171, 173 (2005),p.32

(3) Hanover Research, op. cit., p. 16

ويمكن الاستعانة في ذلك بإطار (NIST) المعهد الوطني للمعايير والتكنولوجيا الذي يقوم على تحسين الأمن السيبراني للبنية 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.

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

والجدير بالذكر أن جهة الإدارة - خاصة في حالة نقص مواردها المالية أو عدم خبرتها بأطر الضبطيين التشريعي والإداري للأمن المعلوماتي - بين خيارين ليسا من السهولة بمكان؛ حيث يتمثل الخيار الأول في تعزيز أمنها المعلوماتي، ويتمثل الخيار الثاني في شراء التكنولوجيا الأجنبية لتعزيز الأمن المعلوماتي⁽¹⁾. لذا يرى البعض أن التشفير يعد وسيلة مهمة لحماية الإدارة من المخاطر المعلوماتية؛ خاصة في حالة تداول البيانات والمعلومات بين جهات إدارة مختلفة في صورة قرارات أو أوامر أو تعاقدات إدارية⁽²⁾.

قد يكون التشفير حلاً مؤقتاً عن طريق تأمين الشبكات المعلوماتية لجهة الإدارة كتغيير طريقة التشفير والمراجعة الدورية لأساليب الحماية، ويمكننا إضافة لذلك بمراعاة حصر الاختصاصات للموظفين الذين يتعاملون مع البيانات والمعلومات الحكومية وغيرها⁽³⁾.

وعامة تشكل العناصر الفنية المعروفة في مجال الأمن المعلوماتي كمثال اختبارات الاختراقات العادية، وبناء شبكة موازية «Parallel network construction» أحد أهم عناصر تعزيز الأمن المعلوماتي لجهة الإدارة إلى جانب العناية الواجبة «Due Diligence»⁽⁴⁾. علاوة على ما سبق تشكل التجربة اليابانية في مجال الأمن

(1) Scott J. Shackelford & others, op. cit., p. 22

وفي اعتقادنا أن ذلك يتوجب أن تمتلك الدولة إمكانيات اقتصادية هائلة في مجال تكنولوجيا المعلومات والأمن المعلوماتي، علاوة على توفر الكوادر المدربة والمؤهلة لذلك؛ لذا من المبادئ الدولية في حماية الأمن المعلوماتي، والتي تلجأ لها بعض الدول مبدأ استبعاد تكنولوجيا الأمن المملوكة للأجانب، وعلى سبيل المثال: الصين، وهي في ذلك تخالف السياسة الأمريكية، والألمانية في حماية وتعزيز الأمن المعلوماتي.

- For more: see Amanda N. 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 في الحفاظ على عيوب البرمجيات السرية - من أجل إجراء التجسس والحرب الإلكترونية - وبين تقاسم تلك العيوب مع شركات التكنولوجيا لضمان الأمن المعلوماتي، فقد توصل القراصنة الإلكترونيون إلى "فيروس الفدية" الذي انتشر مؤخراً من خلال استغلال الثغرات الصفرية الموجودة في برامج تشغيل ويندوز للتجسس على الأفراد والحكومات والتي طورتها وكالة الأمن القومي الأمريكية.

(2) د/ بشير علي باز: دور الحكومة الإلكترونية في صناعة القرار الإداري والتصويت الإلكتروني، مجلة روح القانون، كلية الحقوق جامعة طنطا، 2007، ص 35، 36.

(3) د/ عماد يوسف حب الله، ورشة عمل حول بناء القدرات في مجال الحماية القانونية على الإنترنت، 4 - 5 شباط 2009، الهيئة المنظمة للانصالات في لبنان - أمن الفضاء السيبراني، ص 27.

«على سبيل المثال حماية التطبيقات المهمة عبر استخدام بنى تحتية مزدوجة ذات طبقات حماية متعددة تضمن ألا يحقق الدخلاء أهدافهم من خلال اختراق وإسقاط نظم المعلومات، وكذلك تعزيز البنى التحتية المعلوماتية باعتماد كلمات سر صعبة الاختراق، وأنظمة حماية متعددة الطبقات، ومنهجية النسخ المتطابقة Mirroring، والأرشفة الاحتياطي للبيانات، وحماية شبكة المعلوماتية في الشركات والمؤسسات التجارية، والاعتماد على مواقع تكون بمثابة نسخة مطابقة للأصل خارج أراضي الدولة عند وجود بيانات عالية السرية.» - «ساعد ذلك جورجيا على تخطي الاختراق الروسي لبياناتها الإلكترونية؛ حيث تم استعمال بوابات بديلة مطابقة للبوابات الأصلية تقع في الأراضي الأمريكية.»

(4) Ibid, p. 24.

المعلوماتي أنموذجاً للشراكة المعلوماتية؛ إذ نجد أن المجتمع الياباني قد انتقل من الحالة الورقية إلى الحالة الرقمية⁽¹⁾.

من هنا لم يكن لجهة الإدارة في اليابان أن تتكل على مجهودات فردية للقيام بالتأمين؛ لذا عمدت إلى بناء جسرين: الأمن المعلوماتي، والأمن القومي، بل تحقيق الشراكة بين القطاع الحكومي والخاص لتعزيز الأمن المعلوماتي.⁽²⁾ وتجدر الإشارة إلى أن المجلس القومي لليابان لسياسات أمن المعلومات يعد من وحدات الضبط الإداري المهمة؛ حيث تم إنشاؤه من خلال توصيات اللجنة التي شكلت لدراسة مشكلات قطاع تكنولوجيا المعلومات والاتصالات في مايو 2005.

وفي اعتقادنا أن ذلك المركز من الأهمية بمكان لقيام نظام عمله على الاتصال بالمؤسسات الحكومية ووحدات جهة الإدارة اليابانية هذا من ناحية، ومن ناحية أخرى وجود ثلاثة مستويات للعمل في ذلك المركز، وبالنظر لمهام المركز نجد أنها تتحدد في نشر الإجراءات الشاملة لسياسات الأمن المعلوماتي عن طريق دعم الجهاز الإداري عند وقوع مخاطر تهدد الأمن المعلوماتي علاوة على تقوية الأمن المعلوماتي في كل المرافق والبنية الأساسية الحيوية بالدولة⁽³⁾. وتتميز التجربة اليابانية في مجال الأمن المعلوماتي بالعديد من المميزات

(1) إذ يتعامل ما يقرب من ثلاثة أرباع الشعب الياباني في محتوى رقمي معلوماتي بالكامل، ومع تلك الزيادة المطردة في الاعتماد على القضاء المعلوماتي زادت مخاطر الأمن المعلوماتي، فالغالبية الساحقة من الشركات والمؤسسات اليابانية تنفذ بشدة إجراءات الأمن المعلوماتي، لكن ثلث تلك الشركات والمؤسسات هو فقط من يطبق سياسة الأمن المعلوماتي الشاملة؛ حيث وجد أن الإجراءات الخاصة بمقاومة الفيروسات منفذة في 99.8 من الشركات والمؤسسات، أما إجراءات منع الوصول غير المشروع منفذة في 88.8 من تلك الشركات والمؤسسات، أما 36.6 فقط من المؤسسات تنفذ السياسات الأمنية الشاملة.

(2) تخطو اليابان خطوات محسوبة في مجال الأمن المعلوماتي بدءاً من عام 2000؛ حيث كانت الخطة التي سارت في مسارين أولهما تعزيز الأمن المعلوماتي في القطاع الإداري، وثانيهما تعزيز الأمن المعلوماتي في البيئة القومية الحيوية، ثم عام 2001 صدرت خطة عمل لمواجهة الإرهاب الإلكتروني الذي يستهدف البيئة الأساسية الحيوية للدولة، ثم في عام 2002 بدأت الشراكة بين القطاع الخاص والحكومي فيما يتعلق بتعزيز الأمن المعلوماتي، وفي عام 2003 تم تنفيذ اختبارات لقياس مدى المخاطر التي يتعرض لها الجهاز الإداري للدولة.

(3) جمال غيطاس - مرجع سابق ص 259.

«يختص ذلك المجلس بما يلي:

تطوير الاستراتيجية الأساسية ما بين خطة طويلة الأجل وأخرى متوسطة الأجل وثالثة سنوية).

التقييم المسبق والتقييم بأثر رجعي لسياسة الأمن المعلوماتي.

قياس الاستجابة لما يطرأ من حوادث معلوماتية.

تطوير إرشادات لسلامة الأمن المعلوماتي.

تقييم سياسات الأمن المعلوماتي لكل وزارة واختيار أفضلها.

علاوة على ما سبق تم إنشاء المركز القومي لأمن المعلومات كجهة تنفيذية يرأسه نائب رئيس الوزراء ومعه مدير عام مناب ومستشار في أمن المعلومات وحوالي 60 موظفاً متخصصاً، ويمكن نقل بعض تجارب ذلك المركز للاستفادة بعمل المجلس السيبراني المصري» ويولي اليابانيون اهتماماً خاصاً بمرافق الدولة الحيوية وأمنها المعلوماتي؛ إذ ينسق المركز مع وزارات المواصلات والبنى الأساسية والاقتصاد

الذي يجعلها خير معين لتبني تجارب مماثلة، وذلك كالتالي:

1 - إنشاء نموذج جديد للشراكة بين القطاع الإداري والقطاع الخاص عن طريق هجر حل المشكلات الآتية والتوجه لإنشاء بنية تتميز بالاستغلال الأمثل لتكنولوجيا المعلومات، علاوة على إشراك شركات ذات صلة بالأمن المعلوماتي تكون مسؤولة عن حدوث أي تغيرات في خدماتها ولا تهدف إلى الربح.

2 - إيجاد توازن بين الملاءمة والأمن إذ يمكن لمستخدمي التكنولوجيا استمرار استغلالها مع الشعور الفعلي بالأمن والسلامة.

3 -توازي الجهود الإدارية والتشريعية مع المبادئ العامة والسلوكية من خلال تكوين عرف عام بين الأفراد، كمثال: التزام الموظف العام بعدم إفشاء أسرار وظيفية⁽¹⁾.

4 - تفعيل الشراكة بين الحكومة المركزية والوحدات الإدارية اللامركزية؛ حيث تتولى الحكومة المركزية في اليابان سياسات الأمن المعلوماتي، ثم يأتي دور الوحدات اللامركزية التي تنفذ تلك السياسات والخطط المركزية، وبذلك يتم القضاء على الإشكاليات البيروقراطية الفرعية وغير الاستراتيجية.⁽²⁾ وهذا ما تبناه في المادة رقم 176 من الدستور المصري المعدل في عام 2014 التي نصت على أن: «تكفل الدولة دعم اللامركزية الإدارية والمالية والاقتصادية...».

5 - تقسيم المخاطر التي تهدد الأمن المعلوماتي إلى معلومات الحكومة المركزية، ومعلومات الوحدات اللامركزية التي تقسم بدورها إلى معلومات عالية السرية ومعلومات شخصية ومعلومات حول الشركات

والتجارة والصناعة والقطاع المالي ومرافق الطاقة وشبكات نقل وتوزيع الكهرباء والمنشآت البترولية والسكك الحديدية والنقل الجوي وشبكات المياه والصرف الزراعي والصحي.

وينقسم ذلك المركز إلى المستويات التالية:

(1) المستوى الأعلى: وهو القيادة الاستراتيجية لتكنولوجيا المعلومات والاتصالات برئاسة رئيس الوزراء وعضوية كل الوزراء، بالإضافة إلى خبراء من القطاع الخاص.

(2) المستوى الثاني: ونجد بذلك المستوى المجلس القومي لسياسات أمن المعلومات إذ ينسق مع مجلس الوزراء

(3) المستوى الثالث: تمثله إدارة وحدات أمن المعلومات بالوزارات والمؤسسات والوكالات الحكومية وغير الحكومية التي تتعامل مباشرة مع المركز القومي لأمن المعلومات، وفي اعتقادنا يمكن الاستفادة من تلك المستويات المتدرجة على صعيد اللجان الحكومية الخاصة بالأمن المعلوماتي وتعزيزه.

(1) نصت المادة 86 من الدستور المصري المعدل في عام 2014 على أن: «الحفاظ على الأمن القومي واجب، والتزام الكافة بمراعاته مسئولية وطنية يكفلها القانون...».

وتجدر الإشارة إلى التفرقة بين ثلاثة أنواع من الأسرار داخل نطاق العمل الحكومي وهي الأسرار الإدارية، والأسرار الحكومية الخاصة بالمستندات وغيرها، وأسرار الأشخاص داخل العمل، وفي اعتقادنا أن الأمن المعلوماتي لجهة الإدارة ينطبق بدرجة أكبر على النوعين الأولين.

(2) قد تكون التجربة اليابانية في الأمن المعلوماتي هي الأنسب لمصر لحدثة تطبيقها؛ حيث بدأت عام 2001 تقريبا كما أنها من حيث الحجم والتنوع ليست ضخمة كالولايات المتحدة، ولكن هناك فارقا ضخما ومستوى التعليم والقدرة على إنتاج واستيعاب أدوات ومنهجيات وطرق الأمن المعلوماتي.

وذلك كالتالي:

- أ - المحتوى المعلوماتي للبنى الأساسية الحيوية؛ حيث لا بد أن تكون على درجة عالية جداً من التأمين المعلوماتي لضمان سير المرافق العامة بانتظام واطراد.
- ب - المحتوى المعلوماتي للشركات؛ حيث لا بد أن تكون على درجة عالية من التأمين المعلوماتي باعتبار تلك الشركات والهيئات توفر المنتجات والخدمات الداعمة للبنية الأساسية لتكنولوجيا المعلومات.
- ج - المحتوى المعلوماتي للأفراد؛ ويعد ذلك المحتوى هو الحلقة الأضعف في مجال أمن الفضاء المعلوماتي.

الخاتمة

- لاعتماد 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 الإدارية 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 عاملاً ناجحاً يحقق أهدافه ويوازن بين اعتبارات الفاعلية والمشروعية، كمثال الخصوصية، وحيازة جهة الإدارة للمعلومات وقواعد البيانات، والشراكة المعلوماتية، ومن المهم دراسة تلك المحددات في العديد من التشريعات المقارنة، وتوضيح بعض أدوار الجهات الإدارية من خلال الضبط الإداري في إعمال ذلك التوازن والحفاظ المشار إليهما.

- خلصنا من خلال البحث لتقصي بعض الإشكاليات الناتجة عن حيازة جهة الإدارة للمعلومات وقواعد البيانات كأحد محددات الضبط التشريعي، والوقوف على جدوى شراكة معلوماتية بين القطاع الخاص والجهات الإدارية، أو بين الدول لتحقيق تكاملية أمنية معلوماتية.

التوصيات

- 1 - تعديل التشريعات المعلوماتية العربية عامة وبدول مجلس التعاون الخليجي خاصة؛ بما يؤدي لتفعيل استراتيجيات إدارية أكثر فاعلية تتيح حيابة المعلومات على نحو مشروع، وخاصة فيما يتعلق بحيابة البيانات الروتينية والمعلومات البيومترية، واحترام الخصوصية كأحد محددات الضبط التشريعي.
- 2 - على الجهات الإدارية بدول مجلس التعاون الخليجي تحديث الآليات المعتادة لرصد وحيابة البيانات والمعلومات والعمل على حل إشكاليات حيابة جهة الإدارة للمعلومات.
- 3 - تعديل التشريعات المعلوماتية العربية عامة وبدول مجلس التعاون الخليجي خاصة؛ بما يساهم في الشراكة المعلوماتية بين القطاعين العام والخاص، فضلا على ضرورة التعاون الدولي لتوفير الحلول والتنسيق بين العديد من القطاعات على مستوى التشريع القانوني والرقابي.

المراجع العربية

أولا : 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 78 / نوفمبر 2003، ترجمة د/ عمر محمد بن يونس، الأكاديمية الدولية للتجارة الدولية، 2008.
- د/ بشير علي باز: دور الحكومة الإلكترونية في صناعة القرار الإداري والتصويت الإلكتروني، مجلة روح القانون، كلية الحقوق جامعة طنطا.
- د/ شريف يوسف خاطر: حماية الحق في الخصوصية المعلوماتية - دراسة تحليلية لحق الاطلاع على البيانات الشخصية - دراسة مقارنة - دار الفكر والقانون، 2015.
- منير محمد الجنيهي، ممدوح محمد الجنيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، 2006.
- د/ ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية - رسالة دكتوراه مقدمة لكلية الحقوق، جامعة القاهرة، 2011.
- د/ هشام محمد فريد رستم - قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992.
- د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت - دار الجامعة الجديدة، 2012.

- رسائل علمية

- أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة سنة 2006.
- راشد محمد المري، «الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة 2013.
- عمر محمد سلامة العليوي، حق الحصول على المعلومات في ضوء القانون الأردني رقم 47 لسنة 2007 - دراسة مقارنة - رسالة دكتوراه، كلية الحقوق، جامعة عين شمس سنة 2011.
- نشوى رأفت إبراهيم أحمد، حماية الحقوق والحريات الشخصية في مواجهة التقنية الحديثة «البيانات

الشخصية، المراسلات والمحدثات الشخصية، الحق في الصورة»، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة 2012.

- 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 2016 ص 10، 11.

- جريدة الشاهد الكويتية الورقية - العدد 2716 صدرت الأربعاء 13 يوليو 2017 الصفحة الثالثة.

- تشريعات

- القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=7121&language=ar>

(آخر تحديث 6/10/2018).

- القانون القطري رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar>

(آخر تحديث 6/10/2018).

- القانون الاتحادي الإماراتي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.gcc-legal.org/BrowseLawOption.aspx?country=2&LawID=3168>

(آخر تحديث 6/10/2018).

- القانون الكويتي رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية، منشور الكويت اليوم العدد 1172 السنة الستون، بتاريخ 23/2/2014.

- قرار وزير الاتصالات وتكنولوجيا المعلومات القطري رقم (5) لسنة 2013 بإنشاء اللجنة الوطنية القطرية لتنسيق الطيف الترددي، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6113&language=a>

(آخر تحديث 6/10/2018).

- قانون الجزاء العماني رقم 7 الصادر عام 1974 بموجب المرسوم السلطاني رقم 72/2001م، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.gcc-legal.org/BrowseLaws.aspx?country=1>

(آخر تحديث 6/10/2018).

- القانون الفيدرالي الأمريكي لأمن المعلومات الصادر في عام 2002.

- المرسوم الملكي السعودي رقم 17 بتاريخ 7/3/1428هـ بنظام مكافحة جرائم المعلوماتية، منشور على شبكة المعلومات الدولية على الرابط:

www.mof.gov.sa/docslibrary/RegulationsInstructions/Documents

(آخر تحديث 6/10/2018).

- قانون تنظيم الاتصالات العماني رقم 30 لسنة 2003، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.gcc-legal.org/BrowseLaws.aspx?country=1>

(آخر تحديث 6/10/2018).

- القانون العماني رقم 12/2011 الخاص بمكافحة جرائم تقنية المعلومات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.gcc-legal.org/BrowseLaws.aspx?country=1>

(آخر تحديث 6/10/2018).

- القانون الكويتي رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات - الكويت اليوم العدد 1244 السنة الحادية والستون، منشور بتاريخ 12/7/2015.

- القرار الأميري القطري رقم (19) لسنة 2016 بإنشاء اللجنة الوطنية لأمن المعلومات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6920&language=ar>

(آخر تحديث 6/10/2018).

- القرار الأميري القطري رقم (8) لسنة 2016 بالهيكل التنظيمي لوزارة المواصلات والاتصالات، منشور على شبكة المعلومات الدولية على الرابط:

<http://www.almeezan.qa/LawPage.aspx?id=6895&language=ar>

(آخر تحديث 6/10/2018).

- أحكام قضائية

- حكم محكمة القضاء الإداري المصرية - الدائرة الثامنة عقود في الدعوى رقم 63055 لسنة 68 ق، بتاريخ أغسطس 2015 (حكم غير منشور).

- الطعن رقم 10171 لسنة 54 ق. عليا المحكمة الإدارية العليا المصرية - الدائرة الثانية - حكم غير منشور.

- مؤتمرات

- المؤتمر السنوي الثالث لأمن المعلومات المنعقد بالدوحة في نوفمبر 2016.

ثانيا : المراجع الأجنبية

- 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 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.
- Cezar PETA: cyber security – current topic of National security Public security studies, volume II, Issue 2013.
- 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).
- Kasperon (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).
- Sieber Ulrich, computer crimes and other crimes related to information technology. I.R.P.. 1994. Vol.
62.

- Scott J. Shackelford, JD, PhD, Scott Russell, JD & Andreas juehn, Defining cybersecurity Due Diligence under International law: lessons from the private sector.
- 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)

(القانون الأمريكي لأمن البيانات لعام 2014 - Data security Act 2014).

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".