كليـة الحقوق

الدراسـات العليـا

الحماية الإدارية لأمن المعلومات

دراسة تحليلية ـ مقارنة

تحت إشراف

الأستاذ الدكتور / صلاح الدين فوزي

أستاذ القانون العام – كلية الحقوق – جامعة المنصورة

محكم دولي – عضو اللجنة العليا للإصلاح التشريعي

وعضو المجمع العلمي المصري

إعداد الباحثة

علياء أنيس أبـو حجازي

١٤٤٢هـ، ٢٠٢٠م

الحماية الإدارية لأمن المعلومات

المقدمة:

ظهر حق تداول المعلومات، لأول مرة في الدستور المصري عام ٢٠١٢ حيث نصت المادة (٤٧) منه على أن " الحصول على المعلومات والبيانات والإحصاءات والوثائق والإفصاح عنها وتداولها، حق تكفله الدولة لكل مواطن بما لا يمس حرمة الحياة الخاصة، وحقوق الآخرين ولا يتعارض مع الأمن القومي وينظم القانون قواعد إيداع الوثائق العامة وحفظها وطريقة الحصول على المعلومات، والتظلم من رفض إعطائها وما قد يترتب على هذا الرفض من مساءلة".

ويؤخذ على هذا النص الغموض فيما يتعلق بمصطلح الأمن القومي " حيث يرسم القانون الحدود المسموح بها الحصول على المعلومات بما يتلاءم مع الأمن القومي، وتخضع جميع الهيئات الحكومية لحق حجب المعلومات عن العامة لحماية الأمن القومي، بيد أن المعنى المبهم لمصطلح " الأمن القومي " يعطي فرصة لتبرير حجب جميع المعلومات. فالعقود التي تبرمها الحكومة ليس لها علاقة بالأمن القومي، وخطط التنمية العمرانية ليس لها علاقة بالأمن القومي وهذا الإبهام من شأنه أن يخلق ثغرة يتهرب بها صناع القرار من المساءلة.

أما في دستور عام ٢٠١٤ فقد تم إلغاء الشروط المقيدة لحق الحصول على المعلومات المساس بالحريات الخاصة، وحقوق الآخرين، والتعارض مع الأمن القومي من نص المادة (٦٨) التي أحالت كل هذا للقانون، كما تم إضافة نص يلزم مؤسسات الدولة بحفظ وتأمين الوثائق حيث تنص المادة (٦٨) من هذا الدستور على أن " المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب والإفصاح عنها من مصادرها المختلفة حق تكفله الدولة لكل مواطن وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها وقواعد

إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمدًا، وتلتزم مؤسسات الدولة بإيداع الوثائق الرسمية بعد الانتهاء من فترة العمل بها بدار الوثائق القومية، وحمايتها وتأمينها من الضياع أو التلف، وترميمها ورقمنتها بجميع الوسائل والأدوات الحديثة، وفقًا للقانون".

والتطور السريع لتقنيات الحاسب كان له آثاره الملحوظة على أمن الحاسبات سوءا سلبًا أو إيجابًا، وهذا التطور السريع في غالب الأحوال أسرع من أن تتم ملاحقته بواسطة خبراء أمن الحاسبات لتغطية الثغرات التي قد تنشأ عن النظم الجديدة الأكثر تعقيدًا مما يتسبب في وجود فجوة تقنية بين السلاح التقني المستخدم في انتهاك المعلومات وبين الأسلحة المضادة التي يلجأ إليها خبراء أمن المعلومات وهذه الفجوة ليست في صالح أمن المعلومات وإحكام الحماية ضد انتهاكها.

وحيث أنه لا يمكن الفصل بين أمن المعلومات وخصوصيتها فإذا كان الأمن المعلوماتي هو المفهوم الواسع الذى تندرج في ظله كافة أوجه حماية النشاط المعلوماتي وأهمها حماية خصوصية المعلومات باعتبارها أهم وجه من أوجه الأمن المعلوماتي، لذا فإننا سوف نتعرض للحماية الإدارية لأمن المعلومات من خلال حماية الخصوصية المعلوماتية، وعليه ينقسم هذا البحث إلى ثلاثة مباحث:

المبحث الأول: الحماية الإدارية لخصوصية المعلومات في الولايات المتحدة.

المبحث الثاني: نظام مفوض المعلومات.

المبحث الثالث: الحماية الإدارية للمعلوماتية في مصر

المبحث الأول

الحماية الإدارية لخصوصية المعلومات في الولايات المتحدة الأمريكية

يعتبر القانون المنظم لحريات الرأي هو الوسيلة التي تعبر عن موقف المشرع من الحق في الحوار العام المؤسس على تكوين الأفكار وتبادلها والإقناع بها بموضوعية بهدف تنظيمها[١]، ولا يوجد في الولايات المتحدة الأمريكية قانون شامل للحق في الخصوصية المعلوماتية يستطيع أن يغطي كافة أنشطة جمع المعلومات، واستخدامها، ومعالجتها سواء على المستوي الحكومي، أو القطاع الخاص، وتعتمد التشريعات الحالية على طبيعة المعلومات التي تجمع، ومن يقوم بجمعها وما هي طبيعة الاستخدامات التي سيتم توجيهها إليها [٢].

والحق في الخصوصية على الإنترنت لا يتم إثارته إلا عند التعامل مع الحكومة حيث أنه بعد الدخول على شبكة الإنترنت فإن سياسة الخصوصية للموقع، هي التي تحكم العلاقة بين المستخدم وبين مشغل الخدمة بموجب شروط وأحكام الخصوصية الموجودة ضمن سياسة الخصوصية.

وتعتبر من أهم التشريعات الفيدرالية التي قررت ضمانات إدارية للخصوصية المعلوماتية في الولايات المتحدة، قانون حرية المعلومات الصادرة عام ١٩٦٦ (FOIA)، والذى خول كل شخص الحق في طلب الوصول إلى المعلومات المسجلة لدي الوكالات الفيدرالية الحكومية وتشترط الوكالات الفيدرالية للكشف عن تلك السجلات طلب مكتوب من صاحب الحق في الوصول للمعلومات باستثناء الحالات التي حددها

---

(١) د. حيدر محمد حسن الوزان، حماية حرية الرأي في مواجهة التشريع، دار النهضة العربية، القاهرة، ٢٠١٧، ص١٨.

(2) for acomprehensive review of US privacy statues, see Roberl smith, compilation of state & federal privacy laws (privacy Journal 1992). http://www.ntia.doc.gove/ntiahome/privwhitepaper.html.

القانون، وتعتبر تلك المعلومات مصونة ومحمية من الكشف عنها وتلك الاستثناءات تندرج في إطار الحماية القانونية الإدارية للحق في الخصوصية وتتولى لجنة التجارة الاتحادية الإشراف على تنفيذها وتشمل هذه المعلومات[1].

- المعلومات التعليقة بالدفاع الوطني والعلاقات الأجنبية الخارجية.
- القواعد والأنشطة الداخلية للوكالات الأجنبية.
- الأسرار التجارية وغيرها من المعلومات التجارية السرية.
- الاتصالات داخل الوكالات أو خارجها التي تحميها امتيازات قانونية.
- المعلومات المتعلقة بمسائل شخصية.
- بعض المعلومات التي تجمع لأغراض تنفيذ القانون
- معلومات تتعلق بالإشراف على المؤسسات المالية.
- المعلومات الجيولوجية والآبار.

وهناك ثلاثة استثناءات تتعلق بالأمن القومي وجهات إنفاذ القانون.

ومن الجدير بالذكر أن قانون حرية المعلومات الفيدرالي FOIA لا يسرى على الكونجرس، أو المكاتب المركزية للبيت الأبيض ولا يطبق أيضا على السجلات الموجودة لدي الحكومات المحلية للولايات المتحدة، ويجوز عند طلب الاطلاع على تلك الملفات أن يتم تقديم طلب إلى المدعي العام لتلك الولاية أو المدعي العام الفيدرالي للوصول إلى تلك السجلات [2].

وقد قررت المحكمة العليا في قضية وزارة العدل ضد لجنة حرية مراسلي الصحف US Department of Justice v.Reporters committee for

(1) http://www.justice.gove/oip/amended.foia-redlined-2010-pdf
(2) http://ww.justice.gove/oip/amended-foia-redlined-2010.pdf
last visited 12/1/2018

freedom of the press بالإجماع عند تطبيق الإعفاء بأن تقرير ما يشكل تعديًا على الخصوصية ينبغي أن يعكس الهدف من قانون حرية المعلومات بفتح أعمال الوكالات الحكومية أمام المراقبة العامة، وأن القانون يركز بالفعل على حق المواطنين في معرفة ما تنوي الحكومة فعله، ويتمثل الهدف الرئيس لقانون حرية المعلومات في ضمان إعمال رقابة الرأي العام على أنشطة السلطة(١).

وقد حظر قانون الخصوصية الأمريكي الصادر عام ١٩٧٤ The privacy actالكشف عن أي معلومات مسجلة في أي نظام إلا بموافقة الشخص الذى تتعلق به هذه البيانات، وذلك باستثناء الحالات السالف ذكرها، ويتم مساعدة الأشخاص بالوسائل اللازمة من أجل الوصول إلى السجلات الحكومية، وتعديل تلك السجلات، وأيضًا تحديد الوكالات التي تمتلك تلك السجلات، كما وضع هذا القانون القواعد التي توفر الممارسة العادلة التي يجب أن تحكم جمع المعلومات الشخصية للأفراد واستخدامها وحفظها ونشرها، ويتم حفظها في قواعد بيانات أو معلومات خاصة بالوكالات الفيدرالية وهذه القواعد هي عبارة عن مجموعة من السجلات يتم وضعها تحت سيطرة وكالة تتمكن من الحصول على المعلومات من خلال اسم الشخص أو بعض الأدوات التعريفية بالفرد، ويفرض قانون الخصوصية على تلك الوكالات أن تقوم بإخطار عامة الناس بوجود سجلات للمعلومات عن الأفراد قبل تسجيل هذه المعلومات في قواعد البيانات(٢).

---

(1) U.S department of justice

(2) "The privacy ACT of 1974, 5 U.S.C. & 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies a system of records is a group of records under the control of agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual."
http://www.justice.gove/opcl/privstat.htm.

وقد قرر قانون الخصوصية سالف الذكر بعض المحظورات في هذا الشأن أهمها ما يلى[١]:

١) أي ضابط أو موظف في أي وكالة يقوم بحكم منصبه، أو موقعه الوظيفي بحيازة أو الوصول إلى سجلات الوكالات التي تحتوي معلومات تعريفية بالأفراد يحظر عليه الكشف عنها بموجب المادة ٥٥٢ من هذا القانون، كما يحظر عليه الكشف عنها بأي صورة لأي شخص، أو هيئة ليس من حقه استلامها.

٢) كما يحظر على أي ضابط أو موظف في أي وكالة أن يحتفظ عمدًا بالسجلات بدون الالتزام بمتطلبات الإخطار الواردة في الفقرة (e) (4) (D) من هذه المادة كما حدد القانون حالات للإعفاء من الاحتفاظ بالسجلات General Exemptions Central intelligence Agency (CIA).

وهي عبارة عن السجلات التي تحتفظ بها الوكالات، أو فروعها، وتتعلق بنشاطها الرئيس، بما في ذلك نشاط البوليس للتحكم في الجريمة، أو لمنعها، أو الحد منها أو القبض على المجرمين، وكذلك أنشطة النيابة العامة والمحاكم وغيرها وتشمل معلومات تعريفية عن المجرمين وعن الجرائم وأغراض التحقيق الجنائي وتقارير المخبرين والمحققين[٢].

---

(1) "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be.

1-To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties :

2-Required under section 552 of this title;

3-For aroutline use as defined in subsection (a) (7) of this section and described under subsection (e) (4) (D) of this section ;

(2) (J) General Exemptions

وهناك قانون إدارة أمن المعلومات

Federal information security management ACT (FISMA)

ويعتبر قانون إدارة أمن المعلومات الفيدرالية الصادر عام ٢٠٠٢ جزء من قانون الحكومة الإلكترونية الأمريكية لعام ٢٠٠٢ وهو يهدف إلى توفير إطار شامل لتعزيز ضوابط وشروط أمن المعلومات، وتحديد الموارد التي تساعد الوكالات الحكومية في تأمين المعلومات والحفاظ على خصوصيتها، وقد عرف هذا القانون مصطلح أمن

The head of any agency may promulgate rules, in accordance with the requirements cincluding general notice of sections 553 (b) (1), (2) and (3) (c) , and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c) (1) and (2), (e) (4) (A) through (F), (e) (6), (7), (9), (10), and (11) and (i) if the system of records is :

1-Maintained by the central intelligence agency; or

2-Maintained by an agency or component there of which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutor, courts, correctional, probation, pardon , or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature disposition of criminal charges sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (c) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553 (C) of this title , the reasons why the system of records, is to be exempted from a provision of this section.

المعلومات بأنه يقصد به حماية المعلومات ونظم المعلومات من الوصول غير المصرح به، أو الاستخدام، أو الإفصاح، أو التعطيل، أو التعديل، أو التدمير من أجل توفير النزاهة والسرية، كما فرض على الوكالات الاتحادية الالتزامات الآتية[١]:

- تعيين موظف يكون مديرًا مسئولًا عن خصوصية المعلومات في كل وكالة.
- تعيين مدير تنفيذي يكون مسئولًا عن الامتثال لأحكام القانون.
- تنفيذ برنامج لأمن المعلومات.
- تقديم تقرير عن مدي ملاءمة وفعالية سياسات الأمن المعلوماتي والإجراءات المتخذة والأنشطة.
- المشاركة في وضع تقييم سنوي مستقل عن برنامج أمن المعلومات.

وقد أوجب قانون إدارة أمن المعلومات الفيدرالي على الوكالات الاتحادية الالتزام بالضوابط المصممة لضمان سرية المعلومات المتعلقة بالنظام وسلامتها وتوافرها، كما يتعين على الوكالات الاتحادية الالتزام بالمعايير الفيدرالية في معالجة المعلومات وغيرها من المتطلبات التشريعية المتعلقة بنظم المعلومات الفيدرالية مثل قانون الخصوصية الصادر عام ١٩٧٤ [٢].

كما خول قانون إدارة أمن المعلومات الاتحادي (FISMA)

المعهد الوطني للمعايير و التكنولوجيا

National Institute of Standards and Technology (NIST)

سلطة تطوير المعايير والمبادئ التوجيهية التي تستخدم في تنفيذ وحماية أمن المعلومات وإدارة المخاطر.

---

(1) http://www.justice.gove/opcl/ federal information security management ACT

(2) https://www.gsa.gov/ agency financial report 2012.

وبعد أثنى عشر عامًا تم تعديل قانون إدارة أمن المعلومات الفيدرالي (FISMA) من خلال قانون تحديث أمن المعلومات الاتحادية Federal Information security modernization ACT الصادر عام ٢٠١٤ والذى يعزز تحديث الممارسات الأمنية الاتحادية في مواجهة المخاطر الأمنية الحالية.

وقد ألزم هذا القانون الوكالات الاتحادية بإخطار الكونجرس بالحوادث الأمنية الرئيسة خلال سبعة أيام، ويكون مكتب الشئون الإدارية مسئولًا عن وضع توجيهات بشأن ما يشكل حادثًا رئيسًا [1].

ومن الجدير بالذكر أن هذه التشريعات تحكم فقط عملية كشف المعلومات الشخصية التعريفية ولكنها لا تتحكم في جمع المعلومات أو استخدامها مما يعرض الحق في الخصوصية على الإنترنت لخطورة كبيرة لاسيما وأن الإنترنت قد جعل إمكانية جمع المعلومات الشخصية أمرًا ميسورًا وبأقل التكاليف ويمكن تحليلها ونقلها وإعادة استخدامها.

الحماية الإدارية للخصوصية المعلوماتية :

ذهب الفقه الأمريكي إلى ترك الرقابة على نظم المعلومات للقواعد العامة دون حاجة لإنشاء جهة إدارية تتولى هذه المهمة، أي أن الولايات المتحدة الأمريكية لم تأخذ بالنظام الفرنسي الذى يعتمد على وجود لجنة تتولى مهمة حماية الخصوصية (اللجنة الوطنية للمعلوماتية والحريات) أو النظام الألماني الإستشاري الذى يأخذ بنظام مفوض المعلومات، ولكنها تعزز، وتشجع ما يعرف بالتنظيم الذاتي (Self-Regulation)

(1) https://www.tenable.com/blog/
The federal information security modernization act of2014

فتعتمد الولايات المتحدة الأمريكية في الحماية الإدارية للخصوصية المعلوماتية على القواعد العامة وعدم وجود جهة إدارية محددة لحماية الخصوصية[١].

والتنظيم الذاتي هو عبارة عن نظام هدفه الأساسي التأكيد على المسئولية الفردية، ويتطلب زيادة الوعي بأهمية الحفاظ على الخصوصية أثناء التواجد على شبكة الإنترنت كما يحتاج إلى مستوي تعليمي يمكن الفرد من الإلمام بأساليب عمل البرامج ومكونات الحاسب الآلي، وقراءة كتيبات التعليمات، وشاشات المساعدة، كما يتعين عليه أن يقرأ سياسة الخصوصية لكل موقع أو شركة تتولى جمع معلومات، ويوجد برنامج أمريكي يقيم مواقع الإنترنت على أساس كفاية حمايتها للحق في الخصوصية الفردية، ومواقع الإنترنت التي توفر حماية كافية للخصوصية الفردية تحصل على حق عرض شعار الأمان الإلكتروني (E.trust) وهو ما يعنى أن الموقع يقوم بإتباع سياسة الخصوصية التي تعزز حماية المعلومات الشخصية للمستخدمين وعدم نشر تلك المعلومات وعدم استخدامها في غير الغرض الذى جمعت من أجله ومن أشهر هذه المواقع موقع جوجل (Google) وفيس بوك (Fecebook) [٢].

وقد استخدمت لجنة التجارة الفيدرالية (FTC) القسم الخامس من قانونها لتوجيه الاتهام للشركات التي فشلت في الامتثال لسياسات الخصوصية الخاصة بها، أو فشلت في حماية البيانات التي تم جمعها ومن الجدير بالذكر أن قانون لجنة التجارة الفيدرالية لا يتطلب صراحة أن يكون لدي الشركة سياسة خصوصية أو أن تكشف عنها، بيد أنه إذا كشفت الشركة عن سياسة الخصوصية فيتعين عليها الالتزام بها، وقد اعتبرت اللجنة أي

---

(١) د/ عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠، ص١٠٠.

(٢) د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، ٢٠١٢، ص٦٢٨.

شركة تقوم بتغيير سياسة الخصوصية بأثر رجعي فإن مسلكها هذا يعد انتهاكًا لقانون لجنة التجارة الاتحادية [١].

وقد وقع الرئيس ترامب في أبريل ٢٠١٧ مشروع قانون يلغى مجموعة من أنظمة الخصوصية وأمن البيانات لمزودي خدمة الإنترنت واسعة النطاق والتي اعتمدتها لجنة الاتصالات الاتحادية في الأشهر الأخيرة من إدارة أوباما حيث كانت لجنة الاتصالات الفيدرالية قد اعتمدت قاعدة الخصوصية لمزودي خدمات الإنترنت واسعة النطاق في نهاية شهر أكتوبر ٢٠١٦ بعد أن أقرت بتطبيق المبادئ التقليدية لحماية الخصوصية على خدمات الاتصالات في القرن الواحد والعشرين والتي تقدمها شبكات النطاق العريض.

وقد وضعت لجنة التجارة الفيدرالية (FTC) توصيات وإرشادات بشأن حماية الخصوصية في الإنترنت (on line) من أجل ضمان مستوي معين من الممارسات العادلة لأنشطة استخدام المعلومات، وكذلك إصدار تشريعات لمواجهة التحديات التي تواجه الخصوصية في بيئة الإنترنت، وتشجيع الجهات الحكومية والخاصة على تبنى سياسات الخصوصية التي تلتزم بالمعايير القياسية لحماية الخصوصية، وكذلك تقييم جهود التنظيم الذاتي من أجل تعزيز الحقوق الفردية[٢].

ومن الجدير بالذكر أن المؤتمر السنوي الثالث الذى تنظمه لجنة التجارة الفيدرالية (FTC) والذي عُقد في فبراير عام ٢٠١٨، وضم العروض المقدمة من

---

(1) (J) Leuan, Data protection in the united states: overview, 1 Jul, 2017, last visited 16 Feb 2018., available at: https://content.next.westlaw.com

(2) See federal trade commission, self regulation and online privacy : A Report to Congress (July 1999) (Concluding that greater in Centives were needed to encourage self- Regulation and ensure wides pread implementation of the basic privacy principles) available at http://www.ftc.gov/privacy/reports.htm last visited 17 Feb 2018.

عشرين باحثًا على مدار أربعة جلسات، وقد شملت الدورة الأولى البحوث المتعلقة بجمع المعلومات الخاصة وتسريبها، وتضمنت الدورة الثانية تفضيلات المستهلكين وتوقعاتهم وسلوكياتهم، في حين احتوت الدورة الثالثة على عروض تتعلق بالاقتصاد والأسواق والتجارب، وركزت الجلسة الأخيرة على البحوث المتعلقة بأدوات إدارة الخصوصية[١].

وقد اشترطت لجنة التجارة الاتحادية (FTC) على الجهات الحكومية والقطاع الخاص تبنى مبادئ رئيسة لضمان خصوصية البيانات، وضمان الممارسات العادلة لأنشطة جمع واستخدام البيانات قبل إنشاء نظام معلوماتي أو موقع إلكتروني، ولذا فإن أغلب الشركات العالمية العاملة في مجال الإنترنت تضع تلك الشروط ضمن سياستها للخصوصية مثل (جوجل، وفيس بوك، وتويتر، وياهو.... الخ) وهذه المبادئ هي مبدأ الإخطار، ومبدأ الاختيار، ومبدأ الحق في الوصول والاطلاع، ومبدأ الأمن [٢].

وهي المبادئ الأساسية التي تحكم الممارسات العادلة والنزيهة في نطاق خصوصية المعلومات، وحماية البيانات داخل البيئة الرقمية وتتمثل في الآتي [٣] :

الإبلاغ والإخطار Notice : ويقصد به أنه يتعين إبلاغ مستخدمي المواقع من قبل مزود الخدمة أو الموقع عما إذا كان الموقع أو مقدمي الخدمة ينويان جمع بيانات شخصية واستخدامها، ونطاق جمع هذه البيانات، وكيفية استخدامها، ويستلزم الإخطار من المتحكم في النظام الآلي الأمريكي أن يلتزم بإخطار الأفراد بالغرض من جمع المعلومات، أو الاستخدامات المتوقعة لهذه المعلومات، والآثار المترتبة على تقديم أو حجب المعلومات،

(1) Federd Trade Commission Releases Agenda for privacy con 2018. available at https://www.ftc.gov/news-events/press/2018/02/ftc.
(2) Federal Trade commission, fair Informtion practices in the Electronic Marketplace: A Report to congress May 2000.
available at http://www.ftc/gov/privacy/reports.htm.
(3) http//www.epic.org/reports/surfer-beware.html

عـن الأفـراد، والإجـراءات الواجـب اتخاذهـا مـن أجـل الحفـاظ علـى سـلامة وجـودة المعلومات.

ويقصـد بالخصوصـية: أن يـتم الحصـول علـى المعلومـات الشخصـية، والكشـف عنهـا، واستخدامها بطريقة تتفق مع احترام خصوصية الفرد، أما سلامة المعلومات فهي تعنى عدم تغيير أو إتلاف المعلومات الشخصية، في حين يقصد بالجودة أن تكون المعلومات دقيقـة، وفـى الوقـت المناسـب، وملاءمـة للغـرض الـذى تـم جمعهـا مـن أجلـه، وحقـوق الإنصـاف يقصـد بهـا التنفيـذ الحكمـي وحـل الشـكاوي، والوسـاطة والتحكـيم بشـكل غيـر رسمي، وهذه الشروط تطبق على جميع أنشطة معالجة المعلومات(١).

- الاختيار choice : ويتطلب هذا المبدأ التزام الشركات مالكة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بشأن استخدام بياناته في غير الغرض الذى جمعت من أجله.
- الوصول والاطلاع على البيانات Access : ويقتضى هذا المبدأ تمكين المستخدمين من الوصول إلى بياناتهم والاطلاع عليها والتأكد من صحتها وتحديثها.
- الأمن Security : ويتعلق هذا المبدأ بالتزام الجهات المسئولة عن جمع البيانات (المواقع ومزودي الخدمة) بمراعاة معايير الأمن الواجب تطبيقها لضمان سرية البيانات وسلامة استخدامها، ومنع الوصول غير المصرح به لها، وتشمل هذه الوسائل كلمات السر، والتشفير، وغيرها من وسائل أمن المعلومات.
- تنفيذ القانون EnForcement : ويقصد به وضع آليات مناسبة يجب اعتمادها لفرض الجزاءات على الجهات التي لا تلتزم بالمبادئ سالفة الذكر، وما يرتبط بها من ممارسات عادلة تتعلق بجمع البيانات الشخصية في البيئة الرقمية(٢).

---

(1) Rebort Bork, "Neurnal Principles and some first Amendment problems", Indiana law Jurnal, Vol 47 (fall 1971), p.23
(2) http://www.ftc.gov/privacy/reports/htm.

ونخلص من كل ذلك إلى أن النظام الأمريكي يولى الأهمية في نظرته للضمانات الإدارية لحماية الخصوصية إلى حرية التعبير، وحرية تدفق المعلومات على حساب الخصوصية المعلوماتية، وعلى خلاف الاتجاه الأمريكي الذي يرفض التدخل الحكومي فإن التوجيه الأوروبي يلزم الأشخاص الذين يرغبون في جمع المعلومات الشخصية ومعالجتها واستخدامها وتخزينها ونشرها، بإخطار الجهة الإدارية المسئولة عن حماية البيانات كما هو الشأن بالنسبة للجنة الوطنية للمعلوماتية والحريات في فرنسا وفى هذا الخصوص من الأهمية بمكان الإشارة إلى حكم المجلس الدستوري رقم ٢٠١٦/٦١١ والذى قضى فيه بعدم دستورية المادة ٢-٥-٢-٤٢١ من قانون العقوبات الفرنسي الصادر في ٣ يونيه ٢٠١٦ والتي تعاقب بالسجن لمدة سنتين وغرامة قدرها ٣٠ ألف يورو كل من يتصل بالجمهور عن طريق الإنترنت ويستخدمه في تقديم رسائل أو صور تحرض بطريق مباشر، أو غير مباشر على ارتكاب أعمال إرهابية إذا تضمنت صور أو تصريحات تبين ارتكاب هذه الأفعال التي تنطوي على أعمال عنف متعمدة.

ولا تسرى هذه المادة على الممارسات العادية التي تتم بحسن نية، أو التي تدخل في إطار البحث العلمي، أو التي يتم تنفيذها من أجل خدمة الإثبات في المحكمة.

وقد دفعت صاحبة الشكوى بأن الأحكام المطعون عليها تتجاهل حرية الاتصال وحرية الرأي طالما أنها تعاقب على مجرد الاتصال بالجمهور عن طريق الإنترنت دون أن تشترط التأكد من توافر النوايا غير المشروعة (القصد الجنائي) لدي الشخص المتصل ومن شأن هذه الأحكام أن تتعارض مع مبدأ شرعية الجرائم والعقوبات وتهدر القيمة الدستورية للقانون بسبب غموض المصطلحات المستخدمة.

وفضلًا عن ذلك فإن مبدأ المساواة سيساء فهمه من جانبين، فمن ناحية لا يسمح القانون إلا لبعض الأشخاص بالوصول إلى هذه المحتويات بسبب مهنتهم، ومن ناحية أخرى فإن الاتصال بالمحتويات التي تثير ارتكاب جرائم إرهابية لا تخضع لعقوبة إلا

عندما تجري على الإنترنت، ومن ثم استبعاد أشكال الدعم الأخرى، وأخيرًا فإن النصوص المطعون عليها تنتهك مبدأ افتراض البراءة لأن الشخص الذي يشارك في الاتصال المزعوم يفترض أنه يرتكب أعمالا إرهابية وهي نفس الأسباب التي أستند إليها المتدخل في الدعوى حيث ذهب إلى أن النصوص المطعون عليها تنتهك حرية الاتصال والرأي ومبدأ شرعية الجرائم العقوبات في حين نصت المادة (١١) من إعلان حقوق الإنسان والمواطن الصادر عام ١٧٨٩ على أن " التواصل الحر للآراء هو واحد من أثمن حقوق الإنسان : فكل مواطن يستطيع أن يتكلم، ويكتب ويطبع بحرية شريطة عدم إساءة استخدام هذه الحرية في الحالات التي يحددها القانون" وفى الحالة الراهنة لوسائل الاتصال وفيما يتعلق بالتطور الواسع لنطاق خدمات الاتصال العام عبر الإنترنت وأهمية هذه الخدمات للمشاركة في الحياة الديمقراطية والتعبير عن الأفكار والآراء وهذا الحق يتضمن حرية الوصول إلى هذه الخدمات، مما يجعل نص المادة سالفة الذكر تتعاض مع هذا الحق [1].

الحماية القضائية الأمريكية :

تقوم الحماية القضائية للحق في الخصوصية في النظام الأمريكي على أساس النظام الأنجلوسكسوني أو نظام القضاء الموحد الذى يعتمد على وجود جهة قضائية واحدة هي جهة القضاء العادي التي تتولى الفصل في كافة المنازعات سواء تلك التي تنشأ بين الأفراد، أو بينهم وبين الإدارة، ويطبق القضاء العادي على المنازعات الإدارية ذات القواعد القانونية التي تحكم منازعات الأفراد ويوجد هذا النظام في الولايات المتحدة الأمريكية، وإنجلترا، واستراليا، والهند، ونيوزيلاندا أي أن الولايات المتحدة الأمريكية لا تعرف القضاء الإداري، وإنما تختص المحاكم العادية بنظر جميع المنازعات سواء كانت

(1) C.C.,10 fevrier 2017, n° 2016-611 , disponible à
Sit: www.conseil.constitutionnel.fr.

إدارية، أو مدنية ويمارس القضاء الأمريكي سلطات واسعة في مواجهة الإدارة لاسيما إصدار الأوامر والنواهي لها وتعديل تصرفاتها[1].

ويعتبر التظلم من القرار الإداري أو طلب إعادة النظر فيه من الحقوق الدستورية وفقا للنظرية الأمريكية التي تعتنق مبدأ سمو القضاء، وهذه النظرية تقر بأن المشرع لا يملك أن يجرد المحاكم من سلطات خولت لها بواسطة الدستور، فالجهاز الإداري لا يمكنه حرمان الفرد من حقوقه المكتسبة أو المزايا المخولة له بدون منحه فرصة تمكنه من إعادة النظر والفحص الجديد بواسطة القضاء، ولا ريب في أنه لا يمكن تطبيق الضمانات الدستورية المقررة للحقوق الشخصية على الأجهزة الإدارية التي لا تملك حقوق طبيعية، بيد أن الأجهزة الإدارية يمكنها إثارة مسائل دستورية أخرى بخلاف ما يمكن إثارته بواسطة الأشخاص الطبيعية [2].

ويتجلى دور التوجيه الأوروبي لحماية البيانات والمعلومات الشخصية لعام ١٩٩٥ إبان تقييم الحماية الإدارية الأمريكية حيث أوجبت المادة (٢٥) منه على الدول الأعضاء سن قوانين تحظر نقل البيانات الشخصية إلى الدول غير الأعضاء التي لا تحقق مستوي كافيا من الحماية، وقد نص التوجيه على أن كفاية الحماية التي توفرها الدول المنقول إليها البيانات يتم تقييمها في ضوء كافة الظروف المحيطة بنقل البيانات والتي تتضمن طبيعة البيانات، والغرض والمدة الزمنية للمعالجة المقترحة، والأحكام التشريعية

(١) أ.د/ محمود أبو السعود حبيب، القضاء الإداري، مطبعة الإيمان، ٢٠٠٦، ص ١٠.
(٢) د/ السيد خليل هيكل، القانون الإداري الأمريكي الجزء الثاني، كيفية الرقابة على القرار الإداري الأمريكي، مجلة العلوم الإدارية، السنة السادسة عشر، العدد الثاني، أغسطس ١٩٧٤، ص ١٣١.

العامة في الدولة المنقولة إليها البيانات، والقواعد المهنية التي يجري الالتزام بها في تلك الدولة [1].

وغنى عن الذكر أن هذا المسعى يتفق مع التوجه الأوروبي للخصوصية كحق من حقوق الإنسان، كما أنه ضروري لحماية خصوصية المواطنين الأوروبيين بصورة عالية في اقتصاد معلومات عالمي، بيد أنه يتم انتقاد المادة (٢٥) من التوجيه الأوروبي سالف الذكر باعتبارها تسعى لترسيخ الحماية الأوروبية لخصوصية المعلومات كمعيار عالمي، ونظرًا لصعوبة فصل البيانات التي يتم جمعها داخل أوروبا عن البيانات التي يتم جمعها في أي مكان آخر، فإن التوجيه يطالب بصورة فعالة أن توفق أنشطة الأعمال متعددة الجنسيات جميع أنشطتها الخاصة بمعالجة البيانات مع قانون الاتحاد الأوروبي، فحتى أنشطة الأعمال التي لا يتم مزاولتها في أوروبا يمكن أن تتعارض مع التوجيه الأوروبي إذا كانت تقوم بجمع البيانات الشخصية ومعالجتها ونشرها من خلال شبكات متعددة الجنسيات.

وقد ترتب على ذلك أن أنشطة الأعمال الأمريكية التي لها مصالح في البيانات الشخصية التي يتم جمعها، أو تخزينها، أو معالجتها في أوروبا لاسيما أنشطة الأعمال الأمريكية التي تقوم بعمليات اقتصادية في أوروبا، أصبحت تخشى من عدم قدرتها على نقل تلك البيانات بصورة مشروعة، مما دفع الولايات المتحدة وأوروبا إلى توقيع اتفاقية سيف هاربور من أجل تنسيق مستويات الحماية فيما بينهما.

وقد توصلت الولايات المتحدة الأمريكية والاتحاد الأوروبي في عام ١٩٩٨ إلى مشروع طموح لتطوير برنامج تستطيع من خلاله الشركات متعددة الجنسيات وشركات

(1) Directive 95/46/ EC of the European Parliament and the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

البرمجيات المؤسسة بالولايات المتحدة التكيف مع القواعد الصارمة المتعلقة بتعليمات الخصوصية التابعة للاتحاد الأوروبي، عند نقل البيانات الخاصة بالمواطنين الأوروبيين حيث كان مسعى برنامج الاتفاقية – اتفاقية سيف هاربور Safe Harbor هو التوصل إلى توافق بين الاتحاد الأوروبي والولايات المتحدة في حالة قيام أي شركة أو مؤسسة بالولايات المتحدة باستخدام، أو نقل البيانات الخاصة بالمواطنين الأوروبيين من أو إلى الولايات المتحدة [1].

وفى ١٢ يناير ٢٠١٧ أعلن عضو المجلس الاتحاد السويسري عن موافقة سويسرا، والولايات المتحدة الأمريكية على إطار درع الخصوصية باعتباره آلية قانونية صالحة للاستجابة للمتطلبات السويسرية عند نقل البيانات من سويسرا إلى الولايات المتحدة ويحل إطار درع الخصوصية privacy shield محل اتفاقية سيف هاربور والسبب في فشل اتفاقية سيف هاربور هو عدم دقة آليات التنفيذ الداخلية والخارجية حيث عينت اتفاقية سيف هاربور مفوضية التجارة الفيدرالية كسلطة تنفيذية خارجية للبرنامج، وفى عام ٢٠٠٤ لم تقاضى، مفوضية التجارة الفيدرالية شركة واحدة تخرق حماية حقوق مواطني الاتحاد الأوروبي وفقًا لاتفاقية سيف هاربور، وقد أدى الافتقار للتنفيذ إلى جعل مواطني الاتحاد الأوروبي، والذين كانوا يعتمدون على آليات التنفيذ التي تقوم بها وكالات الخصوصية ويقومون بأنفسهم بتقديم تقارير عن اختراق اتفاقية سيف هاربور، ومن ذلك على سبيل المثال اختراق بيانات شركة ما والذى يؤدي إلى سرقة آلاف الهويات، وتختلف القوانين الخاصة بإشعارات الخصوصية كلية، والأسوأ من ذلك أنه بموجب اتفاقية سيف هاربور لا تتطلب الشركة إشعار مواطني الاتحاد الأوروبي الواقعين تحت

(1) 2000 / 520 / EC : Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European parliament and of the council (Safe harbor principle).
available at: https//2016.Export.gov/safeharbor,lastvisited10/3/2018

تـأثير الخـرق، حيث قد يتم فقد البيانـات الخاصـة بمـواطن مـن الاتحـاد الأوروبـي، أو يـتم بيعهـا، وقد تبين للمـواطن الأوروبـي أنـه مـن المستحيل تحديد الشـركة التـي تعد مصـدرًا للخـرق، وبـدون معرفـة الشـركة الضـحية لا يسـتطيع المـواطن الأوروبـي الاسـتفادة مـن قوانين الحماية الخاصة باتفاقية سيف هاربور، وترتب علـى فشل الجانـب الأمريكـي أكثر مـن مـرة فـي حمايـة الخصوصـية (كمـا هـو الحـال فـي دمـج الشـبكات عـن طريـق موقـع جوجل) إلـى انهيـار الثقـة بين وكـالات التنفيذ الأمريكيـة والأوروبيـة حيث رأي الجانـب الأوروبي أن الشـركات الأمريكيـة قد فشـلت فـي الالتـزام بفحـوى ومضـمون اتفاقيـة سيف هاربور[1].

ويتبين علـى هدي مـا تقدم أن اتفاقيـة سيف هـاربور لـم تحقق للاتحـاد الأوروبـي الحماية الفعالة للخصوصية.

(1) "Un like the us approach to privacy protection , which relies on industry specific legislation, regulation and self – regulation, the European Union relies on comprehensive privacy legislation".
Available at : http://www.export.gov/safeharbor/index.asp

المبحث الثاني : نظام مفوض المعلومات

لقد تبنى النظام القانوني الألماني نظام مفوض المعلومات حيث عهد القانون الألماني الاتحادي الصادر عام ١٩٧٧ بمهمة الرقابة على تطبيق القانون إلى مفوض نظام المعلومات الذى يختص بحماية البيانات، وقد حدد ثلاثة أنواع من المفوضين، فيوجد مفوض لحماية البيانات المعالجة بمعرفة الحكومة، وهناك مفوض آخر يختص بحماية البيانات التي يتم معالجتها بمعرفة الشركات والهيئات الخاصة لتحقيق أغراض متعلقة بها، كما يوجد مفوض ثالث مسئول عن حماية البيانات المعالجة بواسطة منظمات خاصة لحساب جهة مغايرة [١].

وقد تبنت ولاية هيس الألمانية فكرة تعيين مفوض لنظم المعلومات يختص بحماية الأشخاص في هذا الشأن، كما يختص برقابة عمليات بنوك المعلومات الشخصية، ويستطيع كل شخص يشعر بأن أحد نظم المعلومات يمس حرمة حياته الخاصة أن يتقدم بشكوى إلى المفوض، ويتولى المفوض بحث الشكوى مع البنك من أجل الوصول إلى حل ودي بين الطرفين وتحرص بنوك المعلومات على الحل الودي من أجل تفادي الدعاوى القضائية[٢].

وتتمثل مزايا نظام مفوض نظم المعلومات في بساطته، وضآلة الأعباء المالية التي يحملها الخزانة العامة، كما أن فعاليته تعتمد على شخصية من يتولى هذا المنصب والذى يشترط فيه أن يكون أهلًا للثقة والاحترام، مما يساعد على قيامه بمهمته، ويدعم من قيمة ما يصدره من قرارات وتوصيات، ولكن يعيب هذا النظام أن تدخل المفوض لحماية البيانات الشخصية لا يكون إلا بناء على شكوى من صاحب الشأن، ومن ثم لا يجوز له

---

(١) أ.د/ عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، مرجع سابق، ص ١٠١.

(٢) د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت، مرجع سابق، ص ٦٤٠.

أن يقوم من تلقاء نفسه بالتحري عن مدي احترام القانون، كما أن المفوض لا تتوافر لديه في الغالب الخبرة الفنية اللازمة للتأكد من أعمال قواعد السلامة والحماية[١].

وفى كندا يتولى مفوض الخصوصية الكندي توفير الحماية الإدارية للخصوصية وقد تم إنشاء تلك الوظيفة بموجب قانون حماية حقوق الإنسان الكندي (الجزء الرابع) Candia Human Rights ACT

وبموجب المادة ٥٧ منه والتي كانت تجعل تعيين المفوض بمعرفة وزير العدل بناء على ترشيح يقدم من رئيس اللجنة الكندية لحقوق الإنسان، أما الآن فأصبح مفوض الخصوصية Privacy Commissioner يتم تعيينه بقرار من الحاكم بعد الموافقة عليه من مجلس الشيوخ والعموم وتكون ولايته لمدة سبع سنوات وفقًا للمادة ٥٣ من قانون الخصوصية الكندي[٢] Privacy act الصادر عام ١٩٨٥.

ويعتبر موظف برلماني يقدم تقاريره مباشرة إلى مجلسي الشيوخ والعموم ويختص مكتب مفوض الخصوصية الكندي office of the privacy commissioner of canada. والذى يعرف اختصارًا (OPC) بالإشراف على تطبيق قانون الخصوصية الكندري Privacy act والذى يغطي أنشطة معالجة المعلومات

(١) أ.د/ حسام الدين كامل الأهوانى، الحق في احترام الحياة الخاصة، مرجع سابق، ص ٢٠.

(2) Article 53 from privacy act "(1) The governor in Council shall, by commission under the Great seal, appoint aprivacy commissioner after consultation with the leader of every recognized party in the senate and House commons and approval of the appointment by resdution of the senate and house of comms tenure (2) Subject to this section, the privacy commissioner holds office during good behaviour for atem of saven years, but may be removed for cause by the Governor in council at any time on address of the senate and house of commons.
Available at : http://laws.lois.justice.gc.ca/eng/acts/p.21/page-8.html. Last visited 14/3/2018

الشخصية في الوزارات والوكالات الحكومية الفيدرالية، وكذلك قانون حماية المعلومات الشخصية والوثائق الإلكترونية [1] Personal information protection and electronic documents ACT (PIPEAD)

وهذا القانون يهدف إلى تعزيز التجارة الإلكترونية عن طريق حماية البيانات والوثائق الإلكترونية، والمعلومات الشخصية التي يتم جمعها، أو استخدامها أو كشفها في حالات معينة، وذلك من خلال توفير الوسائل الإلكترونية اللازمة للاتصال وتسجيل المعلومات والمعاملات الإلكترونية وهذا القانون يحدد اختصاصات مفوض المعلومات الكندي لحماية البيانات والخصوصية الإلكترونية[٢].

ويتولى مكتب مفوض الخصوصية الكندي تعزيز حماية الحق في الخصوصية للأفراد وهو يعمل كسلطة مستقلة عن الحكومة الكندية، ويتولى التحقيق في الشكاوي المقدمة من الأفراد سواء ضد الحكومة أو القطاع الخاص فيما يتعلق بقضايا الخصوصية وحماية البيانات الشخصية[٣].

(1) Personal Information protection and Electronic Documents Act (S.C.2000, C.5)
Available at http://www-lois.justice.gc.ca/acts/p-8.6/index.html
(2) An act to support that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the canada Evidence Act, the statudtory instruments Act and the statue revision Act".
Available at : http://laws-lois.justice.gc.ca/eng/acts/p-8-6/page-1.htm1 last visited 15/3/2018.
(3) http://www.priv.gc.ca/index-e.cfm.last visited 16/3/2018.

ويختص مفوض الخصوصية الكندي بما يلى[1] :

- التحقيق في الشكاوي المقدمة إليه، وتقديم تقارير، وتوصيات للمؤسسات الحكومية الفيدرالية، ومنظمات القطاع الخاص لمعالجة تلك الشكاوي وفقًا لكل حالة على حدة.
- متابعة الإجراءات القانونية والدعاوي التي لم يتم تسويتها أمام المحاكم الفيدرالية.
- التأكد من مراعاة الالتزامات الواردة في قانون الخصوصية الكندي Privacy act، وقانون حماية المعلومات الشخصية (PIPEDA) عن طريق إجراء فحص مستقل ومراقبة الأنشطة ونشر تقارير علنية في حالة وجود مخالفات.
- كما يقوم مفوض الخصوصية الكندي (OPC) بتقديم الاستشارات ومراجعة واستعراض تأثير الأنشطة الحكومية على الخصوصية وحماية البيانات.
- وأيضًا يتولى مفوض الخصوصية الكندي تقديم الخبرات للمساعدة في مراجعة واستعراض مشروعات القوانين التي تستهدف التطور التشريعي في البرلمان من أجل ضمان احترام حق الأفراد في الخصوصية.
- توجيه الأفراد الكنديين وأعضاء البرلمان والمنظمات إلى اتخاذ خطوات استباقية بشأن قضايا الخصوصية الناشئة والمستحدثة.
- التوعية بضرورة الالتزام بقوانين حماية الخصوصية عن طريق وضع آليات لحماية الحق في الخصوصية وتنفيذ الالتزامات القانونية من خلال الاشتراك مع المؤسسات الحكومية الفيدرالية واتحادات الصناعات، والأوساط القانونية والاتحادية، والجمعيات المهنية، وأصحاب المصالح الآخرين، ونشر مواد للتثقيف العام بشأن الخصوصية.
- تقديم الآراء القانونية ورفع الدعاوي القضائية لتفسير وتطبيق قوانين الخصوصية الفيدرالية.

---

(١) د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت، مرجع سابق، ص ٦٤٣، ٦٤٤.

- رصد الأنشطة التي تنتهك الخصوصية وتحديد قضايا الخصوصية التنظيمية التي تحتاج إلى معالجة.

وفى استراليا نجد مفوض خصوصية المعلومات الإسترالي هو المسئول عن إدارة وتنظيم الخصوصية The Australian privacy commissioner is the national privacy regulator ويخضع في أداء وظائفه لقانون الخصوصية الإسترالى الصادر عام ١٩٨٨ The Privacy act وتكون مهامه محددة وفقًا للقانون في مجالات معينة مثل تقديم المعلومات والمشورة حول الخصوصية وقانونها وتلقى الشكاوي والقيام بأنشطة تثقيفية بشأن الخصوصية.

كما يتولى المفوض مراقبة أمن ودقة المعلومات المحتفظ بها لدي الكيانات أو الهيئات، وفحص سجلات هذه الكيانات للتأكد من أنها لا تستخدم المعلومات في غير الأغراض المصرح بها، واتخاذ التدابير اللازمة لمنع الكشف غير المشروع عن هذه المعلومات، وكذلك فحص سجلات مفوض الضرائب للتأكد من أن المفوض لا يستخدم معلومات رقم الملف الضريبي في أغراض تخرج عن نطاق اختصاصه(١).

---

(1) Privacy Act 1988 "27 functions of the commissioner"
1-the commissioner has the following functions :
a)the functions that are conferred on the commissioner by or under :
(i) this Act; or
(ii) any other law of the common wealth;
a) the guidance related functions ;
b) the monitoring related functions ;
c) the advice related functions ;
d) to do anything incidental or conducive to the performance of any of the above functions.
1- The commissioner has power to do all tings necessary or convenient to be done for, or in connection with, the performance of the commissioner's functions.

ومكتب مفوض خصوصية المعلومات هو هيئة قانونية تعرف اختصارًا (OAIC)

The Office Of The Privacy Commissioner Is Astatutory Authority

---

2- Without limiting subsection (2), the commissioner may establish a panel of persons with expertise in relation to a particular matter to assist the commissioner in performing any of the commissioner's functions.

3- Section 38 of the Healthcare identifiers act – 2010, rather than section 12B of this act applies in relation to an investigation of an act or practice referred to in subsection 29 (1) of that Act in the same way as it applies to parts 3 and 4 of that Act. 28 guidance related functions of the commissioner.

1- The following are the guidance related function of the commissioner.

(a) Making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals;

(b) Making, by legislative instrument, guidelines for the purposes of paragraph (d) of Australian privacy principle b.3;

(c) Promoting an understanding and acceptance of :

(d) The Australian privacy principles and the objects of those principles; and.

(i) A registered APP code; and.

(ii) The provisions of part III A and the objects of those provisions; and

(iii) The registered CR code ;

(e) Undertaking educational programs for the purposes of promoting the protection of individual privacy.

2- The commissioner may publish the guidelines referred to paragraphs (1) (a) and (b) in such manner as the commissioner considers appropriate.

3- The educational programs referred in paragraph (1) (d) may be under taken by :

a. The commissioner; or

b. A person or authority acting on behalf of the commissioner.

4- Guidelines made under paragraph (1) (a) are not a legislative instrument.

Available at http://www.privacy.gov-au/index-php last visited 17/3/2018.

وهو يتبع رئيس الوزراء الاسترالي مباشرة مع الأخذ في الاعتبار أنه رغم أن مكتب مفوض الخصوصية يعتبر وكالة حكومية Government agency إلا أنه مستقل تمامًا في أداء وظائفه التنظيمية ووضع سياسات العمل الخاصة به وهو يهدف إلى تعزيز حماية الخصوصية في إستراليا، ويعمل على تطبيق قانون الخصوصية الصادر عام ١٩٨٨، والذى حدد الطريقة التي يمكن بها جمع المعلومات الشخصية، ومدي دقتها ووسائل تأمينها والحفاظ على سريتها، وكيفية استخدامها، أو الكشف عنها، ونص كذلك على حقوق الأفراد في الوصول إلى المعلومات، والحق في تصحيح المعلومات لدى المنظمات والهيئات الحكومية والخاصة التي تحتفظ بها(١).

وقد صدر عام ٢٠١٠ قانون مفوض المعلومات الإسترالي Australian information commissioner act2010 وقد خول هذا القانون لمفوض المعلومات السلطات اللازمة للقيام بكل ما هو ضروري لأداء الوظائف المنوطة به بموجب هذا القانون ويقوم مفوض المعلومات بأداء وظيفته بناء على معتقداته، وإذا قام مفوض المعلومات باستخدام السلطة المخولة له في مسألة معينة فإن ذلك لا يمنعه ولا يمنع مفوض الخصوصية من ممارسة ذات السلطة أو أداء ذات الوظيفة في مسألة أخرى أو مناسبة مختلفة(٢).

---

(1) The information privacy principles (IPPS) are the – base line privacy standards which the Australian and ACT government agencies need to comply with in relation to personal information kept in their records. Available at http://www.privacy.gov.au/law/act/ipp.

(2) Australian Information commissioner ACT 2010.

"11 funcations and powers of the freedom of information commissioner

1. The freedom of Information commissioner has the freedom of information functions.
2. The freedom of information commissioner may also perform the privacy functions.

وقد أجاز القانون سالف الذكر لمفوض المعلومات أن يفوض كتابة كل أو بعض مهامه، أو صلاحيته إلى عضو من موظفي مكتب المفوض الاسترالي للمعلومات وذلك باستثناء ما يلي:

أ) مهام مفوض المعلومات الممنوحة بموجب الفقرة السابعة (أ) (إبلاغ الوزير).

ب) إعداد التقرير المذكور في القسم ٣٠.

ج) إصدار مبادئ توجيهية على النحو المذكور في الفقرة الثامنة (هـ).

---

3. The freedom of information commissioner has power to do all things necessary or convenient to be done for or in connection with the performance of functions conferred by this section.
4. However, the following actions may only be taken with the approval of the information commissioner.
   a) The issue, variation or revocation of a guideline mentioned in paragraph 8 (e);
   b) The making of a report or recommendation under paragraph 8(f) to the minister about :
   (i) Proposals for legislative change to the freedom of information Act 1982 ; or
   (ii) Administrative action necessary or desirable in relation to the operation of that Act.
5. If the freedom of information commissioner must perform the function or exercise the power upon his or her own belief or state of mind (to the extent that the performance or exercise is dependent on the belief or state of mind of the information commissioner) ; and
   b) the function or power is taken to have been performed or exercised by the information commissioner, and.
   c) neither the information commissioner, nor the privacy commissioner, is prevented from performing the same function, or exercising the some power, on another, occasion (in relation to a different matter).
   Available at: https://www.legislation.gov.au/Details/ c2010A00052 last visited 20/3/2018.

د) الوظيفة المخولة له بموجب المادة (٥٥) فقرة (هـ) من قانون حرية المعلومات الصادر عام ١٩٨٢ (طلب مراجعة مواد القانون أمام المحكمة الفيدرالية الاسترالية).

ه) الوظيفية المخولة بموجب المادة ٥٥ فقرة (هـ) من قانون حرية المعلومات الصادر عام ١٩٨٢.

و) الوظيفة المخولة بموجب المادة ٥٥ فقرة (ق) من قانون حرية المعلومات سالف الذكر.

ز) الوظيفة المخولة بموجب المادة ٧٣ من قانون حرية المعلومات.

ح) الوظيفة المخولة بموجب المادة ٨٦ من قانون حرية المعلومات (الالتزام بالإخطار عند الانتهاء من التحقيق).

ط) الوظيفة المخولة بموجب المادة ٨٩ فقرة (ك) من قانون حرية المعلومات (إصدار إعلان مزعج لمقدم الطلب).

ي) إصدار مبادئ توجيهية بموجب المادة (١٧) من قانون الخصوصية الصادر عام ١٩٨٨.

ك) اتخاذ قرارات لأغراض المادة ٥٢ من قانون الخصوصية الصادر عام ١٩٨٨[1].

(1) 25Delegation by the Information commissioner the information commissioner may delegate, in writing, all or any of his or her functions or powers to a member of staff of the office of the Australian information commissioner other than the following:
(a) The information commissioner functions conferred by paragraph 7 (a) (reporting to the minister);
(b) Preparing the report mentioned in section 30;
(c) Issuing guidelines as mentioned in paragraph 8 (e) ;

وقد أنشأ الجزء الرابع من قانون مفوض المعلومات الإسترالي لجنة استشارية Information Advisory Committee مساعدة مفوض المعلومات في الأمور المتعلقة بأداء وظائفه وتتكون هذه اللجنة من مفوض المعلومات رئيسًا، وكبار موظفى الوكالات المعينين من قبل الوزير بالتشاور مع الوزراء المعنيين والأشخاص الذين يرى الوزير أنهم يحملون مؤهلات وخبرات مناسبة[1].

(d) The function conferred by section 55 H of the freedom of information act 1982 (referring questions of law in a review to the federal Court of Australia);
(e) The function conferred by section 55 k of the freedom of information Act 1982 (making a decision on an IC (review) ;
(f) The function conferred by section 55 Q of the freedom of information Act 1982 (correcting errors in IC review decisions) ;
(g) The function conferred by section 73 of the freedom of information Act 1982 (discretion not to investigate a complaint) ;.
(h) The function conferred by section 86 of the freedom of information Act 1982 (obligation to notify on completion of investigations) ;
(i) The function conferred by sections 89 and 89A of the freedom of information Act 1982 (implementation not ices and reports) ;
(j) The function conferred by sections 89k of the freedom of information Act 1982 (making a vexatious applicant declaration);.
(k) Issuing guidelines under section 17 of the privacy Act 1988.
(l) Making determinations for the purposes of section 52 of the privacy Act 1988.
(m) Available at https://www.legislation.gov.au/details/c2070A00052. Last visited 20/3/2018
(1) Part 4 – Information Advisory committee 26 Guide to this part
"This part establishes on information Advisory committee to assist and advise the information commissioner an matters relating to the performance of the information commissioner functions 27 Establishment and functions"

وفى ألمانيا صدر قانون حرية المعلومات الألماني The German Freedom of Information ACT. والذى دخل حيز النفاذ في يناير عام ٢٠٠٦، وقد أنشأ هذا القانون حقًا قانونيًا للوصول إلى المعلومات الرسمية التي تحتفظ بها السلطات الاتحادية وأصبح مفوض المعلومات في ظل هذا القانون يطلق عليه المفوض الفيدرالي لحماية البيانات وحرية المعلومات (FFDF) ويتم تعيين مفوض المعلومات عن طريق قيام الحكومة الألمانية بترشيحه ثم يتم عرض الأمر على البرلمان، ويتم انتخاب مفوض المعلومات عن طريق البرلمان الألماني وهو يعتبر موظفًا عامًا ومدة انتخابه خمس سنوات قابلة للتجديد وهو كيان إداري له سلطة مستقلة يتولى الرقابة على حماية البيانات في القطاعات الحكومية العامة، وشركات الاتصالات السلكية واللاسلكية والخدمات البريدية، ويقدم تقرير نصف سنوي عن نشاطه في مجال حماية الخصوصية وحرية المعلومات(١).

ومن الجدير بالذكر أن قانون حرية المعلومات الألماني قد جعل المعلومات التي تحتفظ بها السلطات العامة متاحة للجميع رغم وجود بعض الاستثناءات ويجب أن تتم معالجة الطلبات المقدمة من قبل السلطة الحكومية التي تستلمها في غضون أشهر ويمكن

1- There is to be an information advisory committee, with the function of assisting and advising the information commissioner in maffers relating to the performance of the information commissioner. functions.
2- The committee consists of the following person:
a) the information commissioner, as chair;
b) senior officers of agencies nominated in writing by the minrster, in consultation with the relevant ministers;
c) such other persons as the Minister thinks fit and who, in the minister's opinion, hold suitable qualifications or experience.
Available at https//www.legislation.gov.au/details/c2010A00052 last visited 20/3/2018
(1) https://wikipedia.org/wiki/federal-commissioner for data-protection-and freedom of information last visited 24/3/2018.

تقديم المعلومات شفهيًا، أو إلكترونيًا، أو خطيًا، والأصل أن المعلومات الأساسية تقدم مجانًا إلا أن وزارة الداخلية قد حددت رسومًا لأنواع معينة من الطلبات، وفى عام ٢٠١١ أطلق ائتلاف من منظمات حرية المعلومات موقعًا على الإنترنت لتيسير عملية تقديم الطلبات، وتشجيع ممارسة الحق في الحصول على المعلومات وقد ساعد الموقع في إطلاق حوالى ٥٠٠٠ طلب للحصول على المعلومات[١].

(1) https://www.Gerany-Freedomhousehtml. Last visited 24/3/2018.

المبحث الثالث

الحماية الإدارية للمعلوماتية في مصر

ترتب على التناقض بين حق الأفراد في الحياة الخاصة، وحق الدولة في الاطلاع على شئون الأفراد زيادة تهديد الحق في الخصوصية والذى تعمق في ظل تدخل الدولة في شئون الأفراد، وليس المقصود بذلك التدخل الاطلاع على معلومات معينة عن الأفراد لتنظيم الحياة الاجتماعية على نحو أفضل كالاحتفاظ بسجلات الولادة، والوفيات، والإحصاءات، وغيرها.

إنما المقصود هو استخدام الدولة للمعلومات الشخصية الخاصة بالفرد في أغراض تتعارض مع صونها واحترامها، وقد ترتب على تطور الجانب التنظيمي للحق في الخصوصية إنشاء العديد من الجهات والهيئات الرقابية كاللجنة الوطنية للمعلوماتية والحريات بفرنسا، ومفوض المعلومات الألماني، ولجنة التجارة الفيدرالية الأمريكية، والهيئات الرقابية إما أن تكون هيئات رقابة إدارية تابعة للجهاز التنفيذي للدولة، أو تكون هيئات خاصة مستقلة عن السلطات الأخرى من خلال إنشاءها بتشريع خاص يتضمن تشكيلها، واختصاصاتها، وأسلوب ممارستها لعملها، ويضمن لها الاستقلال في مواجهة السلطات المختلفة [1].

ومصر تأخذ بالأسلوب الأول في الحماية الإدارية من خلال أجهزة تابعة للجهاز التنفيذي للدولة.

أما الحماية الإدارية على المستوى الأوروبي فتتجه إلى اعتناق مبادئ لحماية الحق في الخصوصية، وإصدار قوانين تنظم استخدام المعلومات الشخصية، وتعتبر دولة السويد أول دولة أوروبية اهتمت تشريعيًا بإصدار قانون لحماية الحق في خصوصية

(١) د/ محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، مطبوعات الكويت، ١٩٩٢، ص ١٢٧.

البيانات، وتأخذ بنظام مفوض المعلومات لتوفير الحماية الإدارية للخصوصية المعلوماتية وتبعتها بعد ذلك الدنمارك، وألمانيا الغربية، ولكسمبرج، والنرويج، وفرنسا، والنمسا، وقد اعتمدت أغلب دول الاتحاد الأوروبي على أحد نظامين في مجال الحماية الإدارية للخصوصية المعلوماتية إما من خلال إنشاء لجنة إدارية مستقلة أو إنشاء نظام مفوض المعلومات لحماية البيانات على شبكة الإنترنت(١).

وتتولى العديد من هيئات الحكومة والقطاع الخاص المصري تجميع بيانات عديدة وتفصيلية عن الأفراد تتعلق بالوضع المادي، أو الصحي، أو التعليم، أو العائلة، أو العادات الاجتماعية، أو العمل، وتستخدم الحاسبات وشبكات الاتصال في تخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الاطلاع على هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل ويفتح المجال لإساءة الاستخدام أو توجيهها توجيهًا منحرفًا أو مراقبة الأفراد وكشف خصوصياتهم، أو الحكم عليها من واقع سجلات البيانات الشخصية المخزنة إلكترونيًا(٢).

ويشير مفهوم الحكومة الإلكترونية إلى استخدام تكنولوجيا المعلومات والاتصالات في الإدارة الحكومية مثل شبكات ربط الاتصالات الخارجية، ومواقع الإنترنت، ونظم الحاسب الآلي من خلال الجهات الحكومية التي تقوم بتقديم الخدمات الحكومية إلكترونيًا، ولا ريب في أن تبنى مصر للحكومة الإلكترونية للتعامل الإلكتروني من شأنه أن يؤثر في العلاقة الأساسية بين الجهات الحكومية من جانب والمواطنين، وأعمالهم من جانب آخر(٣)

---

(١) د/ محمد عبد المحسن المقاطع، المرجع السابق، ص ١٣٤

(2) http://www.f-law.net/law/showthread.php last visited 5/4/2018.

(3) http://adlen.atspace.com/gov2.htm last visited 5/4/2015.

وتشمل اختصاصات الحكومة الإلكترونية المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام، ومنها التصاريح المختلفة والخدمات التي تقدمها الجمارك والضرائب ومصلحة الأحوال المدنية وكذلك كل ما يقدم إلى الجهات الحكومية من طلبات، والتي من الممكن أن تتم عن طريق المحررات الإلكترونية التي تصدرها الجهات سالفة الذكر ويتم توقيعها من قبل الموظفين العموميين في هذه الجهات مما يسبغ هذه المحررات الإلكترونية. الحكومية صفة المحررات الرسمية وذلك نتيجة قيام الموظف العام بالتوقيع عليها إلكترونيًا، وذلك بهدف رفع كفاءة العمل الإداري والارتقاء بمستوي أداء الخدمات الحكومية بما يتفق مع متطلبات العصر[١].

ولا ريب في أن تطبيق المعايير القانونية لحماية الخصوصية والأمن على الإنترنت هو من اختصاص الحكومة الإلكترونية وهنا تبرز أهمية وجود سلطة إدارية مستقلة (لجنة مستقلة لحماية الخصوصية، أو نظام مفوض البيانات والخصوصية) لحماية خصوصية مستخدمي الإنترنت والمساهمة في مكافحة الجرائم الإلكترونية، فضلًا عن تفعيل دور الحكومة الإلكترونية لإيصال الخدمات إلى المواطنين والتسهيل عليهم، وفى الوقت ذاته المطالبة بأن تكون البيانات التي يتم الحصول عليها بواسطة الحكومة الإلكترونية، تخضع لذات الضمانات القانونية المعمول بها في القانون المقارن من خلال تمتعها بالحماية، وعدم إمكانية الوصول إليها إلا وفقًا لضوابط قانونية محددة على سبيل الحصر وبناء على إذن قضائي من أجل تفادي انتهاك حرمة الحياة الخاصة، أو سرقة المعلومات [٢].

وقد أفرز التطور السريع للمعلوماتية ضرورة وجود هيئة إدارية مستقلة تتولى حماية خصوصية الأفراد عن طريق قانون يخدم مصالح الأفراد، ويوفر لهم الحماية حيث

---

(١) د/ أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، ٢٠٠٠، ص ٥١.

(٢) د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت، مرجع سابق، ص ٦٥٤.

لا ينبغي أن تكون المعلوماتية وسيلة للانتقاص من الكرامة الإنسانية أو الحياة الخاصة ومن هنا كانت فكرة مشروعات القوانين في مجال حماية المعلوماتية في البيئة الرقيمة، والذى ترجم إلى أرض الواقع لينظم المعاملات الإلكترونية ويضع لها الضوابط والأحكام فالبيانات المسجلة في وحدات المرور والأحوال المدنية تحتوي على معلومات تفصيلية عن الشخص، وصورته الشخصية والاسم، ورقم التليفون، والعنوان، ورقم البطاقة القومي الخاص به وجميع البيانات الشخصية المعرفة لشخصية المواطن دون حماية إدارية فعالة.

ويقوم الجهاز القومي لتنظيم الاتصالات بتوفير الحماية الإدارية في مجال الاتصالات السلكية واللاسلكية وفقًا لأحكام قانون تنظيم الاتصالات وحماية حقوق المستخدمين حيث تنص المادة الثانية منع على أنه " تقوم خدمات الاتصالات على مراعاة القواعد الآتية :

١- علانية المعلومات.

٢- حماية المنافسة الحرة.

٣- توفير الخدمة الشاملة.

٤- حماية حقوق المستخدمين.

وذلك على النحو المبين بهذا القانون"[١].

ويعتبر الجهاز القومي لتنظيم الاتصالات هو الجهة الإدارية المختصة بتنظيم الاتصالات وحماية الأفراد المستخدمين في بيئة الاتصالات في مواجهة المتحكمين في تلك الخدمات، وهو ليس جهة إدارية مستقلة بل يتبع وزير الاتصالات الذى يراس الجهاز. ويقوم بتعيين رئيس الجهاز التنفيذي، ويقدم الجهاز حماية محدودة للخصوصية في بيئة الإنترنت والاتصالات حيث أن وظيفته تنظيم الاتصالات ومنح التراخيص وليس

(١) المادة (٢) من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

حمايـة البيانـات التـي تنتقـل عبـر الاتصـالات ويقـوم الجهـاز علـى حمايـة خصوصـية المستخدمين في حالات محددة وليس له التوسع فيها [1].

ـ كما نصت المادة (١) من قانون تنظيم الاتصالات سالف الذكر على أنه :

" يقصد في تطبيق أحكام هذا القانون بالمصطلحات التالية المعاني المبينة قرين كل منها :

١ـ الاتصـالات: أيـة وسـيلة لإرسـال أو اسـتقبال الرمـوز، أو الإشـارات أو الرسـائل، أو الكتابـات أو الصـور، أو الأصـوات، وذلـك أيًـا كانـت طبيعتهـا وسواء كان الاتصال سلكيًا أو لاسلكيًا.

٢ـ خدمة الاتصالات: توفير أو تشغيل الاتصالات أيا كانت الوسيلة المستعملة.

٣ـ شبكة الاتصالات: النظام أو مجموعة النظم المتكاملة للاتصالات شاملة ما يلزمها من البنية الأساسية.

٤ـ المستخدم : أي شخص طبيعي أو اعتباري يستعمل خدمات الاتصالات أو يستفيد منها.

٥ـ مقدم خدمة الاتصالات : أي شخص طبيعي أو اعتباري مرخص له من الجهاز بتقديم خدمة أو أكثر من خدمات الاتصالات للغير.

٦ـ المشغل : أي شخص طبيعي أو اعتباري مرخص له من الجهاز بإنشاء أو تشغيل شبكة للاتصالات.

٧ـ الطيف الترددي: حيز الموجات التي يمكن استخدامها في الاتصال اللاسلكي طبقًا لإصدارات الاتحاد الدولب للاتصالات.

---

(١) وليد السيد سليم، المرجع السابق، ص ٦٥٨.

٨- الأمن القومي : ما يتعلق بشئون رئاسة الجمهورية والقوات المسلحة والإنتاج الحربي وزارة الداخلية والأمن العام وهيئة الأمن القومي وهيئة الرقابة الإدارية والأجهزة التابعة لهذه الجهات.

٩- أجهزة الأمن القومي: تشمل رئاسة الجمهورية ووزارة الداخلية وهيئة الأمن القومي وهيئة الرقابة الإدارية.

١٠- خدمات اتصالات الإغاثة والطوارئ: وتشمل بوجه خاص الإسعاف والنجدة والدفاع المدني والحريق".

وقد نصت المادة (٣) من هذا القانون على أنه:

"تنشأ هيئة قومية لإدارة مرفق الاتصالات تسمى "الجهاز القومي لتنظيم الاتصالات "ويكون للجهاز الشخصية الاعتبارية العامة ويتبع الوزير المختص ويكون مقره الرئيسي محافظة القاهرة أو الجيزة وله إنشاء فروع أخرى بجميع أنحاء جمهورية مصر العربية".

مجلس إدارة الجهاز :

ومجلس الإدارة هو السلطة المختصة بشئون الجهاز، وتصريف أموره وله أن يتخذ ما يراه لازما من قرارات لتحقيق الأهداف التي أنشئ الجهاز من أجلها، ويباشر المجلس اختصاصاته على الوجه المبين بهذا القانون ويختص بإقرار خطط وبرامج نشاط الجهاز في إطار الخطة العامة للدولة، واعتماد الهيكل التنظيمي والإداري للجهاز، ووضع الضوابط والأسس الخاصة بالجودة الفنية والقياسات المعيارية وقياسات جودة الأداء لمختلف خدمات الاتصالات مما يؤدي إلى رفع مستوي الأداء والمتابعة الدورية لنتائج تطبيق هذه الضوابط والأسس والقياسات مع مراعاة المعايير الصحية والبيئية، واتخاذ ما يلزم لتنفيذ الخطط والمقترحات الكفيلة بتحقيق الأهداف التي يقرها مجلس الوزراء لتوفير خدمات الاتصالات المناسبة في جميع مناطق الجمهورية، واعتماد خطة

استخدام الطيف الترددي ومراجعتها وتعديلها كلما دعت الضرورة وذلك بمراعاة قرارات وتوصيات الاتحاد الدولي للاتصالات ووضع قواعد، وشروط منح التراخيص الخاصة بإنشاء البنية الأساسية لشبكات الاتصالات بما لا يخل بأحكام القوانين المنظمة لأعمال البناء والتخطيط العمراني وقوانين البيئة والإدارة المحلية، وكذلك تراخيص تشغيل هذه الشبكات، وإدارتها والتراخيص الخاصة بتقديم خدمات الاتصالات، وإصدار هذه التراخيص، وتجديدها ومراقبة تنفيذها طبقا لأحكام هذا القانون بما يضمن حقوق المستخدمين وخاصة حقهم في ضمان السرية التامة طبقا للقانون، وبما لا يمس بالأمن القومي والمصالح العليا للدولة ومعايير التخطيط العمراني[1]

وظيفة الجهاز القومى لتنظيم الاتصالات :

وقد حدد القانون الهدف من إنشاء الجهاز القومي لتنظيم الاتصالات وهو تنظيم مرفق الاتصالات وتطوير ونشر جميع خدماته على نحو يواكب أحدث وسائل التكنولوجيا ويلبي احتياجات المستخدمين بأنسب الأسعار ويشجع الاستثمار الوطني والدولي في هذا المجال في إطار قواعد المنافسة الحرة ويختص بما يأتي :

١- ضمان وصول خدمات الاتصالات إلى جميع مناطق الجمهورية بما فيها مناطق التوسع الاقتصادي والعمراني والمناطق الحضرية والريفية والنائية.
٢- حماية الأمن القومي والمصالح العليا للدولة.
٣- ضمان الاستخدام الأمثل للطيف الترددي وتعظيم العائد منه طبقًا لأحكام هذا القانون.
٤- ضمان الالتزام بأحكام الاتفاقيات الدولية النافذة والقرارات الصادرة عن المنظمات الدولية والإقليمية المتعلقة بالاتصالات والتي تقرها الدولة

(١) المادتان (١٢، ١٣) من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

ومراقبة تحقيق برامج الكفاءة الفنية، والاقتصادية لمختلف خدمات الاتصالات[1].

كما يكون للجهاز في سبيل تحقيق أهدافه أن يباشر جميع التصرفات والأعمال اللازمة لذلك وله على الأخص ما يأتي :

١- وضع الخطط والبرامج وقواعد وأساليب الإدارة التي تتفق ونشاطه طبقًا لأحكام هذا القانون والقرارات الصادرة تنفيذًا له ودون التقيد باللوائح والنظم الحكومية.

٢- العمل على مواكبة التقدم العلمي والفني والتكنولوجي في مجال الاتصالات مع مراعاة المعايير الصحية والبيئية.

٣- إعداد ونشر بيان بخدمات الاتصالات وأسماء المشغلين ومقدمي الخدمة والأسس العامة التي يتم منح التراخيص والتصاريح بناء عليها.

٤- تحديد الأسس العامة التي يلتزم بها مشغلو ومقدمو خدمات الاتصالات.

٥- تحديد معايير وضوابط خدمات الاتصالات غير الاقتصادية التي يجب أن توفر لجميع المناطق التي تعاني من نقص فيها، وتحديد الالتزامات التي يتحمل بها مشغلو مقدمو خدمات الاتصالات غير الاقتصادية طبقًا لأحكام هذا القانون.

٦- وضع القواعد التي تضمن حماية المستخدمين بما يكفل سرية الاتصالات وتوفير أحدث خدماتها بأنسب الأسعار مع ضمان جودة أداء هذه الخدمات وكذلك وضع نظام لتلقى شكاوي المستخدمين والتحقيق فيها والعمل على متابعتها مع شركات مقدمي الخدمة.

---

(١) المادة (٤) من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

٧- الإشراف على المعاهد التي تؤهل للحصول على الشهادات الدولية في الاتصالات بالتنسيق مع المعهد القومي للاتصالات.

٨- وضع القواعد اللازمة لمنح تصاريح المعدات.

٩- وضع خطة الترقيم القومي للاتصالات والإشراف على تنفيذها.[١]

ويبين على هدى ما تقدم أن الجهاز مسئول عن وضع القواعد التي تضمن حماية خصوصية المستخدمين بما يكفل سرية الاتصالات ووضع نظام لتلقى شكاوى المستخدمين والتحقيق فيها والعمل على متابعتها مع شركات مقدمي خدمات الاتصالات[٢].

ويقوم الجهاز بتشكيل لجنة لحماية حقوق المستخدمين وتضم هذه اللجنة ممثلين لمستخدمي خدمات الاتصالات والجمعيات المعنية بحماية المستهلك، وتتولى اللجنة تقديم المشورة في شأن حماية مصالح مستخدمي الاتصالات[٣].

وتلتزم جميع الجهات، والشركات العاملة في مجال الاتصالات بموافاة الجهاز بما يطلبه من تقارير، أو إحصاءات، أو معلومات تتصل بنشاطه عدا ما يتعلق منها بالأمن القومي [٤].

ومن الجدير بالذكر أنه لا يجوز إنشاء، أو تشغيل شبكات اتصالات، أو تقديم خدمات الاتصالات للغير، أو تهديد المكالمات التليفونية الدولية، أو الإعلان عن شيء من ذلك دون الحصول على ترخيص من الجهاز وفقًا لأحكام هذا القانون والقرارات المنفذة له، ومع ذلك لا يلزم الحصول على ترخيص من الجهاز لإنشاء أو تشغيل شبكة اتصالات

---

(١) المادة (٥) من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.
(٢) د/ أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دار النهضة العربية، ٢٠٠٥، ص ٢٢٢.
(٣) المادة (١٨) الفقرة (٢) من قانون تنظيم الاتصالات.
(٤) المادة (١٩) من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

خاصة لا تستخدم أنظمة اتصال لاسلكية ويلتزم المشغل المرخص له بإخطار الجهاز بالشبكات الخاصة التي تنشأ على بنيته الأساسية [1].

ويحدد الترخيص الصادر الالتزامات التي تقع على عاتق المرخص له والتي تشمل على الأخص ما يأتي:

١- نوع الخدمة والتقنية المستخدمة.
٢- مدة الترخيص.
٣- الحدود الجغرافية لتقديم الخدمة وخطة التغطية السلكية واللاسلكية ومراحل تنفيذها.
٤- مقاييس جودة وكفاءة الخدمة.
٥- الالتزام باستمرار تقديم الخدمة والإجراءات الواجبة الإتباع في حالة قطع الخدمة أو إيقافها.
٦- تحديد سعر الخدمة وطريقة التحصيل والالتزام بالإعلان عن ذلك.
٧- إتاحة الخدمة لجمهور المستخدمين دون تمييز.
٨- الالتزامات الخاصة بعدم المساس بالأمن القومي.
٩- تقديم ما يطلبه الجهاز من المعلومات والبيانات المتصلة بموضوع الترخيص.
١٠- ضمان سرية الاتصالات والمكالمات الخاصة بعملاء المرخص له ووضع القواعد اللازمة للتأكد من ذلك[2].

وتقوم شركات الاتصالات في مصر بالحصول على بيانات تفصيلية عند قيام أي مواطن بالاشتراك في الخدمة، وتشمل هذه البيانات الاسم، ورقم تليفون، والمنزل،

---

(١) المادة (٣١) من قانون تنظيم الاتصالات.
(٢) المادة (٢٥) من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

والعنوان، ورقم البطاقة القومي الخاص بالمشترك، وكافة البيانات الشخصية المحددة لشخصيته، ولا تتوافر لهذه البيانات حماية معقولة ضد التدخل في سريتها من قبل تلك الشركات، أو بناء على إذن قضائي من النيابة العامة يكشف تلك البيانات عند طلبها من الأجهزة الأمنية.

كما أصدر المشرع القانون رقم (١٥) لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني وأنشأ هيئة إدارية تتولي حماية البيانات، والمعلومات، والتعاملات الإلكترونية التي تتم عبر الموقع الإلكتروني وهي هيئة تنمية صناعة تكنولوجيا المعلومات وهي هيئة غير مستقلة وتتبع وزير الاتصالات ولها رئيس تنفيذي يعينه رئيس الوزراء بناء على ترشيح من وزير الاتصالات، وتقدم حماية محدودة للخصوصية لأن وظيفتها تنصب على تنظيم نشاط خدمات التوقيع الإلكتروني وغيرها من الأنشطة في مجال المعاملات الإلكترونية وصناعة تكنولوجيا المعلومات[١].

<u>قانون مكافحة جرائم تقنية المعلومات والتعليق عليه :</u>

وقد أصدر السيد / رئيس الجمهورية يوم السبت الموافق ١٨ أغسطس ٢٠١٨ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، وقد تضمن القانون أربعة أبواب **تناول الباب الأول الأحكام العامة لتطبيق القانون**، والذى تضمن وضع تعاريف للألفاظ والعبارات الواردة بالقانون، وقد فرض القانون بعض الالتزامات على مقدمو الخدمة من أهمها المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص

(١) د/ عمر أبو بكر يونس، الجرائم الناشئة عن استخدامات الإنترنت، دار النهضة العربية، ٢٠٠٤، ص٤٢٧.

والجهات التي يتواصلون معها، كما يلتزم مقدمو الخدمة بتأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها، أو اختراقها أو تلفها، كما يتعين على مقدم الخدمة أن يوفر لمستخدمي خدماته، ولأي جهة حكومية مختصة في الشكل وبالطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة البيانات والمعلومات الآتية :[1]

- اسم مقدم الخدمة وعنوانه.
- معلومات الاتصال المتعلقة بمقدم الخدمة بما في ذلك عنوان الاتصال الإلكتروني.
- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.
- أية معلومات أخرى يقدر الجهاز القومي لتنظيم الاتصالات أهميتها لحماية مستخدمي الخدمة ويحددها القرار الصادر من الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات.

كما يلتزم مقدمو الخدمة والتابعون لهم بأن يوفروا حال طلب جهات الأمن القومي ووفقًا لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقًا للقانون وذلك دون الإخلال بحرمة الحياة الخاصة التي يكفلها الدستور.

ومن الجدير بالذكر أنه إذا كان القانون قد رخص لمقدمي خدمات تقنية المعلومات، ووكلائهم وموزعيهم التابعين لهم والمنوط بهم تسويق تلك الخدمات الحصول على بيانات المستخدمين، إلا أنه قد حظر على غير هؤلاء القيام بذلك[2]

(١) المادة (٢) من قانون جرائم مكافحة تقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨.
(٢) المادة (٢) من قانون مكافحة جرائم تقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨.

الأحكام والقواعد الإجرائية في قانون مكافحة المعلومات:

وتناول الباب الثاني من القانون الأحكام والقواعد الإجرائية حيث أجاز لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها بوضع أي عبارات أو أرقام أو صور، أو أفلام، أو أية مواد دعائية، أو ما في حكمها مما يعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدًا للأمن القومي، أو تعرض أمن البلاد، أو اقتصادها القومي للخطر أن تأمر بحجب الموقع، أو المواقع محل البحث كلما أمكن تحقيق ذلك فنيًا، ويتعين على جهة التحقيق عرض أمر الحجب على المحكمة المختصة منعقدة في غرفة المشورة خلال ٢٤ ساعة مشفوعًا بمذكرة برأيها، وتصدر المحكمة قرارها في الأمر مسببًا خلال مدة لا تجاوز ٧٢ ساعة من وقت عرضه عليها بالقبول أو بالرفض، ويجوز في حالة الاستعجال لوجود خطر حال أو ضرر وشيك الوقوع من ارتكاب جريمة أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز القومي لتنظيم الاتصالات ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع، ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه[1]

وترى الباحثة أن هذا النص لم يحدد طبيعة الحجب المفروض في هذه الحالة وهل هو حجب كلي؟ أم أنه حجب لبعض الروابط إذا انطوت على جريمة من الجرائم التي يحددها القانون؛ ومن ثم فإنه من الممكن أن يتم حجب موقع يحوي ملايين الصفحات بسبب محتوى منشور على صفحة واحدة فقط وذلك لأن القانون لم يحدد حالات الحجب الكلي والحجب الجزئي، ولا ينال من ذلك القول بأن هذا الأمر متروك للائحة التنفيذية للقانون وذلك لأن اللائحة التنفيذية للقانون تفسر وتفصل نصوص القانون دون أن يكون لها استحداث نص جديد في القانون أو تعديل نص موجود أو حذفه، كما أن القانون قد منح جهات التحقيق صلاحية حجب المواقع مباشرة وجعل الرقابة القضائية على هذه

(١) المادة (٧) من قانون مكافحة جرائم تقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨.

القرارات رقابة لاحقة، حيث خول جهات التحقيق أن تطلب حجب مواقع إلكترونية؛ لذا رأت أن هذه المواقع تمثل تهديدًا للأمن القومي، أو تعرض أمن البلاد، أو اقتصادها القومي للخطر وهي عبارات فضفاضة وغير منضبطة.

وعلى جهة التحري والضبط المبلغة أن تعرض محضرًا تثبت فيه ما تم من إجراءات على جهة التحقيق المختصة، وذلك خلال ٤٨ ساعة من تاريخ الإبلاغ الذى وجهته للجهاز، وتصدر المحكمة المختصة قرارها في هذه الحالة أما بتأييد ما تم من إجراءات حجب أو بوقفها وإذا لم يعرض المحضر في الموعد المحدد يعتبر الحجب الذى تم كأن لم يكن.

ولمحكمة الموضوع أثناء نظر الدعوي أو بناء على طلب جهة التحقيق، أو الجهاز القومي لتنظيم الاتصالات، أو ذوى الشأن أن تأمر بإنهاء القرار الصادر بالحجب، أو تعديل نطاقه، وفى جميع الأحوال يسقط القرار الصادر بالحجب بصدور أمر بالأوجه لإقامة الدعوي الجنائية، أو بصدور حكم نهائي فيها بالبراءة[1] وقد نظم المشرع التظلم من القرارات الصادرة بشأن حجب المواقع حيث خول كل من صدر ضده أمر قضائي بحجب المواقع وفقًا للمادة (٧) من هذا القانون، وللنيابة العامة، ولجهة التحقيق المختصة، ولذوي الشأن أن يتظلم منه أو من إجراءات تنفيذه أمام محكمة الجنايات المختصة بعد انقضاء ٧ أيام من تاريخ صدور الأمر، أو من تاريخ تنفيذه حسب الأحوال، وفى حالة رفض التظلم يجوز تقديم تظلم جديد بعد انقضاء ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ويكون التظلم في جميع الأحوال بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم، والجهاز

(١) المادة (٧) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

القومي لتنظيم الاتصالات، وكل ذي شأن، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز ٧ أيام من تاريخ التقرير به[١]

وقد أجاز المشرع للنائب العام أو من يفوضه من المحاميين العامين الأول بنيابات الاستئناف، ولجهات التحقيق المختصة عند الضرورة، أو عند وجود أدلة كافية على جدية الاتهام في ارتكاب أو الشروع في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون أن يأمر بمنع المتهم من السفر خارج البلاد، أو بوضع اسمه على قوائم ترقب الوصول بأمر مسبب لمدة محددة.

ويجوز لمن يصدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة خلال ١٥ يومًا من تاريخ علمه به وفى حالة رفض التظلم يجوز له أن يتقدم بتظلم جديد بعد انقضاء ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ويتم التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تعلن بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز ١٥ يومًا من تاريخ التقرير به، بحكم مسبب، وذلك بعد سماع أقوال المتظلم، وسلطة التحقيق المختصة، وللمحكمة أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها في هذا الشأن.

ويجوز للنيابة العامة وجهات التحقيق المختصة في كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع اسمه من على قوائم المنع من السفر، أو ترقب الوصول لمدة محددة إذا دعت الضرورة لذلك.

---

(١) المادة (٨) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

وفى جميع الأحوال ينتهي المنع من السفر بمضي سنة من تاريخ صدور الأمر، أو بصدور قرار بألا وجه لإقامة الدعوي الجنائية، أو بصدور قرار نهائي فيها بالبراءة أيهما أقرب[1].

حجية الأدلة المستخرجة من وسائل تقنية المعلومات:

وقد أضفى المشرع على الأدلة المستخرجة من الأجهزة، والمعدات والوسائط الإلكترونية، أو النظام المعلوماتي، أو برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات القيمة والحجية المقررة للأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية وهي:

١. أن تتم عملية جمع، أو الحصول، أو استخراج، أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير، أو تحديث، أو محو، أو تحريف للكتابة أو البيانات والمعلومات، أو تغيير، أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو البرامج، أو الدعامات الإلكترونية وغيرها.

٢. أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته، أو نفيه، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة.

٣. أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخول لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، على أن يبين في محاضر الضبط، أو التقارير الفنية نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخواتم Hash الناتج عن استخراج نسخ مماثلة ومطابقة

---

(١) المادة (٩) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ والمنشور في الجريدة الرسمية، العدد (٣٢)، مكرر (ج)، في ١٤ أغسطس ٢٠١٨.

للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني، مع ضمان استمرار الحفاظ على الأصل دون عبث به.

٤. في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص والتحليل.

٥. أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وتوثيق مكان ضبطه ومكان حفظه، ومكان التعامل معه ومواصفاته[١]

ونخلص من جماع ما سبق أن المشرع المصري قد ترك الرقابة على نظم المعلومات للقواعد العامة وكنا نأمل أن يتبنى المشرع إنشاء سلطة إدارية مستقلة تتولى مهمة الرقابة على نظم المعلومات وتضمن حماية الحريات الشخصية في مواجهة نظم المعلومات، كما هو الشأن في التشريع المقارن.

حيث جعل القانون الجهاز القومي لتنظيم الاتصالات هو المهيمن على كل ما يتعلق باتصالات المعلومات وتقنياتها.

وقد سلك المشرع مسلك محمود عندما ضمن القانون نص المادة (٢٥) والذى فرض عقوبة الحبس مدة لا تقل عن ستة أشهر وغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائة ألف جنيه، أو إحدى هاتين العقوبتين على كل من اعتدى على أي من المبادئ، أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات نظام، أو موقع لترويج السلع أو الخدمات دون موافقته، أو قام بالنشر عن طريق الشبكة

(١) المادة (٩) من اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات والمنشورة بالجريدة الرسمية، العدد ٣٥، تابع (ج)، في ٢٧أغسطس ٢٠٢٠.

المعلوماتية، أو احدى وسائل تقنية المعلومات لمعلومات، أو أخبار، أو صور، وما في حكمها تنتهك خصوصية أي شخص دون رضاه سواء كانت المعلومات المنشورة صحيحة، أو غير صحيحة.

وهذا النص يكفل حماية المبادئ والقيم الأسرية في المجتمع المصري، كما يضمن حماية حرمة الحياة الخاصة للأفراد التي كفلها الدستور في المادة ٥٧ منه وتحقيق التوازن بين حرية التعبير وحماية خصوصية الأفراد.

ويؤخذ على هذا القانون أنه قد توسع في مفهوم الأمن القومي ليشمل كل ما يتصل باستقلال واستقرار، وأمن الوطن، ووحدته، وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي ووزارة الدفاع والإنتاج الحربي ووزارة الداخلية والمخابرات العامة وهيئة الرقابة الإدارية والأجهزة التابعة لتلك الجهات، وقد جاء هذا التوسع على حساب خصوصية المعلومات.

كما توسع القانون أيضا في جهات الأمن القومي وعددها في رئاسة الجمهورية، ووزارة الدفاع ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، فإذا كان مفهوم الأمن القومي المتعارف عليه هو كل ما يتعلق بأمن الدولة وسيادتها واستقلالها ومصالحها العليا ووحدتها وسلامة أراضيها فإن إدراج كل ما يتعلق بشئون رئاسة الجمهورية، ووزارة الداخلية، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات ضمن مفهوم الأمن القومي ليس له مبرر أو مسوغ قانوني.

كما أن التوسع في جهات الأمن القومي وإلزام مقدمو الخدمة التابعون لهم بأن يوفروا لهذه الجهات كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقًا للقانون، وذلك من شأنه انتهاك حرمة الحياة الخاصة للأفراد وخصوصية معلوماتهم لاسيما في حالة إساءة استخدام هذه المعلومات من قبل تلك الجهات، لذا كان الأجدر بالمشرع أن يعمل على تضييق جهات الأمن القومي لتحقيق التوازن بين حماية الأمن

القومي، وصون حرمة الحياة الخاصة للأفراد وخصوصية معلوماتهم، لاسيما وأن مفهوم الأمن القومي هو مفهوم واسع وفضفاض، وقد خلا القانون من وضع تعريف واضح ومحدد له.

ومع ذلك فإنه لا ريب في أن إصدار قانون مكافحة جرائم تقنية المعلومات يعتبر خطوة هامة في مجال حماية نظم المعلومات ومواكبة التطور التكنولوجي، وأثره على الحريات الفردية، لذا نأمل من المشرع المصري أن يحذو حذو المشرع المقارن وأن يصدر قانون مستقل يتعلق بأمن نظم المعلومات، ويكفل حماية الخصوصية المعلوماتية كي تكتمل المنظومة التشريعية التي بدأها بإصدار قانون مكافحة جرائم تقنية المعلومات.

وقد صدر قرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠[١] بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات وقد فرضت اللائحة التنفيذية عدة التزامات على مقدموا خدمات تقنيات المعلومات تتمثل في الآتي:

١. تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل.
٢. تنصيب واستخدام نظم وبرامج ومعدات مكافحة البرمجيات والهجمات الخبيثة، والتأكد من صلاحيتها وتحديثها.
٣. استخدام بروتوكولات آمنة مثل بروتوكول نقل النص التشعبي المؤمن HTTPS.
٤. وضع صلاحيات بالشبكات والملفات وقواعد البيانات، وتحديد المسئولين لضمان حماية الوصول المنطقي Logical Access إلى الأصول المعلوماتية والتقنية لمنع الوصول غير المصرح به .

(١) الجريدة الرسمية، العدد ٣٥ تابع "ج" الصادر بتاريخ ٢٧ أغسطس ٢٠٢٠.

٥. إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها، وكذا بيان بالنظم والبرامج والتطبيقات، وقواعد البيانات المستخدمة ومواصفاتها.
٦. تطبيق أفضل الممارسات والضوابط عند اختيار مواصفات كلمات السر أو المرور وفقًا للملحق رقم (١) المرفق باللائحة التنفيذية.
٧. توثيق إجراءات التنصيب والتشغيل الخاصة بالأنظمة.
٨. ضمان تنفيذ وتشغيل وصيانة الأنظمة وإلزام الأطراف المتعاقدة معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة وحدود مسئولية كل جهة.
٩. إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري وإتمام الاختبارات اللازمة قبل إجراء التحديثات .

تقييم الحماية الإدارية في مصر :

ويبين من استقراء القوانين المصرية التي تعالج حماية الخصوصية أنه لا يوجد في مصر حتى الآن جهة إدارية مسئولة عن حماية الحق في الخصوصية على الإنترنت (On line) أو خارج الإنترنت (Off line) كما لا يوجد في مصر قانون شامل للحق في الخصوصية، كما لا يوجد قانون لحماية أمن المعلومات، ولا يوجد قانون لحماية البيانات الشخصية، كما هو الشأن في القانون المقارن ويظهر هذا النقص التشريعي الجسيم خلال تعامل الأجهزة الإدارية الحكومية مع بيانات المواطنين حيث لو تجرأ مواطن وسأل موظف في أي جهة حكومية عن إجراءات أمن المعلومات، أو الشفافية، أو حق الوصول والاعتراض والتصحيح وخاصة في الجهات الأمنية والإدارية والخدمية لأخذها الموظف من قبيل الهزل ولم يحملها على محمل الجد.

لذا فإننا نرى أنه ينبغي الإسراع في إنشاء هيئة إدارية مستقلة تكون مهمتها حماية أمن المعلومات وصون خصوصية الأفراد على المواقع الإلكترونية ووضع مبادئ عامة لاستخدام البيانات الشخصية أسوة بالمشرع المقارن.

موقف القضاء الإداري من حماية حرية الرأي على الإنترنت:

وقد تصدى القضاء الإداري للدعوى المتعلقة بقطع خدمات الاتصالات أثناء ثورة ٢٥ يناير[١] وقررت المحكمة الإدارية بجلسة ٢٠١١/٥/٢٨ أنه "وقد ثبت للمحكمة بيقين أن قطع خدمات الاتصالات والرسائل القصيرة (SMS) عن الهواتف النقالة (المحمول) وخدمات الإنترنت جاء انتهاكًا واعتداء على مجموعة من الحقوق والحريات العامة وعلى رأسها حرية التعبير، والحق في الاتصال، والحق في الخصوصية، والحق في استخدام الطيف الترددي، والحق في المعرفة، وما يتصل به من الحق في تدفق المعلومات وتداولها، وارتباطه بكل من الحق في التنمية، والحق في الحياة، و من ثم فقد بات على النيابة العامة تحريك الدعوي الجنائية ضد كل من أسهم بفعله أو بمشاركته في ارتكاب الجريمة الجنائية المشار إليها، كما بات على الدولة كفالة التعويض العادل لكل من وقع عليه ذلك الاعتداء، على أن تنظر ذلك في ضوء مسئولياتها المقررة وفقًا لنظرية المخاطر المنصوص عليها في المادة (٦٨) من قانون تنظيم الاتصالات المشار إليه من تعويض شركات الاتصالات من مقدمي ومشغلي الخدمات وكذلك جموع المواطنين من المشتركين مستخدمي تلك الخدمات عن طريق تلك الشركات.

وليس من شك في أن ثمة علاقة وثيقة بين الحق في الاتصال وضرورة كفالته وبين (الحق في الخصوصية) ووجوب حمايتها، فلا يجوز أن يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو (مراسلاته) ولكل شخص وفقًا لما قررته المادة (١٢) من الإعلان العالمي لحقوق الإنسان الحق في حماية حياته من مثل هذا التدخل، وهو ما تم التأكيد عليه في المادة (١١) من الإعلان الدستوري – المقابلة للمادة (٤٥) من

(١) يوم الجمعة الموافق ٢٠١١/١/٢٨ تم قطع الاتصالات في مصر (المحادثات الهاتفية – الرسائل النصية والصوتية على جميع مستخدمي الشبكات الثلاث) بدون إنذار أو تحقيق.

الدستور المصري الساقط – بتقرير أن لحياة المواطنين الخاصة حرمة يحميها القانون، وللمراسلات البريدية والبرقية والمحادثات التليفونية."[1]

ويأتي على خلاف الحكم السابق ما قضت به المحكمة الإدارية العليا في ٢٤ مارس ٢٠١٨ حيث ألغت حكم تغريم مبارك والعادلي في قضية قطع الاتصالات إبان ثورة يناير ٢٠١١، وأكدت المحكمة الإدارية العليا في حيثيات حكمها إلغاء الحكم المطعون فيه بشأن تغريم الرئيس الأسبق محمد حسنى مبارك وأحمد نظيف رئيس مجلس الوزراء الأسبق وحبيب العادلي ووزير الداخلية الأسبق ٥٤٠ مليون جنيه تعويضًا عن قطع الاتصالات أثناء ثورة ٢٥ يناير وأخذت بما ذكرته محكمة الجنايات أن قرار قطع الاتصالات كان قرارًا صائبًا ولا يشبوه انحراف بالسلطة أو التربح.

"وأوضحت المحكمة في حيثيات حكمها أن القرار كان للصالح العام ويصب في مصلحة أمن الدولة، واستندت المحكمة أن العادلي صدر بحقه حكم إدانة في أول درجة ثم تم تبرئته بعد ذلك في قضية تنظر أمام محكمة الجنايات بتهمة التربح والاستيلاء على المال العام، كما ذكرت المحكمة الإدارية العليا أنها استندت على شهادة الشهود وقتذاك والذين أكدوا أمام محكمة الجنايات أن مصر كانت تمر بظروف عصيبة، وكانت هناك أيدي خفية تعبث وتحاول تخريب البلاد وعناصر خارجية مندسة من إسرائيل وأمريكا تحاول زعزعة الاستقرار وتفتيت الوطن وإحداث الفتنة، فضلًا عن شهادة الأمن الوطني والتي أكدت القيادات بها بأن قرار قطع الاتصالات كان في مصلحة البلاد نظرًا لما تقتضيه ويتطلبه الأمن القومي وقتذاك.

لذلك رأت المحكمة أن الحكم الصادر في حق العادلي من محكمة جنائية حكم بات وأيدته محكمة النقض حيث أصبح نهائي، لذلك اعتبرت القرار سليم ولا تشوبه

---

(١) حكم محكمة القضاء الإداري، دائرة المنازعات الاقتصادية والاستثمار، الدعوى رقم ١٢٦٨٥٥ لسنة ٦٥ق، جلسة ٢٠١١/٥/٢٨.

شـائبة، ولا يعتبـر انحـراف بالسـلطة كمـا تبـين للمحكمـة أن القـرار لـم يشـوبه عـدم المشروعية، وانتفى فيه ركن الخطأ لذلك لا يوجد أي تعويض لخزانة الدولة حيث إنها لم يقع عليها أي ضرر لذا رأت المحكمة إلغاء التغريم"[1].

وتـرى الباحثـة أن حكـم محكمـة القضـاء الإداري سـالف الـذكر قـد جـاء مسـايرًا للظروف السياسية، والأمنية التي مرت بها مصر في ذلك الحين هذا فضـلا عن الرفض العارم من قبل الرأي العام لقرار قطع الاتصالات والذى كان له أثر كبير على حكم محكمـة القضـاء الإداري حيث جاءت معظم الأحكام في هذه الفترة بغية إرضـاء الرأي العام ومحاولة تهدئة الجماهير.

أما حكم المحكمة الإدارية العليا فقد جاء في ظروف سياسية مغايرة للظروف السابقة ولم يواكب الفترة السابقة على صدوره غضب شعبي مما جعل الحكم يصدر على هذا النحو.

ونستنتج من هذين الحكمين أن القضاء الإداري يتأثر في أحكامه باتجاه الرأي العام وبالظروف السياسية السائدة وقت صدور هذه الأحكام وهو ما ينبغي أن ننأى عنه حيث يتعين أن تبتعد وسائل الإعلام التي تلعب دورًا كبيرًا في توجيه الرأي العام عن مناقشـة الموضـوعات المطروحـة أمـام القضـاء، وألا يفـتح البـاب للمناقشـة فـي هـذه الموضوعات إلا بعد صدور أحكام نهائية بشأنها، كما يتعين أن تكون الأحكام القضائية بعيدة كل البعد عن الظروف السياسية فالحكم القضائي البات هو عنوان الحقيقة المطلقة، والحقائق ثابتة ولا تتغير بتغير الظروف السياسية التي تمر بها الدولة.

---

(١) حكم المحكمة الإدارية العليا، الدعاوى أرقام ٣٧٧، ٣٧٧٥٩، ٣٨٢٥٩، ٣٨٤٠٠، لسنة ٥٩ إدارية عليا، جلسة ٢٠١٨/٣/٢٤، جريدة الأهرام، العدد الأول، ٢٠١٨/٣/٢٥.

كما قضت الدائرة الثانية بمحكمة القضاء الإداري بعدم قبول الدعوي التي تطالب بحجب موقع التواصل الاجتماعي " فيس بوك " عن مصر[١].

ولا شك في أن هذا الحكم يعلى من قيمة حرية الرأي والتعبير على الإنترنت ويعمل على تحقيق التوازن بين حرية الرأي على مواقع التواصل الاجتماعي، وحماية الأمن الوطني، والنظام العام فإذا كان استخدام مواقع التواصل الاجتماعي من شأنه المساس بالأمن الوطني، والنظام العام فإنه يتعين على الجهاز القومي لتنظيم الاتصالات التدخل لحجب، وتقييد تلك الصفحات على المواقع من أجل حماية النظام العام.

(١) أ/ حازم عادل، حيثيات حكم القضاء الإداري برفض دعوى حجب "فيس بوك، جريدة اليوم السابع، ٢٠١٥/٨/٢٥.
متاح على موقع: .https://m.youm7.com/story

الخاتمة

تعرضنا في هذا البحث إلى الحماية الإدارية لأمن المعلومات ورأينا أن التطور السريع لتقنيات الحاسب كان له آثاره الملحوظة على أمن الحاسبات سواء سلبًا أو إيجابًا، وهذا التطور السريع في غالب الأحوال أسرع من أن تتم ملاحقته بواسطة خبراء أمن الحاسبات لتغطية الثغرات التي قد تنشأ عن النظم الجديدة الأكثر تعقيدًا مما يتسبب في وجود فجوة تقنية بين السلاح التقني المستخدم في انتهاك المعلومات وبين الأسلحة المضادة التي يلجأ إليها خبراء أمن المعلومات وهذه الفجوة ليست في صالح أمن المعلومات وإحكام الحماية ضد انتهاكها.

كما رأينا أن الفقه الأمريكي قد ذهب إلى ترك الرقابة على نظم المعلومات للقواعد العامة دون حاجة لإنشاء جهة إدارية تتولى هذه المهمة، أي أن الولايات المتحدة الأمريكية لم تأخذ بالنظام الفرنسي الذي يعتمد على وجود لجنة تتولى مهمة حماية الخصوصية واللجنة الوطنية للمعلوماتية والحريات"، ولكنها تعز وتشجع ما يعرف بالتنظيم الذاتي فتعتمد الولايات المتحدة الأمريكية في الحماية الإدارية للخصوصية المعلوماتية على القواعد العامة وعدم وجود جهة إدارية محددة لحماية الخصوصية.

فالنظام الأمريكي يولي الأهمية في نظرته للضمانات الإدارية لحماية الخصوصية إلى حرية التعبير وحرية تدفق المعلومات على حساب الخصوصية المعلوماتية.

في حين رأينا أن النظام القانوني الألماني تبنى نظام مفوض المعلومات حيث عهد القانون الألماني الاتحادي الصادر عام ١٩٧٧ بمهمة الرقابة على تطبيق القانون إلى مفوض نظام المعلومات الذي يختص بحماية البيانات وقد حدد ثلاثة أنواع من المفوضين، فيوجد مفوض لحماية البيانات المعالجة بمعرفة الحكومة، وثمة مفوض آخر يختص بحماية البيانات التي يتم معالجتها بمعرفة الشركات والهيئات الخاصة لتحقيق أغراض متعلقة بها، كما يوجد مفوض ثالث مسئول عن حماية البيانات المعالجة بواسطة منظمات خاصة

لحساب جهة مغايرة، ولا ريب في أن نظام مفوض نظم المعلومات يتميز ببساطته وضآلة الأعباء المالية التي يحملها للخزانة العامة، كما أن فاعليته تعتمد على شخصية من يتولى هذا المنصب والذي يشترط فيه أن يكون أهلاً للثقة والاحترام مما يساعد على قيامة بمهمته، ويدعم من قيمة ما يصدره من قرارات وتوصيات.

بيد أنه يعيب هذا النظام أن تدخل المفوض لحماية البيانات الشخصية لا يكون إلا بناء على شكوى من صاحب الشأن، ومن ثم لا يجوز له أن يقوم من تلقاء نفسه بالتحري عن مدى احترام القانون، كما أن المفوض لا تتوافر لديه في الغالب الخبرة الفنية اللازمة للتأكد من إعمال قواعد السلامة والحماية.

كما رأينا أن التناقض بين حق الأفراد في الحياة الخاصة وحق الدولة في الاطلاع على شئون الأفراد قد أدى إلى زيادة تهديد الحق في الخصوصية والذي تغلغل في ظل تدخل الدولة في شئون الأفراد، وليس المقصود بالتدخل هنا الاطلاع على معلومات معينة عن الأفراد لتنظم الحياة الاجتماعية على نحو أفضل كالاحتفاظ بسجلات الولادة والوفيات والإحصاءات وغيرها؛ وإنما المقصود هو استخدام الدولة للمعلومات الشخصية الخاصة بالفرد في أغراض تتعارض مع صونها واحترامها، وقد ترتب على تطور الجانب التنظيمي للحق في الخصوصية إنشاء العديد من الجهات والهيئات الرقابية، وهذه الهيئات الرقابية إما أن تكون هيئات رقابية تابعة للجهاز التنفيذي للدولة، أو تكون هيئات خاصة مستقلة عن السلطات الأخرى من خلال إنشاءها بتشريع خاص يتضمن تشكيلها، واختصاصاتها، وأسلوب ممارستها لعملها، ويضمن لها الاستقلال في مواجهة السلطات المختلفة، ورأينا أن مصر تأخذ بالأسلوب الأول في الحماية الإدارية من خلال أجهزة تابعة للجهاز التنفيذي للدولة.

ورأينا أيضًا أن التطور السريع للمعلوماتية قد أفرز ضرورة وجود هيئة إدارية مستقلة تتولى حماية خصوصية الأفراد عن طريق قانون يخدم مصالح الأفراد، ويوفر لهم

الحماية حيث لا ينبغي أن تكون المعلوماتية وسيلة للانتقاص من الكرامة الإنسانية، أو الحياة الخاصة ومن هنا كانت فكرة مشروعات القوانين في مجال حماية المعلوماتية في البيئة الرقمية، والذي ترجم إلى أرض الواقع لينظم المعاملات الإلكترونية ويضع لها الضوابط والأحكام كما هو الشأن في قانون تنظيم الاتصالات، وقانون مكافحة جرائم تقنية المعلومات.

وقد انقسم هذا البحث إلى ثلاثة مباحث؛ تناول المبحث الأول الحماية الإدارية لخصوصية المعلومات في الولايات المتحدة، في حين عالج المبحث الثاني نظام مفوض المعلومات، وتم تكريس المبحث الثالث للحماية الإدارية للمعلوماتية في مصر.

النتائج:

١- لا يوجد في الولايات المتحدة الأمريكية قانون شامل للحق في الخصوصية المعلوماتية يستطيع أن يغطي كافة أنشطة جمع المعلومات واستخدامها ومعالجتها سواء على المستوى الحكومي أو القطاع الخاص.

٢- أوجب قانون إدارة أمن المعلومات الفيدرالي على الوكالات الاتحادية الالتزام بالضوابط المصممة لضمان سرية المعلومات المتعلقة بالنظام وسلامتها وتوافرها، كما يتعين على الوكالات الاتحادية الالتزام بالمعايير الفيدرالية في معالجة المعلومات وغيرها من المتطلبات التشريعية المتعلقة بنظم المعلومات الفيدرالية مثل قانون الخصوصية الصادر عام ١٩٧٤.

٣- ذهب الفقه الأمريكي إلى ترك الرقابة على نظم المعلومات للقواعد العامة دون حاجة لإنشاء جهة إدارية تتولى هذه المهمة أي أن الولايات المتحدة لم تأخذ بالنظام الفرنسي الذي يعتمد على وجود لجنة تتولى مهمة حماية الخصوصية كما هو الشأن في اللجنة الوطنية للمعلوماتية والحريات في فرنسا.

٤- النظام الأمريكي يولي الأهمية في نظرية للضمانات الإدارية لحماية الخصوصية على حرية التعبير وحرية تدفق المعلومات على حساب الخصوصية المعلوماتية.

٥- تقوم الحماية القضائية للحق في الخصوصية في النظام الأمريكي على أساس نظام القضاء الموحد الذي يعتمد على وجود جهة قضائية واحدة هي جهة القضاء العادي التي تتولى الفصل في كافة المنازعات سواء تلك التي تنشأ بين الأفراد أو بينهم وبين الإدارة ويطبق القضاء العادي على المنازعات الإدارية ذات القواعد القانونية التي تحكم منازعات الأفراد.

٦- تبنى النظام القانوني الألماني نظام مفوض المعلومات حيث عهد القانون الألماني الاتحادي الصادر عام ١٩٧٧ بمهمة الرقابة على تطبيق القانون إلى مفوض نظام المعلومات الذي يختص بحماية البيانات.

٧- خول قانون مفوض المعلومات الاسترالي لمفوض المعلومات السلطات اللازمة للقيام بكل ما هو ضروري لأداء الوظائف المنوطة به بموجب هذا القانون.

٨- جعل قانون حرية المعلومات الألماني المعلومات التي تحتفظ بها السلطات العامة متاحة للجميع رغم وجود بعض الاستثناءات.

٩- الهيئات الرقابية إما أن تكون هيئات رقابة إدارية تابعة للجهاز التنفيذي للدولة، أو تكون هيئات خاصة مستقلة عن السلطات الأخرى من خلال إنشائها بتشريع خاص ومصر تأخذ بالأسلوب الأول في الحماية الإدارية من خلال أجهزة تابعة للجهاز التنفيذي للدولة.

١٠- يعتبر الجهاز القومي لتنظيم الاتصالات هو الجهة الإدارية المختصة بتنظيم الاتصالات وحماية الأفراد المستخدمين في بيئة الاتصالات في مواجهة المتحكمين في تلك الخدمات.

١١- منح قانون مكافحة جرائم تقنية المعلومات جهات التحقيق صلاحية حجب المواقع مباشرة وجعل الرقابة القضائية على هذه القرارات رقابة لاحقة.

١٢- أضفى المشرع على الأدلة المستخرجة من الأجهزة والمعدات، والوسائط الإلكترونية، أو النظام المعلوماتي، أو برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات القيمة والحجية المقررة للأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية.

١٣- أجاز قانون مكافحة جرائم تقنية المعلومات التصالح للمتهم في أية حالة كانت عليها الدعوى الجنائية وقبل صدور الحكم البات.

التوصيات:

١- أهمية وجود لجنة مستقلة أو نظام لمفوض المعلومات يختص بالرقابة على نظام المعلومات على نحو يضمن حماية خصوصية الأفراد كما هو الشأن في التشريع المقارن.

٢- ضرورة سن قانون يتعلق بأمن المعلومات ينظم حق الأفراد في طلب للاطلاع على المعلومات المتعلقة بهم وتصحيحها وتعديلها، ويضمن عدم استخدام هذه المعلومات بصورة تسيء إلى أصحابها.

٣- أهمية صدور قانون ينظم حرية تداول المعلومات وطريقة الحصول عليها، والتظلم من رفض إعطائها إعمالاً لحق الحصول على المعلومات الذي كفلته المادة (٦٨) من الدستور.

٤- يتعين وضع ضوابط تحكم حرية التعبير على الإنترنت ومواقع التواصل الاجتماعي بشكل يعمل على تحقيق التوازن بين حرية التعبير وبين حقوق وحريات الأفراد، ويكفل عدم استخدام الإنترنت، ومواقع التواصل الاجتماعي بصورة تسيء إلى سمعة الآخرين تحت ستار حرية التعبير.

٥- ضرورة تدخل المشرع بتعديل تشريعي لقانون مكافحة جرائم تقنية المعلومات لتحديد طبيعة الحجب الذي خوله المشرع لجهة التحقيق المختصة لأن القانون لم يحدد حالات الحجب الكلي والحجب الجزئي؛ ولا ينال من ذلك القول بأن هذا الأمر متروك للائحة التنفيذية للقانون حيث إن اللائحة التنفيذية للقانون تفسر وتوضح نصوص القانون دون أن يكون لها استحداث نص جديد في القانون، أو تعديل نص قائم أو حذفه، هذا فضلا عن أن اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات قد صدرت دون أن تحدد طبيعة الحجب المنصوص عليه في القانون سالف الذكر.

قائمة المراجع:

- د/ أسامة أبو الحسن مجاهد ، حماية المصنفات على شبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٠.
- د/ أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠٥.
- أ.د/ حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، دار النهضة العربية، ١٩٧٨.
- د/ حسن طاهر داود، الحاسب وأمن المعلومات، بدون دار نشر، ٢٠٠٠.
- د/ حيدر محمد حسن الوزان، حماية حرية الرأي في مواجهة التشريع، دار النهضة العربية، القاهرة، ٢٠١٨.
- د/ عبد العزيز محمد سلمان، الحماية الدستورية لحرية الرأي، الهيئة المصرية العامة للكتاب، ٢٠١٧.
- د/ عمر أبو بكر يونس، الجرائم الناشئة عن استخدامات الإنترنت، دار النهضة العربية، ٢٠٠٤.
- د/ عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠.
- أ.د/ غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، ٢٠١٢.
- د/ فاروق الأباصيري، عقد الاشتراك في قواعد المعلومات الإلكترونية، دراسة تطبيقية لعقود الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٣.
- د/ ماجد عمار، المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، ١٩٨٩.
- د/ مجدي محمد أبو العطا، أمن المعلومات والإنترنت، ط١، كمبيوسيانس، ٢٠١٦.
- د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤.
- د/ محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، مطبوعات الكويت، ١٩٩٢.
- أ.د/ محمود أبو السعود حبيب، القضاء الإداري، مطبعة الإيمان، ٢٠٠٦.

- د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، ٢٠١٢.
- د/ يسري حسن القصاص، الضوابط الجنائية لحرية الرأي والتعبير، دار الجامعة الجديدة، الإسكندرية، ٢٠١٤.

رسائل الماجستير والدكتوراه:

- ا. عبد الله ممدوح مبارك، دور شبكات التواصل الاجتماعي في التغيير السياسي، رسالة ماجستير، كلية الإعلام، جامعة الشرق الأوسط، بدون سنة نشر.
- د.أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، ٢٠٠٠.

مقالات في دوريات:

- د/ السيد خليل هيكل، القانون الإداري الأمريكي الجزء الثاني، كيفية الرقابة على القرار الإداري الأمريكي، مجلة العلوم الإدارية، السنة السادسة عشر، العدد الثاني، أغسطس ١٩٧٤، ص ١٣١.
- أ/ حازم عادل، حيثيات حكم القضاء الإداري برفض دعوي حجب " فيس بوك، جريدة اليوم السابع، ٢٠١٥/٨/٢٥، ص١، ٢.
- أ/ محمد طارق، البرلمان يواجه تهديدات " الإنترنت " بـ "قانون مكافحة جرائم المعلومات"، مقال منشور، في جريدة الوطن، ٢٠١٨/٣/٤، ص١.

الأحكام القضائية:

- حكم المحكمة الإدارية العليا، الدعاوى أرقام، ٣٧٧، ٣٧٧٥٩، ٣٨٢٥٩، ٣٨٤٠٠، لسنة ٥٩ إدارية عليا، جلسة ٢٠١٨/٣/٢٤.
- حكم محكمة القضاء الإداري، دائرة المنازعات الاقتصادية والاستثمار، الدعاوى رقم ١٢٦٨٥٥، لسنة ٦٥ ق، جلسة ٢٠١١/٥/٢٨.

فهرس الموضوعات