(ISSN: 2356 - 9492)

وسائل الحماية الدستورية لحرمة الحياة الخاصة في ظل انتشار التكنولوجيا السيبرانية "دراسة مقارنة"

دكتورة/ نورا عيسى زكريا
مدرس بقسم القانون العام
كلية الحقوق – جامعة عين شمس

الملخص باللغة العربية:

يعتبر الحق في الخصوصية من الحقوق الدستورية الأساسية التي تحظى باهتمام دولي كبير. فالخصوصية مرتبطة بوجود الإنسان باعتبارها أساس لحماية كرامة واستقلال الفرد، كما تتصل بها الكثير من الحقوق الأخرى. وبالتالي يجب على المجتمع احترام هذه الخصوصية من أي تعسف أو اعتداء بوضع قواعد دستورية تكفله. ومع تطور تكنولوجيا المعلومات أصبحت عمليات نقل وتبادل المعلومات تتم بسهولة كبيرة، وصارت معظم المعاملات اليومية تتم بشكل رقمي، فأصبحت الشركات والأجهزة المختلفة للدول تمتلك كمية هائلة من البيانات الشخصية للأفراد. وقد أدى ذلك التطور الرقمي الهائل إلى زيادة التحديات التي تواجه الحق في الخصوصية كحق فردي. ونلمس اليوم اتجاه غالبية الدول إلى تعديل تشريعاتها الحالية وسن قوانين شاملة، تعتمد فيها على القواعد المستقر عليها دوليا، وتهدف إلى وضع إطار عام يضمن حماية الحياة الخاصة للأفراد، وضمان خصوصية البيانات الشخصية في ظل التطورات التكنولوجية الحديثة. وسوف نحاول في هذه الدراسة تحليل الأنظمة الدستورية والقانونية المختلفة في هذا المجال، وصولا إلى أفضل الممارسات المطبقة.

مقدمة :

إن الشرائع السماوية ودساتير الدول والمواثيق الدولية تكفل للإنسان الحرية في ممارسة بعض الحقوق اللصيقة بشخصيته. وتأبي النفس البشرية بطبيعتها التدخل في شئونها الخاصة. ويجب على المجتمع احترام هذه الخصوصية باعتبارها جزء أساسي من الوجود الإنساني، يستلزم حمايته من أي تعسف أو اعتداء بوضع قواعد دستورية

تكفله. وعلى مدى الثلاثة الأخيرة، أصبح الحق في الخصوصية يمثل قيد دستوري في غالبية الدول على سلطة الحكومات في مواجهة المواطنين(١).

وعلى الرغم من أهمية هذا الحق والاهتمام الذي حظي به عالمياً، إلا أنه لا يوجد اتفاق فقهي على تعريفه وتحديد نطاقه، خاصة بعد احتلال التكنولوجيا الرقمية مكانة كبيرة في ادارة الدول لخدماتها العامة. فقد بدأ تطبيق الإدارة الإلكترونية في معظم البلدان المتقدمة كوسيلة لتبسيط وتسهيل وصول الخدمات للمستخدم وزيادة كفاءة الإدارات. كذلك بدأت العديد من البلدان النامية في الاتجاه نحو تطبيق التقنيات الحديثة في تشغيل المرافق العامة. وأصبحت شبكة الانترنت ومواقع التواصل الاجتماعي مؤثرة بشكل كبير على المجتمع وأساليب التنشئة الاجتماعية(٢).

والتحليل السليم لفكرة الخصوصية يجب ألا يتم بمعزل عن التطورات التي تحدث في المجتمعات. فمعظم الدساتير تعترف منذ فترة طويلة بالحرية الفردية، وحماية الخصوصية. ولكن مع مرور الوقت يتطور النص القانوني ليراعي الجوانب المختلفة للحياة المجتمعية وما يطرأ عليها من تغيرات.

لذلك فإنه من الضروري تحديد ما يحميه الحق في الخصوصية، والأسس التي يقوم عليها هذا الحق. وسوف نتناول في هذه الدراسة تحليل المناهج المطبقة في الأنظمة القانونية المختلفة للوصول الي معيار قابل للتطبيق في ظل التطورات التكنولوجية.

---

(1) Jed Rubenfeld, "The Right of Privacy", Harvard Law Review , Feb., 1989, Vol. 102, No. 4 (Feb., 1989), pp. 737-807.

(٢) على سبيل المثال فإن إحصائيات وسائل التواصل الاجتماعي في مصر من أكتوبر ٢٠١٨ إلى أكتوبر ٢٠١٩. توضح أن مستخدمي Facebook بلغت نسبتهم 74.67٪، ويوتيوب لديه ١٨,١٣٪ مستخدم وTwitter لديه ٢,٩٦٪ مستخدم. انظر: Statecounter, "Social Media States Egypt"، October 2019 < https://gs.statcounter.com/social-media-stats/all/egypt>. كما أكدت صحيفة لوموند العالمية أن فيسبوك يجتاز ملياري مستخدم. وقد وصل عدد المستخدمين في فرنسا، حوالى ٣٣ مليون مستخدم نشط شهريًا انظر: Tual Morgane," Facebook passe la barre des deux milliards d'utilisateurs, Le Monde, 27 juin 2017, disponible sur : http://www.lemonde.fr/pixels/article/2017/06/27/facebook-passe-la-barre-des-2-milliards-dutilisateurs_5152063_4408996.html > ووفقًا لوزارة الاقتصاد الفرنسية، يستخدم ٧٤٪ من سكان فرنسا هذه الوسائل الجديدة للتواصل، منهم ٦٣٪ لإجراء اتصالات مع السلطات العامة.

(ISSN: 2356 - 9492)

فصل تمهيدي

المدلول العام للحق في الخصوصية المعلوماتية

لا يوجد اتفاق فقهي أو قانوني على تعريف شامل للحق في الخصوصية. ويرجع ذلك من ناحية، الي ارتباط هذا الحق بالثقافة والقيم والأنظمة السياسية السائدة في كل مجتمع، ومن ناحية أخري، بالتطورات التي قد تطرأ على المجتمعات. وسوف نعرض في هذا الفصل للآراء الفقهية المختلفة في هذا الشأن:

المبحث الأول

مفهوم الحق في الخصوصية المعلوماتية

إن كلمة الخصوصية في اللغة مشتقة من الفعل خص، وهي تعني أن ينفرد الشخص بالشيء دون غيره ويجعله خاصا به(٣). أما الخصوصية في الاصطلاح يمكن تعريفها – وفقاً لما ذهب اليه معهد القانون الأمريكي – بأنها حق الشخص في عدم اتصال أموره الي علم الغير أو عدم عرض صورته على أنظار الجمهور(٤). وانتهج هذا التعريف معيار واسع، حيث يدخل في إطاره كافة الأمور المتصلة بالإنسان.

وهناك اتجاه من الفقه يضيق من تعريف الخصوصية، فينظر لها باعتبارها حق من حقوق الإنسان الذي يتمتع به كل شخص بحكم وجوده. ويمكن أن تشمل الخصوصية وفقا لهذا الاتجاه الحق في السلامة الجسدية والاستقلال الشخصي وتقرير المصير والسرية. ويذهب هذا الاتجاه الي وجوب تحديد الحق في الخصوصية على أساس كل حالة على حدة(٥).

وعلى الرغم من أن مصطلح الخصوصية قد يبدو حديث النشأة، إلا أن مضمون الحق في الخصوصية يعد من أقدم وأعرق الحقوق الشخصية، حيث يرتبط بوجود الإنسان(٦).

---

(٣) مجمع اللغة العربية، المعجم الوجيز، ص ١٨٩.

(٤) د/ مصطفى احمد، "الحياة الخاصة ومسئولية الصحفي"، دار الفكر العربي، ٢٠٠١، ص ٥٣.

(5) Krishnadas Rajagopal, “The lowdown on the right to privacy”, *In* The Hindi, July, on : https://www.thehindu.com.

(٦) د/ علي أحمد عبد الزعبي، " حق الخصوصية في القانون الجنائي "، المؤسسة الحديثة للكتاب، ٢٠٠٦.

ويربط الفقه الحديث فكرة الحق في الخصوصية المعلوماتية بحق الأفراد في تحديد نطاق وصول المعلومات المرتبطة بحياتهم الشخصية والخاصة واستخدامها ومعالجتها بشكل الكتروني. فيشمل التعريف المستحدث ضمان عدم الاطلاع على البيانات الشخصية للأفراد بواسطة عمليات المعاجلة الإلكترونية لها.

وفي هذا الصدد اتجه بعض الفقه الي ربط تعريف الحق في الخصوصية المعلوماتية بتقنية المعلومات. فنجد أن الفقيه الأمريكي ألان ويستن Alan F. Westin قد عرف الخصوصية المعلوماتية في كتابه "الخصوصية والحرية" بانها حق الفرد في التحكم في المعلومات المتعلقة به وتحريرها وإدارتها وحذفها، وتقرير متى وكيف ومدى اتصال تلك المعلومات إلى الآخرين"(٧).

وقد ورد تعريف للحق في الخصوصية المعلوماتية في كتاب الفقيه أرثر ميلر Arthur R. Miller المعنون "الاعتداء على الخصوصية" باعتبارها قدرة الشخص على السيطرة على نشر المعلومات المتعلقة به(٨).

وقد عرض الفقيه ميلر لفكرة استخدام المعلومات الخاصة بدلاً من الحصول عليها. وتدور فكرة تنظيم المعلومات القائمة على الاستخدام فقط، حول فرضية أن المعلومات الشخصية تستخدم لغرض معين وتوجه إلى جمهور محدود وتلتزم الجهة التي تستخدم المعلومات بعدم استخدامها إلا في الغرض المحدد أو الكشف عنها لأي جهة أخرى. فعلي سبيل المثال يري ميلر وجوب عدم استخدام بيانات الائتمان الممنوحة للبنك – لأغراض الحصول على قرض مثلا – لأي غرض آخر أو رؤيتها من قبل أي جمهور آخر، فلا ينبغي إتاحة بيانات الائتمان لأصحاب الشركات أو المشروعات الذين يتعاملون مع البنك(٩).

(7) Alan F. Westin, Daniel J. Solove, “Privacy and Freedom”, Ig Publishing, 2015, 500 P.

(8) Michael S. Josephson, “The Assault on Privacy by Arthur R. Miller”, Michigan Law Review , Jun., 1971, Vol. 69, No. 7 (Jun., 1971), pp. 1389-1397.

(٩) نفس المرجع السابق.

(ISSN: 2356 - 9492)

كما يمكن تعريف انتهاك الحق في الخصوصية وفقا لما ورد ببعض منشورات منظمة الأمم المتحدة، بأنه التدخل التعسفي في خصوصيات أي شخص أو أسرته أو بيته أو مراسلاته، بما في ذلك الاعتداء على شرفه وسمعته. ولكل شخص الحق في الحماية القانونية من مثل هذا التدخل أو الاعتداء.

وقد ذهب اتجاه من الفقه إلى أن التدخل في المراسلات والاتصالات الشخصية أو جمع البيانات المتعلقة بها، دون التعرض لمضمونها، لا يشكل في حد ذاته انتهاكا للحق في الخصوصية(١٠).

ولكن الرأي السابق قد تم انتقاده استنادا إلى أن تجميع المعلومات أو البيانات عن المراسلات والاتصالات الشخصية، والتي يطلق عليها "البيانات الوصفية" قد يعطي فكرة عن سلوك الفرد، وعلاقاته الاجتماعية، بشكل قد يتجاوز المعلومات التي يمكن الوصول لها من خلال التدخل في محتوى الاتصالات الخاصة.

كذلك ذهبت محكمة العدل التابعة للاتحاد الأوروبي في أحد أحكامها(١١) إلى أن البيانات الوصفية للاتصالات قد تتيح استخلاص استنتاجات دقيقة جداً بشأن الحياة الخاصة للأشخاص الذين تم الاحتفاظ ببياناتهم. وقد أدى الاعتراف بهذه النظرية إلى اتخاذ مبادرات من الحكومات لإصلاح السياسات والممارسات القائمة في الواقع العملي لضمان حماية أقوى للخصوصية.

وبالتالي فإن أي تجميع للبيانات الوصفية للاتصالات الشخصية أو احتفاظ بها قد يمثل تدخلاً في الخصوصية، سواء تم الرجوع إلى تلك البيانات أو استخدامها لاحقاً.

(10) Human Rights Council, “The right to privacy in the digital age”, Report of the Office of the United Nations High Commissioner for Human Rights, Twenty-seventh session, Agenda items 2 and 3, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General.

(11) Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, paras. 26-27, and 37.

وفي ذات الإطار فإن التدخل في الحياة الخاصة لا يعد انتهاك لحق الفرد في الخصوصية إلا إذا تم بشكل تعسفي أو غير قانوني. وقد أوضحت اللجنة المعنية بحقوق الإنسان التابعة للأمم المتحدة في تعليقها العام رقم ١٦[١٢] أن عبارة "غير قانوني" تعني ضمناً أنه لا يمكن أن يحدث أي تدخل في الحياة الخاصة إلا في الحالات التي ينص عليها القانون. فلا يمكن أن يتم التدخل الذي تأذن به الدول إلا على أساس القانون الذي يجب أن يمتثل بدوره لأحكام المواثيق الدولية المنظمة لحقوق الإنسان وأهدافها وغاياتها. وبعبارة أخرى، فإن التدخل المسموح به بموجب القانون الداخلي للدول قد يكون غير قانوني إذا كان ذلك القانون الداخلي يتعارض مع أحكام الدساتير المحلية أو المواثيق الدولية. فبذلك يمكن أن تمتد عبارة "التدخل التعسفي" لتشمل التدخل المنصوص عليه في القانون الوطني إذا خالف هذا الأخير ما جاء بدستور الدولة أو المواثيق الدولية. وأشارت اللجنة أن الغرض من الأخذ بهذا المفهوم هو ضمان أن يكون التدخل – حتى الذي ينص عليه القانون – متفقا مع القواعد المتعارف عليها دوليا وفي حدود المعقول. وقد فسرت اللجنة مفهوم المعقولية في هذا الإطار بأنها تشير إلى أن أي تدخل في الخصوصية يجب أن يكون متناسبا مع الغاية المنشودة وأن يكون ضروريا وفقا لظروف كل حالة.

المبحث الثاني
أنواع البيانات الخاصة

تقوم الأنظمة المعلوماتية على تجميع عدد ضخم من المعلومات في مجالات محددة وحفظها على الحاسب الآلي. وقد أدي التطور في تقنيات تكنولوجيا المعلومات إلى إنشاء ما يعرف ببنوك المعلومات[١٣]. كما أصبح تبادل المعلومات الشخصية عبر شبكة

(12) Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI, para.3, 4.

(١٣) الدكتور/ حسام الدين الأهواني، "الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني"، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، يناير ويوليو ١٩٩٠، العددان الأول والثاني، السنة الثانية والثلاثون، ص ٧ وما بعدها.

(ISSN: 2356 - 9492)

الإنترنت يتم بسهولة وسرعة فائقة بشكل يجعل المعلومات الخاصة بالأفراد محل لإساءة الاستعمال.

وقد أشار البعض إلى أن الإفصاح عن المعلومات الشخصية وتبادلها عن طريق الوسائل الإلكترونية يعد تصرف واع من جانب الأفراد من خلاله يتم طوعا اتاحة معلومات عن أنفسهم مقابل الوصول الرقمي إلى السلع والخدمات والمعلومات.

وفي هذا الصدد، يثار التساؤل حول مدى إدراك المستهلكين لأهمية البيانات والمعلومات التي يقومون بالإفصاح عنها، وعن وسائل استخدامها ومن يحق له الاطلاع عليها. وتشير أحد التقارير الصادرة عن الحكومة الأمريكية، إلى أن البيانات الضخمة التي يتم تجميعها، يكون من الصعب جدا الاحتفاظ بها سرية. كما أنه من الناحية العملية، فإن الاهتمام بتعزيز القدرة على تجميع ودمج البيانات أكبر بكثير من الاهتمام بالوسائل التكنولوجية التي تعزز الخصوصية. وعلاوة على ذلك، أشار التقرير إلى أن التركيز على مراقبة وجمع البيانات الشخصية والاحتفاظ بها – على الرغم من أهميته في مجالات كثيرة – إلا أن تأثيره السلبي على الحق في الخصوصية لا يمكن الالتفات عنه. ويرجع ذلك إلى أن البيانات الضخمة التي يتم تجميعها عبر الوسائط الالكترونية تتيح استخدامات جديدة وغير منضبطة لها بشكل غير متوقع مما يصعب معه السيطرة عليها[١٤].

وتتنوع البيانات والمعلومات التي يمكن أن تشكل تهديدا لخصوصية الإنسان. فبالرجوع إلى تعريفات الخصوصية، نجد أنها ترتبط ارتباطا وثيقا بالمعلومات من حيث التعريف. فاتصال الخصوصية بالمعلومات يعني أنه من الممكن التمييز بين فئات مختلفة من هذه المعلومات والبيانات. فعلى سبيل المثال هناك معلومات متعلقة بالاتصالات الخاصة، ومعلومات متعلقة بخصوصية الجسم، ومعلومات الشخصية،

(14) Executive Office of the President of the United States, “Big Data: Seizing Opportunities, Preserving Values”, May 2014, on: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf , p. 54.

ومعلومات متعلقة بالممتلكات الشخصية. وسيجري تناول كل فئة من هذه الفئات بإيجاز[١٥].

أولا: الاتصالات الخاصة

يقصد بعملية الاتصال انتقال المعلومات من مرسل إلى متلقي عن طريق وسيلة اتصال. وهناك اتصال شخصي مباشر يتم بين عدد من الأشخاص بدون وسيط عن طريق استخدام الكلمات أو الحركات أو الإشارات. ويوجد ايضا الاتصال الشخصي غير المباشر كنوع من أنواع الاتصال الذي يتم بين مجموعة من الأشخاص بواسطة استخدام الوسائل التكنولوجية لإرسال الرسائل واستقبالها.

والمقصود بالاتصالات الخاصة في هذا الموضع هي جميع أشكال التواصل الشخصي التي يرغب الشخص في الحفاظ عليها وعدم إطلاع الغير عليها. فتشمل هذه الفئة جميع الاتصالات السلكية واللاسلكية وكذلك أي عملية الكترونية تتم عن طريق إرسال، أو استقبال، أو تداول، أو تبادل معلومات أو بيانات باستخدام أحد الوسائط السلكية أو اللاسلكية.

ثانيا: المعلومات المتعلقة بخصوصية الجسد

يقصد عادة بالمعلومات المتعلقة بخصوصية الجسد المعلومات الطبية الخاصة بالأشخاص. وتتمتع هذه المعلومات بحماية قانونية خاصة في معظم تشريعات الدول. فالقانون الإنجليزي – على سبيل المثال – يمنح للأشخاص الحق في أن يتم إبلاغهم بطبيعة المرض وآثاره، ويتضح ذلك في قضية Csoma ضد دولة رومانيا والتي قضت فيها المحكمة الأوروبية[١٦] بمسئولية الدولة عن انتهاك حق سيدة في الحياة الخاصة عندما فشل الأطباء في الحصول على موافقة منها أو شرح خيارات العلاج قبل إجراء العملية، مما أدى إلى استئصال الرحم لإنقاذ حياتها وجعلها غير قادرة على الإنجاب.

(15) J. J. BRITZ, "TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges to the Information Profession", Department of Information Science University of Pretoria 0002 Pretoria, South Africa, on : http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html.

(16) The European Court of Human Rights, Case of Csoma v. Romania, Strasbourg, 15 April 2013.

(ISSN: 2356 - 9492)

كذلك يعطي القانون الإنجليزي للفرد الحق في عدم إجباره على الإفصاح عن حالته الصحية للآخرين. ويرد استثناء وحيد على المبدأ السابق وهو عندما تكون صحة الآخرين أو حياتهم معرضة للخطر بسبب هذا المرض. ومثال على ذلك، إذا كان الشخص مصابا بفيروس معدي قد يؤدي إلى إصابة أشخاص آخرون، يجوز في هذه الحالة الإفصاح عن طبيعة مرضه استثناء من مبدأ الخصوصية.

ونجد تطبيقات للاستثناء السابق في قوانين أخرى، فعلى سبيل المثال، ينص القانون البلجيكي على أن يتم إخضاع الأطفال بشكل إجباري للأشعة السينية للوقاية من السل، ولا يشكل ذلك انتهاكا للحق في الحياة الخاصة والأسرية لاستهدافه غاية مشروعة. وفي هذا الشأن قضت المحكمة الأوروبية(١٧) برفض دعوى أقامها أبوين ضد الحكومة البلجيكية، يدعون فيها انتهاك الحكومة للحق في خصوصية جسد طفلهم. فقد ألزمتهم الحكومة البلجيكية بدفع غرامة لرفضهم إخضاع طفلهم للأشعة الشار اليها بالمخالفة للقانون البلجيكي. وفي هذا الصدد ذهبت المحكمة الأوروبية إلى أنه لدى تقييم ضرورة التدخل في الحياة الخاصة، يجب أن نضع في الاعتبار الغاية وراء هذا التدخل. وبناء على ذلك، رأت المحكمة أن التدخل في القضية المذكورة متناسب مع الهدف المنشود وضروريا لحماية الصحة العامة في المجتمع بالمعنى المقصود في الفقرة ٢ من المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان.

ولكن من جهة أخرى، فإن أي تدخل طفيف يؤثر على السلامة البدنية أو العقلية للشخص قد يمثل انتهاكاً للحق في خصوصية الجسد إذا ما تم ضد إرادة الشخص. ففي قضية Storck ضد دولة ألمانيا(١٨)، تم إعطاء سيدة أدوية معينة بشكل متكرر ضد إرادتها، وهو ما رأته اللجنة الأوروبية لحقوق الإنسان بمثابة انتهاك للمادة ٨ من الاتفاقية الأوروبية.

(17) The European Court of Human Rights, Case of Roger ACMANNE and others v. BELGIUM, 10 December 1984.
(18) The European Court of Human Rights, CASE OF STORCK v. GERMANY, STRASBOURG,16 June 2005.

كذلك يعد انتهاكا لخصوصية الجسد كل إجبار للأشخاص على الخضوع لفحص طبي دون إرادتهم. فقد خلصت لجنة الأمم المتحدة لحقوق الإنسان إلى أن محكمة محلية في دولة ألمانيا منحت طبيباً نفسياً سلطة تقييم الحالة البدنية والعقلية لشخص ما، وذلك يمثل انتهاك للحق في خصوصية الجسد. وفي هذا الشأن، قررت اللجنة أن قرار المحكمة جاء دون الاستماع للشخص المعني، ودون وجود سبب كافٍ للشك في قدرتها، مما يجعل حكم المحكمة غير متناسب مع الغاية المنشودة(١٩).

ثالثا: المعلومات الشخصية

تشير المعلومات الشخصية إلى فئات المعلومات التي تتعلق بشخص معين دون غيره. ومن أمثلة المعلومات الشخصية الاسم والعنوان وبيانات الحسابات البنكية.

ويشتق من المعلومات الشخصية المعلومات المتعلقة بالممتلكات الخاصة. فهذه المعلومات ترتبط ارتباطا وثيقا بحق الملكية. فالأصل أن يكون من حق الإنسان أن يتحكم في المعلومات المتعلقة بممتلكاته الشخصية. فله الحق في عدم الإفصاح عن حجمها أو وصفها أو مكانها إلا في الحالات التي يحددها القانون مثل حالات الإقرارات الضريبية للوفاء بالحقوق المالية للدولة.

والخلاصة أن المعلومات الشخصية – بما في ذلك الصور الشخصية والرسائل الخاصة والسجلات الطبية وغيرها – يجب ألا يتم الإفصاح عنها دون إذن من صاحبها، إلا في ظروف معينة. فلا يحق لأي شخص أو أي جهة التدخل في الحياة الشخصية للأفراد في غير الحالات التي تجيزها القوانين الحاكمة.

وقد فسرت المحاكم الإنجليزية مفهوم "الحياة الخاصة" تفسيراً واسعاً جداً ليشمل أمور غير مألوفة مثل الحق في تحديد التوجه الجنسي الخاص، ونمط الحياة، وطريقة اللباس والمظهر. كما يشمل هذا النوع كذلك أمور أخرى كالحق في حرمة الجسد، والحق في المشاركة في الأنشطة الاقتصادية والاجتماعية والثقافية والترفيهية الأساسية.

(19) Human Rights Committee, Case of M.G. v. Germany, 2006, on: https://tbinternet.ohchr.org.

(ISSN: 2356 - 9492)

المبحث الثالث
الأمن السيبراني

يمكن تعريف الأمن السيبراني بأنه جمع الأدوات والسياسات والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتكنولوجيات التي يمكن استخدامها لحماية البيئة الإلكترونية وأصول المستخدمين(٢٠).

وتشمل تدابير حوكمة الأمن السيبراني الجوانب التقنية، والتنظيمية، والسياسية، والقانونية. وتتناول الجوانب التقنية لإدارة الأمن السيبراني وضع وتنفيذ تدابير الحماية التقنية لنظم الحواسيب والهياكل الأساسية للشبكات، بينما تتناول الجوانب التنظيمية تطوير القدرات المؤسسية لتعزيز الأمن السيبراني، مثل وضع القوانين ومنظمات الإنفاذ وكذلك تطوير القدرات المؤسسية بما في ذلك إنشاء أفرقة الاستجابة للطوارئ الحاسوبية (CERTs) لتقديم خدمات حيوية مثل الوقاية والإنذار المبكر، والكشف عن حوادث الأمن السيبراني وإدارتها. وتتناول الجوانب السياسية والقانونية لإدارة الأمن السيبراني السياسات والتدابير القانونية التي تهدف إلى تعزيز الأمن السيبراني.

وعادة ما تعتبر التدابير القانونية من بين الجوانب الأكثر أهمية في مكافحة الجريمة السيبرانية. وتشمل هذه التدابير وضع قوانين تحظر الأعمال التي تنتهك أمن أو سلامة أو توافر البيانات والنظم أو الشبكات الحاسوبية، والهجمات على الهياكل الأساسية الحيوية للمعلومات. وتشمل أيضاً تدابير قانونية لتيسير التعاون عبر الحدود في مجال الأمن السيبراني بما في ذلك منع الأفعال المحظورة والتحقيق فيها وملاحقتها قضائيا(٢١).

الباب الأول
الأصول الدولية والدستورية للحق في الخصوصية

تحتل الحقوق والحريات الأساسية للإنسان مكانة اجتماعية رفيعة. ويعتبر الحق في الخصوصية أحد أهم هذه الحقوق، باعتباره من الحقوق اللصيقة بشخص الإنسان. وقد

(20) Uchenna Jerome Orji, "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?", Article *In* Masaryk University Journal of Law and Technology · September 2018, p. 93.

(٢١) نفس المرجع السابق، ص ٩٤.

أولى المجتمع الدولي اهتماما كبيرا للحقوق والحريات الأساسية للإنسان كضمانة لتحقيق العدالة والسلم الدولي. كما تلتزم الدول باتخاذ التدابير اللازمة في قوانينها الداخلية لحماية تلك الحقوق والحريات. لذلك حرصت دساتير غالبية الدول على الاعتراف بالحق في حماية الحياة الخاصة وإقرار الضمانات اللازمة لها، بالإضافة إلى وضع قواعد لتجريم أي اعتداء على هذا الحق أو تدخل غير مشروع ووسائل التعويض عن الضرر.

وسوف يتناول هذا الباب الحماية الدولية للحق في الخصوصية بموجب المواثيق الدولية في فصل أول، ثم التنظيم الدستوري لهذا الحق في دساتير الدول المختلفة في فصل الثاني.

الفصل الأول

الحماية الدولية للحق في الخصوصية

تزخر المواثيق الدولية بالنصوص التي تكفل صون حرمة الحياة الخاصة وتُحرم اختراقها وتُجرم أي عمل من شأنه التعدي على خصوصية الأفراد. وقد حظي الحق في الخصوصية باهتمام كبير من جانب المنظمات الدولية والإقليمية على حد سواء. ولكن الثورة التكنولوجية أصبحت تشكل تهديدا واضحا على خصوصية الأفراد.

وفي هذا الإطار يحظى الحق في الخصوصية باهتمام كبير من جانب المنظمات الدولية. وسوف نناقش في هذا الفصل مدى ملائمة النصوص التي أقرتها المواثيق الدولية والإقليمية لحماية الحق في الخصوصية في ظل انتشار التكنولوجيا الرقمية.

المبحث الأول

دور المواثيق الدولية في حماية الحق في الخصوصية

يوفر القانون الدولي لحقوق الإنسان إطاراً واضحاً وعالمياً لتعزيز وحماية الحق في الخصوصية. وقد نصت العديد من المواثيق الدولية على حماية هذا الحق، مما يعبر عن الاهتمام الذي توليه الدول لحماية خصوصية الأفراد. ويثبت هذا الاهتمام من خلال التزام الدول بمراجعة وتعديل نصوصها الداخلية لتتوافق مع نصوص الاتفاقيات الدولية التي تكون الدولة طرفا فيها وسوف نعرض لأبرز هذه المواثيق في المطالب الآتية:

- المطلب الأول: الإعلان العالمي لحقوق الإنسان

(ISSN: 2356 - 9492)

– المطلب الثاني: العهد الدولي للحقوق المدنية والسياسية

– المطلب الثالث: الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم

المطلب الأول

الإعلان العالمي لحقوق الإنسان

اهتمت منظمة الأمم المتحدة منذ نشأتها بإصدار إعلانات الحقوق والاتفاقيات الدولية المتعلقة بحقوق الإنسان. وقد قررت لجنة حقوق الإنسان التابعة لمنظمة الأمم المتحدة اصدار قائمة للحقوق والحريات الأساسية، تسمى الإعلان العالمي لحقوق الإنسان وذلك بموجب القرار رقم ٢١٧ بتاريخ ١٠ ديسمبر ١٩٤٨ في دور الانعقاد العادي الثالث.

ويعتبر الإعلان العالمي لحقوق الإنسان وثيقة بارزة في تاريخ حقوق الإنسان. وقد تمت صياغته بواسطة ممثلون من خلفيات قانونية وثقافية مختلفة من جميع أنحاء العالم. وقد أعلنت الجمعية العامة للأمم المتحدة في باريس في ١٠ ديسمبر أنه يعد معيار مشترك لجميع الشعوب وجميع الأمم. وقد تحدد فيه – للمرة الأولي – حقوق الإنسان الأساسية التي ينبغي أن تحظى بحماية عالمية، كما تمت ترجمته إلى أكثر من ٥٠٠ لغة. وقد صدقت مصر على هذا الإعلان وبالتالي تلتزم بكافة نصوصه.

وفيما يتعلق بالحق في الخصوصية جاءت المادة ١٢ من الإعلان العالمي لحقوق الإنسان لترسخ مبدأ الخصوصية وتلزم الدول المصدقة على الإعلان بعدم السماح بانتهاك هذا الحق. ونصت المادة المشار اليها على أنه "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".[٢٢]

ويتضح من المادة السابقة أن الإعلان العالمي لحقوق قد وضع التزاما عاما على كافة الدول الأعضاء بوضع ضمانات تكفل حماية الحياة الخاصة في تشريعاتها الداخلية.

المطلب الثاني

(٢٢) راجع الموقع الرسمي لمفوضية الأمم المتّحدة لحقوق الإنسان (https://www.ohchr.org)

العهد الدولي للحقوق المدنية والسياسية

العهد الدولي للحقوق المدنية والسياسية هو معاهدةٌ متعَدّدة الأطراف تم اعتمادها وعرضها للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم ٢٢٠٠ ألف (د-٢١) المؤرخ في ١٦ ديسمبر ١٩٦٦. وقد انضمت مصر لهذه المعاهدة وتلتزم بما جاء بها من نصوص.

تضمنت نصوص العهد الدولي على كفالة وحماية الحق في حماية الحياة الخاصة للأفراد، حيث تنص المادة ١٧ منه على أن "لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شئون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

ومن جانب آخر نصت ذات المادة بطريق غير مباشر على التزام الدول الأعضاء بتعديل تشريعاتها أو سن تشريعات جديدة لكفالة حماية الحق في الخصوصية، فتنص الفقرة الثانية من المادة ١٧ على أنه من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس.

ونشير إلى أن العهد الدولي يتمتع بقوة أدبية على الصعيد الدولي، بحيث تسعي معظم الدول الى جعل تشريعاتها متسقة مع أحكامه.

المطلب الثالث

الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم

انضمت مصر أيضا إلى الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم. وقد تم اعتماد هذه الاتفاقية بقرار الجمعية العامة للأمم المتحدة رقم ٤٥ بتاريخ ١٨ ديسمبر ١٩٩٠. وتهدف الاتفاقية إلى تنظيم وضمان حقوق العمال المهاجرين وأفراد أسرهم والاعتراف الدولي بها.

وفيما يتعلق بالحق في الحياة الخاصة، فقد جاءت المادة ١٤ لتنص على عدم جواز تعرض العامل المهاجر أو أي فرد من أسرته للتدخل التعسفي أو غير المشروع في حياته الخاصة أو في شئون أسرته أو بيته أو مراسلاته أو اتصالاته الأخرى، أو

(ISSN: 2356 - 9492)

للاعتداءات غير القانونية على شرفه وسمعته. ويحق لكل عامل مهاجر ولكل فرد من أسرته التمتع بحماية القانون ضد هذا التدخل أو هذه الاعتداءات.

ويقصد بالعامل المهاجر الشخص الذي سيزاول أو يزاول أو ما برح يزاول نشاطا مقابل أجر في دولة ليس من رعاياها.

المبحث الثاني

الإطار الإقليمي لحماية الحق في الخصوصية

هناك مجموعة من الصكوك الإقليمية الهامة التي تتناول تنظيم الحق في حماية الحياة الخاصة في مناطق معينة تجمعها قواسم مشتركة. وتهدف هذه المعاهدات بصفة عامة إلى تعزيز وحماية حقوق الإنسان الأساسية وتحديد الإطار الإقليمي للحفاظ عليها.

المطلب الأول

الاتفاقيات الإقليمية غير الملزمة لمصر

من أبرز الاتفاقيات الإقليمية التي تعرضت لموضوع الحق في الخصوصية، الاتفاقية الأوروبية لحقوق الإنسان والاتفاقية الأمريكية لحقوق الإنسان. وعلى الرغم من عدم التزام مصر بهذه المعاهدات، إلا انه من الضروري إلقاء الضوء على النصوص المنظمة للحق في الخصوصية الواردة بها للوقوف على الموقف الدولي والإقليمي في هذا الشأن.

أولا: الاتفاقية الأوروبية لحقوق الإنسان

تعد الاتفاقية الأوروبية لحقوق الإنسان من أهم الاتفاقيات الإقليمية الدولية. وقد صدرت هذه الأخيرة بعد أن وقعت عليها مجموعة من الدول الأوربية المنضمة للمجلس الأوروبي في مدينة روما بإيطاليا بتاريخ ٤ نوفمبر ١٩٥٠.

تنص "الاتفاقية الأوروبية لحقوق الإنسان" على عدد من الحقوق والحريات الأساسية مثل، الحق في الحياة، وحظر التعذيب، وحظر الرق والعمل القسري، والحق في الحرية والأمن، والحق في محاكمة عادلة، وعدم المعاقبة بدون قانون، والحق في احترام الحياة الخاصة والأسرية، وحرية الفكر، والوجدان والدين، وحرية التعبير، وحرية التجمع وتكوين

الجمعيات، والحق في الزواج، والحق في المحاكمة العادلة، وحظر التمييز. وتنظم البروتوكولات الإضافية للاتفاقية المزيد من الحقوق.

وتتعهد الدول الأطراف بتأمين هذه الحقوق والحريات لكل شخص في نطاق ولايتها. ولضمان مراعاة الالتزامات التي تَعهد بها الأطراف، أنشئت المحكمة الأوروبية لحقوق الإنسان في ستراسبورغ بدولة فرنسا. وتتناول هذه المحكمة الالتماسات الفردية والالتماسات المقدمة من الدول. ويجوز للمحكمة أيضا، بناء على طلب لجنة وزراء مجلس أوروبا، أن تقدم فتاوى بشأن تفسير الاتفاقيات والبروتوكولات الملحقة بها. وللجنة الوزراء أيضا سلطة طلب تفسير الحكم من المحكمة.

وفيما يتعلق بالحق في الخصوصية فقد نصت المادة ٨ من هذه الاتفاقية على الآتي:

"١- لكل شخص الحق في احترام حياته الخاصة والأسرية، ومنزله ومراسلاته.

٢- لا يجوز أن تتدخل سلطة عامة في ممارسة هذا الحق إلا إذا كان ذلك وفقاً للقانون، وضرورياً في مجتمع ديمقراطي لمصلحة الأمن الوطني أو السلامة العامة أو الرفاه الاقتصادي للبلد، أو لمنع الفوضى أو الجريمة، أو لحماية الصحة أو الأخلاق، أو لحماية حقوق الآخرين وحرياتهم."

وبالرجوع إلى مضمون الفقرة الأولى من المادة السابقة، نجد أنها أقرت الحق في احترام الحياة الخاصة والأسرية وحرمة المسكن وسرية المراسلات بالنسبة لجميع المواطنين المتواجدين على إقليم الدول الأطراف في الاتفاقية الأوروبية. ويساوي النص بين مواطني الدول الأعضاء وغير الأعضاء في الاتفاقية طالما كانوا مقيمين في إحدى الدول الأطراف فيها. وتنتهج الاتفاقية في هذا الصدد منهج واسع في حماية الحق في الخصوصية.

ثانيا: الاتفاقية الأمريكية لحقوق الإنسان

إن الاتفاقية الأمريكية لحقوق الإنسان معروفة أيضاً باسم "ميثاق سان خوسيه"، وهي من الصكوك الإقليمية لحقوق الإنسان. وقد تم اعتمادها من قبل العديد من البلدان. وقد نظمت الحق في الخصوصية في المادة ١١ منها والتي نصت على الآتي:

(ISSN: 2356 - 9492)

"١- لكل شخص الحق في أن يُحترم شرفه وأن تُعترف له بكرامته.

٢- لا يجوز أن يكون أحد موضع تدخل تعسفي أو مسيء في حياته الخاصة أو أسرته أو منزله أو مراسلاته أو من الاعتداءات غير القانونية على شرفه أو سمعته.

٣-لكل فرد الحق في حماية القانون من مثل هذا التدخل أو الاعتداء."

ونلاحظ أن الاتفاقية الأمريكية انتهجت ذات المعيار المتبع في الاتفاقية الأوروبية لحقوق الإنسان، حيث شملت بالحماية كافة الأفراد المقيمين في الدول الخاضعة لأحكام هذه الاتفاقية. كذلك نصت بشكل واضح على حماية الحياة الخاصة للأفراد من أي تدخل تعسفي فيها نما في ذلك الحياة الأسرية وحرمة المنزل والمراسلات الخاصة.

المطلب الثاني

الاتفاقيات الإقليمية الملزمة لمصر

أسهمت مصر بدور كبير في تأسيس الاتحاد الإفريقي الذي جاء خلفاً لمنظمة الوحدة الإفريقية. كما كانت مصر من الدول المؤسسة لمنظمة الوحدة الإفريقية عام ١٩٦٣. وقد قامت بالتصديق على عدد من الاتفاقيات في إطار الاتحاد، منها ما دخلت حيز النفاذ ومنها التي لازالت في حيز النفاذ المؤقت. ومن بين الاتفاقيات التي تنظم الحق في الخصوصية في إطار الاتحاد الإفريقي، نذكر على سبيل المثال الميثاق الأفريقي لحقوق الإنسان والشعوب والميثاق الإفريقي لحقوق ورفاهية الطفل واتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية. كذلك صدقت مصر على إعلان القاهرة حول حقوق الإنسان في الإسلام باعتبارها عضوا في منظمة مؤتمر العالم الإسلامي. وسوف نعرض فيما يلي لأهم النصوص المنظمة للحق في الخصوصية في المواثيق المشار اليها.

أولا: الميثاق الإفريقي لحقوق الإنسان والشعوب

تم إجازة الميثاق الإفريقي لحقوق الإنسان والشعوب من قبل مجلس الرؤساء الأفارقة بدورته العادية رقم ١٨ في نيروبي "كينيا" في يونيو ١٩٨١. ويعد جميع الدول الأعضاء في منظمة الوحدة الإفريقية، ومن بينهم مصر، أطراف في هذا الميثاق.

ويكتسب الميثاق الإفريقي أهمية خاصة بين المواثيق الإقليمية من حيث أنه يضع إطارا عاما لكافة حقوق الإنسان الأساسية بما يعبر عن قضايا القارة الإفريقية وتطلعاتها في هذا الشأن.

وعلى الرغم من عدم الإشارة بشكل صريح للحق في الخصوصية في مواد الميثاق، إلا أن فكرة الخصوصية بوصفها تمثل جزء من حرية الأفراد يمكن أن تندرج تحت النصوص المنظمة للحقوق والحريات الأساسية. فتنص المادة الرابعة من الميثاق على عدم جواز انتهاك حرمة الانسان، وضرورة ضمان احترام حياته وسلامة شخصه. كما تنص المادة السادسة على عدم جواز حرمان أي شخص من حريته إلا في الحالات التي يحددها القانون. وبذلك يمكن أن يخضع الحق في الخصوصية تحت التفسير الواسع للحق في الحرية الشخصية واحترام الحياة.

ثانيا: الميثاق الإفريقي لحقوق ورفاهية الطفل

تعد جميع الدول الإفريقية أعضاء منظمة الوحدة الإفريقية، ومن بينهم مصر، أطراف في هذا الميثاق. وقد تم إجازة الميثاق الإفريقي لحقوق ورفاهية الطفل عام ١٩٩٠، وبدأ العمل به في ٢٩ نوفمبر ١٩٩٩.

وحرص الميثاق على إقرار حق الطفل في حماية حياته الخاصة، حيث تنص المادة ١٠ منه على عدم جواز تعرُض طفل للتدخل التعسفي أو غير المشروع في خصوصيته أو بيت أسرته أو مراسلاته، أو يكون عرضة للتهجم على شرفه أو سمعته، بشرط أن يكون للآباء أو الأوصياء القانونيين الحق في ممارسة الإشراف المعقول على سلوك أطفالهم، ويكون للطفل الحق في حماية القانون ضد مثل هذا التدخل أو التهجم.

ثالثا: إعلان القاهرة حول حقوق الإنسان في الإسلام

صدقت مصر على إعلان القاهرة حول حقوق الإنسان في الإسلام. وقد تم إجازته من قبل مجلس وزراء خارجية منظمة مؤتمر العالم الإسلامي بالقاهرة في ٥ أغسطس ١٩٩٠.

وقد نظمت المادة ١٨ من الإعلان حماية الحق في الحياة الخاصة للأفراد، حيث أقرت الفقرة الثانية من المادة حق الإنسان في الاستقلال بشئون حياته الخاصة في

(ISSN: 2356 - 9492)

مسكنه وأسرته وماله واتصالاته، ونصت أيضا على عدم جواز التجسس أو الرقابة عليه أو الإساءة إلى سمعته وتجنب حمايته من كل تدخل تعسفي أو غير قانوني.

كما أكدت الفقرة الثالثة من المادة المشار اليها على حرمة المسكن في جميع الأحوال وعدم جواز دخوله بغير إذن أهله أو بصورة غير مشروعة، وعدم جواز هدمه أو مصادرته أو تشريد أهله منه.

رابعا: اتفاقية الاتحاد الإفريقي[٢٣] بشأن الأمن السيبراني وحماية البيانات الشخصية

تمت صياغة اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية في عام ٢٠١١، في إطار الجهود الساعية لوضع هيكل تنظيمي للأمن السيبراني في منطقة أفريقيا. ويتمثل الهدف الرئيسي من الاتفاقية في حماية البيانات الخاصة وتنظيم المعاملات الإلكترونية وتعزيز الحوكمة الإلكترونية والأمن السيبراني ومكافحة الجريمة السيبرانية.

وقد تم تأجيل اعتماد هذه الاتفاقية عدة مرات حتى صدر قرار من الاتحاد الإفريقي باعتمادها في يونيو ٢٠١٤.

وتتناول اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية ثلاثة محاور أساسية هي:

- المعاملات الإلكترونية
- حماية البيانات الشخصية
- الأمن السيبراني والجريمة السيبرانية

ولكن لم تدخل الاتفاقية حيز النفاذ بسبب عدم تصديق غالبية الدول الإفريقية عليها، حيث لم تكن قد أصدرت قوانين لحماية البيانات[٢٤]. ولازالت مصر من الدول التي لم توقع على الاتفاقية اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية.

---

(٢٣) الاتحاد الأفريقي هو هيئة إقليمية حكومية دولية توحد الدول ذات السيادة في القارة الأفريقية بأسرها. تأسس الاتحاد الإفريقي في عام ٢٠٠١ ليحل محل منظمة الوحدة الافريقية. ويقع مقره في اديس ابابا بأثيوبيا. ويضم الاتحاد الإفريقي حاليا ٥٥ دولة افريقية ذات سيادة.

(٢٤) راجع الموقع الرسمي للاتحاد الإفريقي: https://ccdcoe.org

وقد كان العجز في الموارد المالية والقدرات الفنية لدى السلطات الوطنية له تأثير على عدم وجود خطط أو آليات للتصدي للتحديات التي تشكلها التكنولوجيا الحديثة لحماية البيانات(٢٥). وبالتالي لم تُقبل الدول الأعضاء في الاتحاد الإفريقي على التصديق على هذه الاتفاقية والالتزام بوضع نظام قانوني لمكافحة الجريمة السيبرانية.

ونظرا لأهمية هذه الاتفاقية لما تقدمه من إطار تتحدد من خلاله الأهداف المرجوة من المجتمع التكنولوجي في دول إفريقيا، والسبيل إلى تعزيز القوانين الداخلية القائمة في مجال تكنولوجيا المعلومات في الدول الأعضاء، فسوف نلقي الضوء على أهم ما جاء بها.

أكدت الاتفاقية على ضرورة تنظيم مكافحة الجريمة السيبرانية في الدول الأعضاء في الاتحاد الإفريقي، كما نصت على التزام الدول الأعضاء بوضع سياسات داخلية تتضمن قواعد موضوعية واجرائية تضمن الأمن السيبراني من خلال تعديل الأطر القانونية والتنظيمية التي تحكم الأمن السيبراني. ونشير أن هذا النهج أوسع من ذلك الذي اتبعته اتفاقية المجلس الأوروبي بشأن الجريمة الإلكترونية(٢٦)، والتي تتطلب من الدول الأعضاء تجريم الجرائم الحاسوبية عن طريق وضع تدابير قانونية جنائية موضوعية فقط، فضلاً عن وضع آليات للتعاون الدولي لإنفاذ القانون (٢٧).

وقد حددت المادة ١٣ من اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية ستة مبادئ يجب على الدول الأعضاء مراعاتها فيما يتعلق بجمع ومعالجة البيانات الشخصية. وتتمثل هذه المبادئ فيما يلي:

المبدأ الأول: إبداء الموافقة على معالجة البيانات ذات الطابع الشخصي

(25) United Nations Human Rights Office of the High Commissioner, Report of the proceedings of the online expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy (27- 28 May 2020), p. 8.

(26) The Council of Europe Convention on Cybercrime, 23 November 2001: https://rm.coe.int/budapest-convention-in-arabic/1680739173.

(27) Uchenna Jerome Orji, *Ibid*, p. 99.

(ISSN: 2356 - 9492)

تعتبر معالجة البيانات ذات الطابع الشخصي مشروعة إذا وافق عليها الشخص المعني. ويمكن التنازل عن شرط الموافقة إذا كانت البيانات ضرورية في الحالات الآتية:

– الامتثال لالتزام قانوني يخضع له المسئول عن عملية المعالجة،

– لتنفيذ مهمة متعلقة بمصلحة عامة أو لممارسة السلطة الرسمية المخولة للمسئول عن المعالجة أو لطرف ثالث تم الافصاح له بالبيانات،

– لتنفيذ عقد يعتبر الشخص موضوع البيانات طرفا فيه أو من أجل اتخاذ إجراءات تعاقدية بناء على طلب من الشخص المعني بالبيانات قبل إبرام العقد،

– لحماية المصالح الحيوية أو الحقوق والحريات الأساسية للشخص موضوع البيانات.

المبدأ الثاني: مبدأ قانونية وعدالة معالجة البيانات الشخصية

يجب أن يتم جمع البيانات الشخصية وتسجيلها ومعالجتها وتخزينها ونقلها بشكل قانوني وعادل وخالي من الاحتيال.

المبدأ الثالث: مبدأ تحديد الغرض من تخزين البيانات ذات الطابع الشخصي ومعالجتها

يجب أن يكون جمع البيانات لأغراض محددة واضحة ومشروعة، ولا يجوز معالجتها لاحقاً بما يتعارض مع الأغراض المذكورة. كذلك يجب أن تكون البيانات كافية وذات صلة بالأغراض التي من أجلها تم تجميعها ومن ثم القيام بمعالجتها. ويجب ايضا حفظ البيانات لمدة لا تتجاوز المدة المطلوبة لتحقيق الأغراض التي تم من أجلها جمع البيانات ومعالجتها.

ولا يجوز بعد الفترة المحددة للمعالجة الاحتفاظ بالبيانات إلا لتلبية احتياجات محددة لمعالجة البيانات التي تتم لأغراض تاريخية أو إحصائية أو بحثية بموجب القانون.

المبدأ الرابع: مبدأ الدقة في البيانات ذات الطابع الشخصي

البيانات التي يتم تجمعيها يجب أن تكون دقيقة ومحدثة عند الاقتضاء. ويجب اتخاذ كل الخطوات المعقولة لضمان محو أو تصحيح البيانات غير الدقيقة أو غير المكتملة، مع مراعاة الأغراض التي جمعت من أجلها أو التي تمت من أجلها المعالجة.

المبدأ الخامس: مبدأ الشفافية في معالجة البيانات ذات الطابع الشخصي

يتطلب مبدأ الشفافية الكشف الإلزامي عن المعلومات المتعلقة بالبيانات ذات الطابع الشخصي من جانب المسئول عن عملية المعالجة.

المبدأ السادس: مبدأ السرية والتأمين في معالجة البيانات ذات الطابع الشخصي

يجب معالجة البيانات ذات الطابع الشخصي بشكل سري مع توفير الحماية، لا سيما عندما تنطوي المعالجة على نقل البيانات عبر شبكة اتصال. وعندما يتم تنفيذ معالجة لحساب المسئول عن عملية المعالجة، يتعين عليه اختيار معالج تتوفر لديه ضمانات كافية. ويكون لزاما على هذا المسئول وعلى المعالج الامتثال للتدابير الأمنية المنصوص عليها في اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية.

وتُلزم المادة ٣/٢٥ من الاتفاقية الدول الأعضاء بضمان عدم انتهاك التدابير القانونية المقررة في إطار الأمن السيبراني، للحقوق الدستورية للمواطنين، مثل الحق في حرية التعبير، والحق في الخصوصية، والحق في محاكمة عادلة، وغير ذلك من الحقوق الأساسية المحمية بموجب القانون الوطني أو الدولي، بما في ذلك الحقوق التي ينص عليها الميثاق الإفريقي لحقوق الإنسان والشعوب. ويتشابه هذا النص مع المعيار الذي اعتمدته اتفاقية المجلس الأوروبي بشأن الجريمة الحاسوبية، حيث تنص الاتفاقية الأخيرة، على التزام الدول الأعضاء بضمان عدم انتهاك صكوكها الإجرائية – المتعلقة بالملاحقة القضائية للجريمة السيبرانية – لحقوق الإنسان الأساسية.

الفصل الثاني

التنظيم الدستوري للحق في الخصوصية

تعترف معظم الدول بالحق في الخصوصية كحق دستوري. والقاعدة أن الدساتير تعني بوضع المبادئ العامة تاركة المسائل التنظيمية للمشرع العادي. وهناك بعض الدول التي تحيل تنظيم الحق في الخصوصية إلى المشرع العادي دون تحديد أي ضوابط. وسوف يتناول هذا الباب تنظيم الحق في الخصوصية في بعض الدساتير المصرية والمقارنة وصولا إلى أفضل الممارسات في هذا الشأن.

(ISSN: 2356 - 9492)

المبحث الأول

تطور الحماية الدستورية للحق في الخصوصية في مصر

تعتبر الوثيقة الدستورية أهم الأدوات التشريعية باعتبارها أعلي وثيقة قانونية في الدولة. وقد تناولت الدساتير المصرية المتعاقبة المبادئ المتعلقة بحقوق الإنسان وحرياته الأساسية المقررة في المواثيق الدولية المختلفة التي صدقت عليها مصر. وقد حرص الدستور المصري علي حماية حرمة الحياة الخاصة وأفرد لها أقصى درجات الحماية بأن جعل الاعتداء عليها من الجرائم التي لا تسقط الدعوى الجنائية ولا المدنية بشأنها بالتقادم. وعدم سقوط الدعوى بالتقادم يضمن عدم إفلات المسئول من الجزاء.

كما كفل الدستور المصري الحق في التعويض العادل لمن وقع اعتداء على حرمة حياته الشخصية، وسوف نعرض فيما يلي لتطور تنظيم الحق في الخصوصية في أهم الدساتير المصرية.

المطلب الأول

حماية الحق في الخصوصية في الدساتير المصرية السابقة

يعتبر دستور ١٩٧١ من أهم مراحل تاريخ تطور الدساتير المصرية. فقد تم إقراره في عهد الرئيس الراحل محمد أنور السادات بناءا على استفتاء شعبي في ١١ سبتمبر ١٩٧١ وتم تسميته بدستور مصر الدائم. وقد وردت على هذا الدستور عدة تعديلات أهمها التعديل الذي جرى في عام ٢٠٠٥.

وقد تضمن دستور ١٩٧١ عدة ضمانات لحماية الحياة الخاصة. فقد نصت المادة ٥٧ منه على تجريم أي اعتداء علي الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون. كذلك نصت ذات المادة على اعتبار هذا الاعتداء جريمة لا تسقط الدعوي الجنائية ولا المدنية الناشئة عنها بالتقادم، وأكدت على أن الدولة تلتزم بتعويض من وقع عليه الاعتداء بتعويض عادل.

وقد أكدت محكمة النقض هذا المبدأ في أحكامها حيث قضت في حكمها الصادر في ٢٧ يناير ١٩٨٣[٢٨] بأنه "وكان ما نصت عليه المادة ٥٧ من الدستور من أن الاعتداء على الحرية الشخصية يعتبر جريمة لا تسقط الدعوى الجنائية والدعوى المدنية الناشئة عنها بالتقادم، إنما هو صالح بذاته للإعمال من يوم العمل بالدستور دون حاجة لسن تشريع آخر أدنى في هذا الخصوص".

وبعد قيام ثورة ٢٥ يناير تم تعطيل دستور ١٩٧١ في ١٣ فبراير ٢٠١١، وصدر عدد من الوثائق الدستورية سوف نتتبع تنظيم الحق في الخصوصية بها بداية من الإعلان الدستوري الذي أصدره المجلس الأعلى للقوات المسلحة في ٣٠ مارس ٢٠١١ ومرورا بدستور ٢٠١٢ وانتهاءا بالوضع الحالي المقرر في دستور ٢٠١٤.

فعلى الرغم من الطابع المؤقت للإعلان الدستوري الصادر في ٣٠ مارس ٢٠١١، إلا أنه لم يغفل التأكيد على حماية الحياة الخاصة للأفراد، حيث أكد في المادة ١٠ على حرمة المساكن وعدم جواز تفتيشها إلا بأمر قضائي مسبب.

ونصت المـادة ١١ على أن "لحياة المواطنين الخاصة حرمة يحميها القانون. وللمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة ووفقا لأحكام القانون.

أما دستور ٢٠١٢ فقد نص كذلك في المادة ٣٨ على أن "لحياة المواطنين الخاصة حرمة، وسريتها مكفولة. ولا يجوز مصادرة المراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال؛ ولا مراقبتها، ولا الاطلاع عليها إلا في الأحوال التي يبينها القانون، وبأمر قضائي مسبب".

كما نصت المادة ٣٩ على حرمة المنازل، وعدم جواز دخولها ولا تفتيشها، ولا مراقبتها إلا في حالات الخطر والاستغاثة وفي الأحوال المبينة في القانون، وبأمر قضائي مسبب محدد به المكان والتوقيت والغرض. كما يشترط تنبيه من في المنازل قبل

(٢٨) محكمة النقض، الطعن رقم ١٢١٦ لسنة ٤٩ ق، جلسة ٢٧ يناير ١٩٨٣، أحكام النقض – المكتب الفني – مدني الجزء الأول، السنة ٣٤، ص ٣٣١.

(ISSN: 2356 - 9492)

دخولها أو تفتيشها. وأقرت المادة ٤٠ التزام الدولة بكفالة الحياة الآمنة للمقيمين على أراضيها.

المطلب الثاني

حماية الحق في الخصوصية في ظل دستور ٢٠١٤

حرص دستور مصر الحالي ايضا على كفالة وحماية الحق في الخصوصية، فأفرد مادة مستقلة لتنظيم هذا الحق وجعلها أكثر تفصيلا من المادة في دستور ١٩٧١ والاعلان الدستوري. كذلك عزز دستور ٢٠١٤ من ضمانات الحق في حماية الحياة الخاصة بتجريم أي اعتداء على هذا الحق.

فتنص المادة ٥٧ من الدستور المصري الحالي على أن "للحياة الخاصة حرمة وهي مصونة لا تمس، وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حُرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مُسبب، ولمدة محددة، وفي الأحوال التي يُبينها القانون".

كما اتخذ دستور عام ٢٠١٤ ذات المنهج المتبع في دستور ٢٠١٢، حيث جاء بمواد تنظم صور معينة من الحق في الحياة الخاصة، مثل حرمة المنازل الخاصة والحق في الحياة الآمنة. فنجد أن المادة ٥٨ تنص على أن "للمنازل حرمة، وفيما عدا حالات الخطر، أو الاستغاثة لا يجوز دخولها، ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا بأمر قضائي مسبب، يحدد المكان، والتوقيت، والغرض منه، وذلك كله في الأحوال المبينة في القانون، وبالكيفية التي ينص عليها، ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، وإطلاعهم على الأمر الصادر في هذا الشأن ".

كما تنص المادة ٥٩ من الدستور الحالي على أن " "الحياة الآمنة حق لكل إنسان، وتلتزم الدولة بتوفير الأمن والطمأنينة لمواطنيها ولكل مقيم على أرضها."

ولم يكتف الدستور المصري الحالي بالنص على وجوب حماية الحياة الخاصة للأفراد، بل جاءت المادة ٩٩ منه لتجرم أي اعتداء على هذا الحق، حيث تنص المادة المشار اليها على أن " كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة

للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر .وتكفل الدولة تعويضا عادلاً لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضماً إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون".

فنجد أن الدساتير المصرية في العصر الحديث، بداية من دستور ١٩٧١ وصولا إلى دستور ٢٠١٤، قد اتفقت على كفالة الحق في حرمة الحياة الخاصة وإقرار كافة الضمانات التي تحميه من الاعتداء عليه بأي شكل.

المبحث الثاني

التنظيم الدستوري للحق في الخصوصية في الدساتير المقارنة

تتفاوت دساتير الدول في الضمانات التي توفرها لكفالة وحماية الحق في الخصوصية. وسوف نعرض في هذا الفصل لموقف مجموعة من دساتير الدول المختلفة.

المطلب الأول

دستور الولايات المتحدة الأمريكية

على الرغم من ان دستور الولايات المتحدة الأمريكية لا يتضمن نص صريح على الحق في الخصوصية، إلا أن هناك مجموعة من التعديلات الدستورية تمت على الوثيقة الأصلية وتم التصديق عليها في ١٥ ديسمبر ١٧٩١ وعرفت باسم "إعلان الحقوق"[٢٩]. وقد قررت التعديلات المشار اليها حماية لجوانب محددة من الخصوصية.

(29) Amendment I of US. Constitution (Privacy of Beliefs) stipulates that “Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”, on : http://hrlibrary.umn.edu/education/all_amendments_usconst.htm.

(ISSN: 2356 - 9492)

فقد نص التعديل الأول على حماية خصوصية المعتقدات. وجاء التعديل الثاني ليقرر خصوصية المنزل ضد ما كان متبع في السابق من المطالبة بإجبار المواطنين على إيواء الجنود في منازلهم(٣٠). أما حماية الخصوصية الفردية والممتلكات في مواجهة عمليات التفتيش غير المبررة، فقد كفلها التعديل الرابع(٣١). وجاء التعديل الخامس ليوفر الحماية لخصوصية المعلومات الشخصية(٣٢). بالإضافة إلى ذلك، ينص التعديل التاسع(٣٣) على أن النص على بعض الحقوق في مواد الدستور لا يجوز تفسيره على أنه إنكار للحقوق الأخرى التي يتمتع بها المواطن.

وقد أثارت مسألة مدى حماية الدستور للخق في الخصوصية في المواضع غير المنصوص عليها صراحة جدلا كبيرا. فمن جانب، نجد بعض الفقهاء ومن بينهم القاضي "روبرت بورك" في المحكمة العليا، قد ذهبوا إلى عدم وجود حق عام في الخصوصية. إلا أن المحكمة العليا، بدءاً من عام ١٩٢٣، وحتى وقتنا الحالي، قد أقرت

(30) Amendment III (Privacy of the Home) ،states that "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law", on : http://hrlibrary.umn.edu/education/all_amendments_usconst.htm.

(31) Amendment IV (Privacy of the Person and Possessions) stipulates that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized", on : http://hrlibrary.umn.edu/education/all_amendments_usconst.htm.

(32) Amendment V states that "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation".

(33) Amendment IX (More General Protection for Privacy?), provides that: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people".

التفسير الواسع للحق في الخصوصية حتى أصبح يشمل القرارات المتعلقة بتربية الأطفال والإنجاب والزواج وإنهاء العلاج الطبي. كما تُظهر استطلاعات الرأي أن معظم المواطنين الأميركيين يؤيدون هذا التفسير الواسع لمواد الدستور[٣٤].

ومن التطبيقات القضائية الهامة في هذا الصدد، نعرض قضية ماير ضد نبراسكا (١٩٢٣)[٣٥]، والتي ألغت فيها المحكمة العليا قانوناً للولاية يحظر تعليم اللغة الألمانية وغيرها من اللغات الأجنبية للأطفال حتى الصف التاسع. ففي هذه القضية ادعت حكومة ولاية نبرسكا أن اللغات الأجنبية يمكن أن تؤدي إلى غرس أفكار ومشاعر في ذهن الطلاب، يمكن أن يكون لها تأثير سلبي على الصالح العام للبلاد. إلا أن القاضي "ماكرينولدز" قد خلص في قراره إلى أن الدولة لم تظهر مبرر قوي للتعدي على حقوق الآباء والمعلمين في تحديد الدورة التعليمية الأفضل للطلاب الصغار. وقضى القاضي "ماكرينولدز" بأنه على الرغم من أن المحكمة لم تحاول أن تضع حدرد دقيقة لنطاق الحرية المكفولة للفرد، فإن الحق في الخصوصية الذي يكفله القانون لا يشير فقط دون شك إلى مجرد الحق في عدم تقييد الحرية الجسدية بالاحتجاز أو الإيقاف دون سند قانوني، بل أيضاً يشمل حق الفرد في ابرام العقود، والعمل، واكتساب المعرفة والحصول على المعلومات، والزواج، وتكوين أسرة وتربية الأطفال، وحرية الاعتقاد، والتمتع بصفة عامة بكافة الامتيازات التي طالما اعترف بها القانون العام Common Law باعتبارها حقوق أساسية مقررة لكافة الأفراد.

وبمرور الوقت ترسخ مبدأ الخصوصية في النظام الأمريكي، عندما ألغت محكمة وارن في الستينات، قانون الولاية الذي يحظر حيازة وبيع وتوزيع وسائل منع الحمل على

(34) Exploring Constitutional Conflicts, “The Right of Privacy”, University OF Missouri-Kansas City, School of Law: http://law2.umkc.edu.
(35) Meyer v. State of Nebraska (1923), Supreme Court of The United States, 262 U.S. 390, 1923, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/Meyer%20v%20Nebraska%20%281923%29.html.

(ISSN: 2356 - 9492)

المتزوجين في قضية غريسوولد ضد كونيكتيكت (١٩٦٥)[٣٦]. وقد قال القاضي "دوغلاس" في هذا الصدد أن القانون المشار اليه يتعدى على الحق في الخصوصية الزوجية ولا يجوز فرضه على المتزوجين. ويبرر ذلك بأن الدستور يضع عدة ضمانات تكفل الحق في الخصوصية"، كما يستند هذا الحق على التفسير الواسع للتعديل التاسع الذي ينص على وجود حقوق أخرى للمواطنين بخلاف تلك المنصوص عليها صراحة في الدستور.

وفي عام ١٩٦٩، خلصت المحكمة بالإجماع إلى أن حق الخصوصية يحمي حق الفرد في حيازة المواد الإباحية في منزله، بما في ذلك المواد الإباحية التي قد تشكل أساساً للملاحقة الجنائية ضد صانعها أو موزعها. وفي هذا الشأن قال القاضي "مارشال" في قضية ستانلي ضد جورجيا[٣٧] أنه مهما كانت المبررات في القوانين التي تنظم مبادئ وأسس المجتمع، فإننا لا نعتقد أنها تصل إلى خصوصية المرء في منزله. ووفقا للتعديل الدستوري الأول[٣٨] فإن الدولة ليس من شأنها التدخل في أفعال رجل يجلس بمفرده في منزله، أو الكتب التي قد يقرأها، أو الأفلام التي يمكن أن يشاهدها الخ. كما أن تراثنا الدستوري كله يرفض فكرة إعطاء الحكومة سلطة السيطرة على عقول المواطنين. كذلك فقد صدرت قرارات في قضايا سابقة مثل غريس وولد و رو، أشارت إلى أنه يجب على الدول أن تقدم دلائل وأسباب قوية ومقنعة عندما تتعرض لخصوصية الأشخاص.

(36) Griswold v. Connecticut (1965), Supreme Court of The United States , 381 U.S. 479, 1965, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/griswold.html.

(37) Stanley v Georgia (1969), Supreme Court of The United States, 394 U.S. 557 April 7, 1969, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/stanley.html.

(38) Amendment I of the US constitution states that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”.

ومع ذلك تظل مسألة كيفية تحقيق التوازن بين مصالح الدول وحماية وكفالة حق الأفراد في الخصوصية محل جدل. وبمعنى آخر، فإن إشكالية تحديد نوع المصالح العامة التي قد تبرر للدول التعرض لمسألة حماية حرية الأفراد وخصوصيتهم لم تُحسم بعد. فلا يزال موضوع حماية الحق في الخصوصية في الولايات المتحدة الأمريكية مسألة مفتوحة، كما توجد مطالبات من الشعب الأمريكي بسد الثغرات الدستورية المتعلقة بهذا الحق من أجل الاعتراف بحق عام في الخصوصية(٣٩).

المطلب الثاني

دستور المملكة المتحدة

إن الدستور البريطاني من الدساتير غير المكتوبة، بمعني أنه لا يوجد في شكل وثيقة واحدة، فهو مستمد من عدد من المصادر مثل القوانين الأساسية والسوابق القضائية والقانون العام "Common law". وفي هذا الصدد سوف نعرض لما جاء بالقانون المنظم للحقوق الأساسية في المملكة المتحدة فيما يتعلق بحماية الحق في الحياة الخاصة.

يحدد قانون حقوق الإنسان لعام ١٩٩٨، الحقوق والحريات الأساسية التي يحق لكل فرد في المملكة المتحدة الحصول عليها. فهذا القانون يدمج الحقوق المنصوص عليها في الاتفاقية الأوروبية لحقوق الإنسان في القانون الانجليزي المحلي. وقد دخل هذا القانون حيز النفاذ في المملكة المتحدة في الأول من أكتوبر عام ٢٠٠٠.

وتنص المادة ٨ من القانون المشار اليه على الحق في حرمة المسكن واحترام الحياة الخاصة والاتصالات بما في ذلك الخطابات والمحادثات التليفونية والبريد الإلكتروني. فتنص على أن:

"١- لكل شخص الحق في احترام حياته الخاصة والأسرية، ومنزله ومراسلاته.

٢- ولا يجوز أن تتدخل سلطة عامة في ممارسة هذا الحق إلا إذا كان ذلك وفقا للقانون، وضروريا – في مجتمع ديمقراطي – لمصلحة الأمن الوطني أو السلامة العامة

(39) Exploring Constitutional Conflicts, *Ibid*.

(ISSN: 2356 - 9492)

أو الرخاء الاقتصادي للبلد، أو لمنع الفوضى أو الجريمة، أو لحماية الصحة أو الأخلاق، أو لحماية حقوق الآخرين وحرياتهم."

ونعرض في هذا الصدد لقضية غدوين و أي ڤي ضد المملكة المتحدة (٢٠٠٢)[٤٠]، والتي نُظرت أمام المحكمة الأوروبية لحقوق الإنسان. فقد طُرح في هذه القضية موضوع الأشخاص المتحولين جنسياً فيما يتعلق بحقهم في الحياة الخاصة وفي الزواج. ويعتبر هذا الحكم تاريخيًا ومؤثرا في معاملة المتحولين جنسيًا، حيث لم يتم الاعتراف بهم في السابق في قانون المملكة المتحدة. لذلك قضت المحكمة الأوروبية بأن هذه المعاملة تنتهك الحق في الحياة الخاصة والحق في الزواج على حد سواء. وبناء على هذا الحكم، أدخلت حكومة المملكة المتحدة قانون الاعتراف بنوع الجنس لعام ٢٠٠٤، الذي وضع آلية للاعتراف لهؤلاء بالحقوق المتعلقة بالحياة الخاصة.

ونرى أن المادة ٨ السابق الإشارة اليها قد حددت مجموعة من الضوابط التي تجيز تقييد الحق في الخصوصية. فيجب على المشرع عند تقييد هذا الحق أن يراعي الشروط والمسوغات المقررة في المادة السابقة. وقد وضع القانون الإنجليزي بعض القيود على الحق في الحياة الخاصة في حالات معينة هي حماية الأمن القومي، حماية السلامة العامة، حماية الاقتصاد القومي، حماية الصحة أو الأخلاق العامة، منع الفوضى أو الجريمة، حماية حقوق وحريات الآخرين. ولكن القانون اشترط لإعمال هذه القيود أن يكون الإجراء المطبق متناسبا وضروريا لمعالجة المشكلة.

المطلب الثالث

دستور المانيا

إن الدستور، الذي يحكم ألمانيا اليوم هو دستور عام ١٩٤٩، والذي صدر بعد الحرب العالمية الثانية. وقد سعى واضعو الدستور إلى إنشاء وثيقة مؤقتة من شأنها أن تحكم ألمانيا الغربية حتى التوحيد. وقد شكل الوزراء ورؤساء الدول الألمانية الغربية

(40) Goodwin & I v United Kingdom [2002], https:// www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life

مجلساً برلمانياً للبدء في صياغة الدستور، وأقر المجلس مشروع القرار في بون في ٨ مايو ١٩٤٩، وأصبح الدستور قانونيا في ٢٤ مايو ١٩٤٩، مما أدى إلى إنشاء جمهورية ألمانيا الاتحادية(٤١).

فالنظام القانوني الألماني قائم على القانون المكتوب، وبالتالي فجميع المسائل القانونية يتم تنظيمها في الدستور والقوانين الألمانية المكتوبة. وفيما يتعلق بمسألة الحق في الخصوصية، فهي تندرج في الدستور الألماني تحت ما يعرف "بالحقوق الشخصية". وقد نظم الدستور الألماني هذه الحقوق الشخصية بالشكل الذي يجعلها خاضعة للحماية الدستورية من تلقاء نفسها دون حاجة إلى قانون لتطبيق هذه الحماية(٤٢).

وقد حرص الدستور الألماني على النص صراحة على حماية مسائل هامة متعلقة بالحياة الخاصة للمواطنين مثل خصوصية الرسائل والاتصالات الشخصية، فتنص المادة ١٠ منه على عدم جواز انتهاك سرية الرسائل والبريد والاتصالات. كذلك تنص على عدم جواز تقييدها إلا بأمر يستند إلى القانون، مع اشتراط أن تكون هذه القيود تخدم حماية النظام الأساسي الديموقراطي الحر أو حماية كيان أو أمن الاتحاد، أو إحدى الولايات.

كذلك وضع الدستور ضمانات لحماية حرمة المساكن، فتنص المادة ١٣ على أن حرمة المسكن غير قابلة للمساس بها، ولا يجوز تفتيش المسكن إلا بأمر من القاضي، أو بأمر من هيئات أخرى منصوص عليها في القوانين، ويكون ذلك عند وقت الضرورة، وبحيث لا تجرى عملية التفتيش إلا على النحو المنصوص عليه في هذه القوانين.

وقد استثنى الدستور الحالة التي توجد فيها وقائع معينة تبرر الاشتباه في ارتكاب أي شخص لجريمة يعتبرها القانون جريمة خطيرة، فإنه للتحري عن هذه الجريمة يجوز استخدام وسائل تقنية لإجراء مراقبة سمعية لأي مسكن يُعتقد أن المشتبه به يقيم فيه،

(41) Constitionnet, “Constitutional History of Germany”, https://constitutionnet.org/country/constitutional-history-germany.
(42) Harry D. Krause, “The Right to Privacy in Germany: Pointers for American Legislation?”, Duke Law Journal, Summer, 1965, Vol. 1965, No. 3 (Summer, 1965), pp. 481-530, p. 505.

(ISSN: 2356 - 9492)

بناء على أمر قضائي، إذا تبين أن الكشف عن حيثيات الجريمة بطرق أخرى قد يصبح صعبا تماما، أو عديم الجدوى. ويجب أن يكون هذا الاستخدام لمدة محدودة، وتتولى إصدار الأمر بهذا الاستخدام هيئة من ثلاثة قضاة. وعندما يكون عنصر الوقت محدود، يجوز أن يتولى قاض واحد إصدار الأمر .

كما أكد الدستور على ضرورة تجنب المخاطر الشديدة على السلامة العامة، وخاصة المخاطر المتعلقة بالحياة. وفي هذا الإطار نص على عدم جواز استخدام الوسائل التقنية لمراقبة المنزل إلا بموجب أمر قضائي. وعندما يكون الوقت عنصرًا هاما ومحدود، يجوز أيضا أن تتولى إصدار الأمر باستخدام هذه التدابير جهات أخرى يحددها القانون؛ على أن يتم إلحاقها بقرار قضائي دون تأخير.

وإمعانا في الضمانات المقررة لحماية المسكن، فإذا كان استخدام الوسائل التقنية مخصصا فقط لحماية من يقومون بتفتيش المسكن، يجوز إصدار الأمر بهذا الإجراء من قبل جهة يحددها القانون. ولا يجوز الاستفادة بأي معلومات تم الحصول عليها أثناء هذا الاستخدام في أي غرض آخر إلا لأغراض الملاحقة الجنائية، أو دفع الخطر، وفي حال الإقرار مسبقًا بشرعية الإجراءات التي أمر بها القاضي من قبل.

ولا يجوز بصفة عامة التدخل بأي إجراء يتعرض لحرمة المساكن – في غير الأحوال السابقة – إلا لدفع خطر على العامة أو على حياة أحد الأشخاص، أو بناء على قانون لدرء خطر شديد يهدد الأمن العام والنظام العام، أو لمكافحة خطر انتشار الأوبئة، أو لحماية الأحداث المُعرضين للخطر.

وقد وضع الدستور استثناء آخر يجيز وضع قيود على الحق في حرمة المسكن بموجب القوانين المتعلقة بالدفاع والمسائل الحربية.

ويحمد للمشرع الدستوري الألماني تصديه بشكل تفصيلي لتنظيم الحق في الحياة الخاصة بصوره المختلفة. ويلاحظ أنه تشدد في الضمانات المقررة لهذا الحق وضيق في المبررات التي يمكن أن تتخذ كأساس لتقييده.

الباب الثاني

التصدي التشريعي للتأثير السلبي لتكنولوجيا المعلومات علي الحق في الخصوصية

إن استخدام التكنولوجيا والذكاء الاصطناعي يمكن أن يسهم بشكل كبيرا في تعزيز حقوق الإنسان وحمايتها. إلا أن الحكومات والشركات التجارية ومنظمات المجتمع المدني والمنظمات الدولية لم تنجح بعد في إيجاد حل للحد من الآثار السلبية لاستخدام التكنولوجيات على حق الفرد في الخصوصية. فمن الواجب أن يتم تقييم الوسائل التكنولوجية في إطار مدى اتفاقها مع التزامات الدول بموجب القانون الدولي لحقوق الإنسان. وتشمل هذه الالتزامات الامتناع عن استخدام الذكاء الاصطناعي بطرق تنتهك الحق في الخصوصية أو حقوق الإنسان الأخرى(٤٣). لذلك تسعى حاليا معظم الدول إلى تعديل تشريعاتها وسن تشريعات جديدة لمواجهة التهديدات التي تشكلها وسائل وتقنيات تكنولوجيا المعلومات على الحق في الخصوصية.

وسوف نعرض في هذا الباب لأهم صور استخدام تكنولوجيا المعلومات في انتهاك الحق في الخصوصية، في فصل أول، ثم نوضح موقف التشريعات المصرية فيما يتعلق بالتصدي للجرائم الإلكترونية وحماية الحق في الخصوصية، في فصل ثانٍ.

الفصل الأول

صور استخدام تكنولوجيا المعلومات في انتهاك الحق في الخصوصية

أصبح استخدام تكنولوجيا المعلومات والاتصالات متفشياً بشكل متزايد على مدى العقدين الماضيين. وأصبح المجال الحاسوبي أحد أهم مكونات المجتمعات المعاصرة.

(43) United Nations Human Rights Office of the High Commissioner, " Online expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine- learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy", 27-28 May 2020, Concept Note, p. 2.

(ISSN: 2356 - 9492)

فوفقا لتقرير نيلسن لعام ٢٠١١[٤٤]، بلغ عدد الأشخاص الذين يستخدمون الإنترنت في العالم ٢،١ مليار نسمة، أي ما يمثل ٣٠٪ من سكان العالم. وخلال العام نفسه، أمضى هؤلاء المستخدمون البالغ عددهم ٢،١ مليار ٣٥ مليار ساعة على الإنترنت، معظمها على مواقع التواصل الاجتماعي. وفي ذات الوقت، أظهرت البيانات المتعلقة باقتصاديات الدول أن نموها يعتمد بشكل متزايد على ما يسمى ب "اقتصاد الإنترنت". حيث أظهر تقرير حديث لأحد شركات الإدارة[٤٥] أنه في عام ٢٠١٢ كان اقتصاد الإنترنت يمثل ٤،٧٪ من اقتصاد الولايات المتحدة واليابان و٨،٣ ٪ من اقتصاد المملكة المتحدة و٥،٥ ٪ من اقتصاد الصين.

ومع نمو الأنظمة الإلكترونية وتطورها لتصبح جزءاً موضوعياً من مجتمعاتنا، أصبح الانترنت، ولا سيما أمنه، مصدر قلق أكثر خطورة مما كان عليه قبل بضع سنوات. فلقد تحول الأمن السيبراني من كونه مسألة ممارسة جيدة لحماية جهاز الحاسوب الخاص بالفرد إلى مسألة تتعلق بالأمن القومي. فالتهديدات التي تستهدف المجال الإلكتروني قد تعرض بسهولة ثروة مجتمعاتنا وكذلك أمن وسلامة مواطنيها لأخطار جسيمة.

لذلك فعلى مدى السنوات القليلة الماضية أصبح الأمن السيبراني مسألة تهتم بها الحكومات الوطنية والسلطات الدولية على حد سواء. كما أصبحت بعض المنظمات الدولية، ومنها حلف شمال الأطلسي، تنظر في إدراجه في اختصاصاتها. ومع ذلك، فإن مشاركة السلطات العامة في إدارة المجال الإلكتروني لا تأتي دون تكلفة، لأنها تبرز الصراع بين الحريات والسلطات. ويتمثل هذا الصراع في التعارض القائم بين الحقوق الفردية والقواعد التي تقيدها والتي تفرضها السلطات العامة لتنظيم المجتمع المدني.

(44) Mariarosaria Taddeo, "Cyber Security and Individual Rights, striking the right balance Special issue of Philosophy & Technology – Online Security and Civil Rights", University of Warwick, 2015, p. 1.
(45) The Boston Consulting Group, "The Internet Economy in the G-20 (The $4.2 Trillion Growth Opportunity)" Report, March 2012, p. 8.

ففي عصر الثورة المعلوماتية أصبحت المعلومات سهلة التخزين والنقل والمعالجة. ولكن عمليات المعالجة ونقل المعلومات قد تؤدي الى الوصول إليها ومعالجتها واستخراجها بواسطة أطراف ثالثة مما قد يتسبب في الكشف عن معلومات شخصية حساسة. كذلك أدي التطور التكنولوجي الى سهولة عمليات المراقبة من جانب أجهزة الدول للمواطنين من خلال البيانات التي يتم تجميعها عنهم باستخدام(٤٦).

وهنا يثور تساؤل عما إذا كان بإمكان القائمين على إنفاذ هذه التدابير، إساءة استخدام المعلومات الشخصية مما يقوض الحقوق الشخصية، ويعرض الحق في الخصوصية وغيره من الحقوق الأساسية للخطر. وسوف نفرد هذا الفصل لعرض أهم صور تقنيات التكنولوجيا الحديثة التي أثرت بشكل واضح على الحق في الخصوصية. وفي هذا الإطار سوف نتعرض لأحد الأشكال الهامة للتدخل الحكومي في الحياة الخاصة للأفراد وهي المراقبة الحكومية، وذلك في مبحث أول. ونتبع ذلك بدراسة صورة أخرى هامة من صور تعرض القطاع الخاص لخصوصية الأفراد، وهي تقنية الحوسبة السحابية، وذلك في مبحث ثانٍ.

المبحث الأول

المراقبة الحكومية

أصبحت تقنيات الاتصالات الرقمية، مثل الإنترنت والهواتف الذكية المحمولة والأجهزة التي تدعم شبكة الانترنت جزءًا من الحياة اليومية. وقد عززت الابتكارات في تكنولوجيا الاتصالات حرية التعبير، وسهلت تبادل المعلومات عالميا. ومن جهة أخرى عززت تكنولوجيات الاتصالات في العصر الرقمي الجديد قدرة الحكومات والمؤسسات والأفراد على القيام بعمليات المراقبة وجمع البيانات. فقد قضى انخفاض تكلفة استخدام التكنولوجيا وتخزين البيانات والمعلومات على المثبطات المالية أو العملية التي تحول دون قيام الدول بإجراء عمليات مراقبة الأفراد على نطاق واسع. وتعد المنابر التكنولوجية

(٤٦) د. محمود عبد الرحمن محمد، "نطاق الحق في الحياة الخاصة"، الطبعة الاولى، منشوارت دار النهضة العربية، القاهرة، ١٩٩٤.

(ISSN: 2356 - 9492)

التي يعتمد عليها النشطاء السياسين والاقتصادين والاجتماعين وغيرهم أصبحت من أكثر المواقع عُرضى للمراقبة.

المطلب الأول

مدلول فكرة المراقبة الحكومية

لا يوجد للمراقبة تعريف دولي أو محلي متفق عليه من الناحية القانونية، وذلك على الرغم من استخدامها أكثر من أي وقت مضى في مجتمعنا الحديث. فيجب أن نعترف إننا نعيش اليوم في قرن من المراقبة المتنوعة. فتتمثل الفلسفة الجديدة للعصر الرقمي في جمع المزيد والمزيد من المعلومات والبيانات عن الأفراد. كما تمس الأنظمة الرقمية جميع القطاعات. فبداية من الحماية القانونية للنظام العام من خلال تركيب كاميرات المراقبة، إلى التشغيل الآلي للمنزل، والحوسبة السحابية والمدن الذكية، واستخدام الانترنت بشكل متوسع في شتي مجالات الحياة، كل ذلك جعل التكنولوجيات تستخدم في كل مكان باعتبارها من ضروريات الحياة(٤٧).

ودائماً ما كان للتكنولوجيا منتقدين وأنصار، وينطبق ذات الشيء على المراقبة. فبينما يركز أنصار التكنولوجيا على ما توفره المراقبة من أمن؛ فإن معارضو التكنولوجيا يفضلون العيش في مجتمع يتميز بالصمت التكنولوجي.

وإذا كانت الدولة والسلطات العامة هي الجهات الفاعلة في مجال المراقبة، فإن استخدام هذه الأخيرة لا ينبغي أن يُختزل فيهم وحدهم، حيث إن تقنيات المراقبة الحديثة يتم تطبيقها بواسطة العديد من الجهات.

وتكمن الإشكالية في أن الدول قد تلجأ لعمليات المراقبة كشكل من أشكال رصد سلوك الأفراد بموجب القانون. وبمعنى آخر، تستخدم الدول تقنية المراقبة في إطار سلطتها بوصفها حامية للنظام العام والأمن القومي والسلامة العامة ومنع الجريمة.

(47) Clémence CODRON, "La surveillance diffuse: entre Droit et Norme", THÈSE en Droit Public, sous la direction de Professeur Jean-Jacques Lavenue, Université de Lille 2, soutenue le 15 juin 2018, p. 31.

وبالتالي فان القول بالحد من المراقبة من جانب الدولة سيحد من سلطة الدولة في الحفاظ على مقتضيات الأمن القومي.

ومن جانب آخر، فإن الحفاظ على الخصوصية أصبحت قضية القرن في ظل وجود انظمة المراقبة. وفي هذا الإطار يجب تحليل عصر ظهور المراقبة باعتباره مرحلة تاريخية حاسمة. فالمراقبة تقوم على فلسفة جديدة تعتمد على جمع أكبر قدر من المعلومات والبيانات الشخصية عن الأفراد. ومن هنا تكمن أهمية دور القانون في حماية الخصوصية والبيانات الشخصية.

وإذا كانت المراقبة تتدخل في حق الشخص في الحياة الخاصة والأسرية، إلا أن الهدف منها قد يكون هدف مشروع وهو منع الجريمة. ولكن في جميع الأحوال يجب أن تكون الإجراءات المتخذة من جانب السلطات العامة متناسبة مع الهدف المرجو منها. فنجد على سبيل المثال أنه في السنوات الماضية، نددت الصحف الأمريكية بعدد من القضايا المتعلقة بمراقبة اتصالات المواطنين، من أشهرها قضية ويكيليكس، والتي تتعلق بقيام منظمة ويكيليكس باصدار عدة آلاف من الوثائق من وكالة الاستخبارات المركزية الامريكية تكشف عن ترسانة ضخمة من الأدوات التي يُزعم أن الوكالة طورتها للتجسس على محادثات المواطنين(٤٨).

وقد أبرزت المحكمة الأوروبية مبدأ التناسب بين التدابير المتخذة والهدف المرجو منها في أكثر من موضع، فعلى سبيل المثال، قضت المحكمة الأوروبية لحقوق الإنسان(٤٩) أن المادة ٤٤ من قانون الإرهاب لعام ٢٠٠٠ متوسعة في الصلاحيات التي تمنحها للسلطات من وقف وتفتيش للأفراد لمنع الجريمة، وقضت بأن استخدام هذه

(٤٨) وقد أصدرت المنظمة التي أسسها جوليان أسانج آلاف الوثائق التي تكشف ممارسات المراقبة التي تقوم بها وكالة الاستخبارات المركزية. هذه المجموعة التي تسمى " Vault٧" تحتوي على ما مجموعه أكثر من غيغابايت واحد من البيانات حول ممارسات المراقبة لأكبر وكالة استخبارات أمريكية. انظر: https://www.latribune.fr

(49) European Court of Human Rights, Case of Gillan and Quinton v. The United Kingdom, 2010, https://hudoc.echr.coe.int.

(ISSN: 2356 - 9492)

التدابير يجب أن يكون متناسب مع ما يلزم فقط لمنع الجرائم الإرهابية دون أن يترك ذلك للسلطة التقديرية للقائمين على إنفاذ القانون.

كما قضت المحكمة الأوروبية في حكم آخر في قضية باربيوليسكو ضد رومانيا(٥٠)، من أن أرباب العمل الذين يراقبون استخدام الموظفين من البريد الإلكتروني ووسائل التواصل الاجتماعي، بحاجة إلى إظهار الأسباب المشروعة لذلك، مع ضرورة توافر التناسب بين الإجراء المتخذ والهدف منه.

بالإضافة الى ما قضت به ذات المحكمة(٥١) بأنه من غير القانوني أن تحتفظ الشرطة بعينات الحمض النووي للأشخاص الذين أسقطت عنهم التهم أو تمت تبرئتهم من الجريمة.

وفي حكم حديث لها، ذهبت المحكمة الإدارية العليا المصرية(٥٢) – في إطار توضيح الحد الفاصل بين فرض الرقابة على الموظفين العموميين والتدخل في حياتهم الخاصة – إلى أنه "من حيث إن استعمال الموظف العام لمواقع التواصل الاجتماعي في العالم الافتراضي أيا كانت (فيسبوك وتويتر وانستجرام وغيرها) هو من الحقوق المباحة للجميع لما لها من سهولة التواصل بين الناس، ومساعدتهم على تبادل المعارف والأفكار والآراء، والتعليم والتثقيف وربط العلاقات، وفتح نافذة لحرية التعبير، الا أنه يتعين أن يكون استعمالها مشروع بأن يقف عند حدود الحفاظ على الأمن القومي والآداب العامة وعدم المساس بسمعة المواطنين أو خرق خصوصيتهم بما يسيء إليهم في ارتكاب أفعال السب والقذف والتشهير والابتزاز والإساءة، وإذا كان ذلك الأمر واجب على المواطنين كافه فإنه اوجب على الموظف العام خاصة عن أعمال وظيفته والمعلومات التي تتعلق بها بما هو سري بطبيعته، فإذا ما تجاوزها يستحق أشد العقاب مغلظا".

(50) European Court of Human Rights, Case of Barbulescu v. Romania, 2017, https://hudoc.echr.coe.int.

(51) European Court of Human Rights, Case of S. and Marper v. The United Kingdom, 2008, https://hudoc.echr.coe.int.

(٥٢) المحكمة الإدارية العليا - الطعن رقم ١٥١١٨ لسنة ٦٥ ق - جلسة ٢١/ ١٢/ ٢٠١٩.

وفي حكم آخر لها، ذهبت المحكمة الإدارية العليا(٥٣) إلى أنه " لا يجوز الحجاج، بما تذرع به الطاعن من أن ما كتبه على صفحته الشخصية الفيس بوك من عبارات مشينة في حق رئيس الجمهورية أنه رأيه الشخصي في مسألة جزيرتي تيران وصنافير وهي قضية وطنية تخص الأمن القومي ولا يجوز مساءلته عن رأيه الشخصي خاصة أنه خارج العمل، ذلك أن قضاء هذه المحكمة قد استقر على أن الموظف العام ملزم بأداء واجبات وظيفته وعدم الخروج على مقتضياتها، وأن أداء واجبات الوظيفة قوامه القيام بالواجبات المنوطة به بموجب بطاقة وصف الوظيفة التي يشغلها وما يكلف به من رؤسائه وأن الخروج عليها أو الإخلال بها يقيم مسئوليته التأديبية ويوجب مجازاته. كما يتوجب أيضاً على الموظف العام عدم الخروج على مقتضيات وظيفته وهي الواجبات التي يتعين الالتزام بها خارج نطاق وظيفته وخارج دائرة عمله بحسبان أنها تمسه في كرامته وتحط من اعتباره وتورده مواطن الشبهات ويمتد هذا بوصفه موظفاً عاماً إلى وظيفته والمرفق الذي ينتمي إليه فتلقي عليهما ظلالاً من سوء ما ارتكبه الموظف من مسلك معيب خارج نطاقهما وهو أيضاً ما يقيم مسئوليته التأديبية ويجيز مجازاته عنها".

ومن حيث أن المشرع المصري – بالقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات – وضع مصر على خريطة العالم الرقمي وجاءت نصوصه كاشفة عن أنه قانون عقابي للمجرم المعلوماتي وليس رقابيا فهو احترازي لا اختراقي، يمنح المواطنين الحرية في الفضاء الإلكتروني أيا كانت وسائله سواء (الفيسبوك او تويتر او انستجرام او غيرها) طالما كانت تلك الحرية تمارس في إطار القانون دون المساس بالأمن القومي للبلاد او بسمعة المواطنين أو خرق حياتهم الخاصة بما يسيء إليهم، وحفاظا على سلامة المواطنين، فإن المشرع انتهج في هذا القانون تجريم هذه الأفعال التي تقع بهذه الوسائل وقرر لها عقابا صارما لأثارها المدمرة على الوطن في مساسها بالأمن القومي له والنظام العام والآداب به، وعلى المواطن بمساسها بشرفه

(٥٣) المحكمة الإدارية العليا - الدائرة الرابعة - في الطعن رقم ٨٦٥٨٤ لسنة ٦٤ ق، جلسة ٢٠٢٠/٦/٢٦.

(ISSN: 2356 - 9492)

وعرضه واعتباره بين أهله وذويه. فنص في المادة ٢٥ من القانون على تحديد الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة و المحتوى المعلوماتي غير المشروع وابان عن انها كل اعتداء على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهاك لحرمة الحياة الخاصة او ارسال بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته أو منح بيانات شخصية إلى نظام او موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

فيتضح من قضاء المحكمة أنها وضعت حدودا فاصلة بين سلطة الجهات الإدارية في فرض نوع من الرقابة على موظفيها، ومحاسبتهم عن الأفعال التي تدخل في نطاق مخالفة مقتضيات عملهم، وبين ما يدخل في نطاق حريتهم الشخصية التي لا يجوز التدخل فيها بأي شكل. كما وضحت أن الحرية الشخصية للمواطنين بصفة عامة والموظفين العموميين بصفة خاصة يجب أن تقف عند حد المساس بالأمن القومي والآداب العامة وسمعة المواطنين أو خرق خصوصيتهم.

المطلب الثاني

مخاطر المراقبة الحكومية على الحياة الخاصة للأفراد

إن المخاطر المتعلقة بفكرة المراقبة قد تكون غير محددة بشكل واضح، ولكنها مرتبطة بشكل وثيق بالخصوصية. وإذا كانت المراقبة تستخدم في السابق لتهديد المواطنين وقمعهم في الدول ذات الأنظمة الديكتاتورية، إلا أن انتشار التكنولوجيا الرقمية أحدث ثورة في العصر الحديث وأوجد سجلات مفصلة عن الموطنين بشكل عام. وفي ظل انتشار الإرهاب بدأت الحكومات تسعى للحصول على هذه البيانات واستخدامها لأغراض غير معروفة. وعلى الرغم من وجود قوانين تحمي المواطنين من المراقبة الحكومية، إلا أنه لا يمكن رقابة البرامج الحكومية السرية حتى يتم اكتشافها. وحتى

عندما تكون الممارسات الحكومية في هذا الشأن معلومة، فإن القوانين عادة ما تضع استثناءات متعلقة بالأمن القومي والصالح العام(٥٤).

وقد أكد المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب(٥٥)، إن الحق في الخصوصية تراجع بسبب استخدام صلاحيات المراقبة والتكنولوجيات الجديدة في سياق مكافحة الإرهاب دون تقديم ضمانات قانونية كافية. كما قرر أن الدول قد عرضت الحق في الخصوصية للخطر عن طريقة عدم تطبيق الضمانات اللازمة لمنع انتهاك هذا الحق. وفي غياب مجموعة من الضمانات القانونية الصارمة ووسيلة لقياس ضرورة التدخل ومدى تناسبه ومعقوليته، لا تملك الدول أي إرشادات تساعدها على تقليص ما تتعرض له الخصوصية من أخطار بفعل سياساتها الجديدة .

وفي هذا الصدد، فقد سن الكونجرس الأمريكي في عام ٢٠٠١ قانون يسمي باتريوت "Patriot Act" يهدف إلى تعزيز الوسائل القانونية للكشف عن الإرهاب ومنعه. وقد تم تمرير قانون باتريوت في الولايات المتحدة بالإجماع تقريبا من قبل مختلف الأطياف السياسية. وكان الهدف الرئيسي من إقرار هذا القانون تحسين وسائل مكافحة الإرهاب.

وبمناسبة تطبيق المادة ٢١٥ من هذا القانون، نعرض لقضية وكالة الأمن القومي الأمريكية لعام ٢٠١٣ التي تعد مثالاً ملموساً على الكيفية التي يمكن بها للسلطة والدولة أن تتعدي على الحق في الخصوصية. فقد تم تكليف وكالة الامن القومي الأمريكية بمراقبة مكالمات عملاء شركة فيريزون للاتصالات Verizon Communications – وهى مزود خدمات هواتف محمولة بها ٩٨،٩ مليون عميل– وذلك بعد أن اصدرت

(54) Neil M. Richards, "The Dangers of Surveillance", 126 Harvard Law Review 1934, 20 May 2013

(٥٥) تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، السيد مارتين شاينين، الجمعية العامة للأمم المتحدة، مجلس حقوق الانسان، الدورة الثالثة عشر - تعزيز وحماية كافة حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية، http://hrlibrary.umn.edu/arabic/AR-HRC/AHRC13-127.pdf .

(ISSN: 2356 - 9492)

محكمة المخابرات[٥٦] امر سرى للشركة بتسليم جميع سجلات المكالمات الخاصة بها لمدة ثلاثة اشهر. ومن الجدير بالذكر أن الأمر الصادر من المحكمة كان غير مقتصر على فئة معينة، مما يعني أن وكالة الأمن القومي يمكنها مراقبة أي مكالمة دون الاشتباه في شخص بعينه. وتم اتخاذ ذلك الإجراء في ٢٥ أبريل ٢٠١٣، وجاء ذلك بعد أيام من تفجير ماراثون بوسطن[٥٧].

وبموجب الأمر الصادر من المحكمة، لا يمكن لوكالة الأمن القومي الحصول الا على البيانات الوصفية للمكالمات[٥٨]، مثل التوقيت الذي تمت فيه المكالمات والأرقام التي تم الاتصال بها، والمكان الذي صدرت منه المكالمة ومدتها. أما الحصول على محتوى المكالمات، أو أسماء أو عناوين المتصلين يعتبر جريمة تنصت من الناحية القانونية.

وفي هذا الشأن ذكرت صحيفة وول ستريت The Wall Street Journal، أن جمع البيانات من سجلات الهاتف المحمول امتد إلى ١٦٢ مليون مستخدم.[٥٩] واتضح ايضا أن البرنامج السري للمراقبة والتنقيب عن البيانات يمنح الحكومة الأمريكية إمكانية الوصول إلى كمية هائلة من رسائل البريد الإلكتروني وسجلات المحادثات وغيرها من البيانات مباشرة من خوادم تسع شركات إنترنت، تشمل شركة جوجل، الفيسبوك، مايكروسوفت، ياهو، أمريكا أون لاين وأبل. وقد أنكرت جميع الشركات المذكورة معرفتها بالبرنامج أو مشاركتها فيه. بينما وصف الرئيس باراك أوباما هذا البرنامج بأنه ضروري للحفاظ على سلامة المواطنين الأميركيين، وقال إن الولايات المتحدة "سيتعين عليها

(٥٦) محكمة مراقبة الاستخبارات الخارجية الأمريكية (FISC)، هي محكمة تم إنشاؤها بموجب قانون مراقبة الاستخبارات الأجنبية لعام ١٩٧٨. وتتمثل وظيفة هذه المحكمة في الإشراف على طلبات أوامر المراقبة ضد الجواسيس الأجانب داخل الولايات المتحدة الأمريكية بواسطة وكالات إنفاذ القانون الفيدرالية ووكالات الاستخبارات.

(57) CNN, "Boston Marathon Terror Attack Fast Facts", CNN Editorial research, 18 December 2020, https://edition.cnn.com.

(58) Public Law 107-56- Oct. 26, 2001, found on : https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf .

(59) Siobhan Gorman, Evan Perez, Janet Hook, "U.S. Collects Vast Data Trove", 7 June 2013, see the official website of Wall Street Journal *on*: http://online.wsj.com

اتخاذ بعض الخيارات لتحقيق التوازن بين الخصوصية والأمن للحماية من الإرهاب". وترتيبا على ذلك تم تقنين وصول وكالة الأمن القومي لمعلومات متعلقة باتصالات المواطنين من خلال التعديلات التي أدخلت على قانون المراقبة الأمريكي في عهد الرئيس جورج بوش والتي تجددت في عهد الرئيس أوباما في ديسمبر ٢٠١٢[٦٠].

ونعرض فيما يلي لتطور التنظيم القانوني لرقابة البيانات الشخصية في الولايات المتحدة الأمريكية[٦١]:

فبتاريخ ٢٦ أكتوبر ٢٠٠١ أقر الكونجرس قانون باتريوت Patriot Act لتوسيع صلاحيات مكتب التحقيقات الفدرالي لمكافحة الارهاب والمراقبة بعد الهجمات الارهابية في ١١ سبتمبر ٢٠٠١. وبموجب المادة ٢١٥ من القانون أصبح من السهل الحصول على أمر من المحكمة لطلب سجلات الهواتف، طالما أن لها صلة بتحقيق استخباراتي أجنبي.

وفي أواخر عام ٢٠٠١ بدأت إدارة الرئيس الأمريكي جورج بوش تطبيق سلسلة واسعة من تدابير المراقبة تسمى ستيلر ويند "Stellar Wind"، وفي هذه الفترة كانت إدارة بوش تأذن لوكالة الأمن القومي بالبدء في جمع بيانات عن الاتصالات دون الحصول على أمر من المحكمة.

وفي عام ٢٠٠٢ تم الإعلان عن مشروع جديد لوزارة الدفاع الأمريكية عرف ببرنامج التوعية الاعلامية الشاملة. وكان هذا المشروع يستهدف العمل على قواعد بيانات ضخمة متعلقة بأنشطة الأفراد، بحثا عن أنماط يمكن أن تشير إلى أي نشاط إرهابي. ولكن بسبب الانتقادات التي وجهت لهذا المشروع، وقف الكونجرس الإنفاق عليه في أكتوبر ٢٠٠٣.

(60) Ian Black, "NSA spying scandal: what we have learned", 10 June 2013, see the official website of The Guardian *on*: https://www.theguardian.com

(61) The New York Times, "Electronic Surveillance Under Bush and Obama", U.S. *In* : https://archive.nytimes.com/www.nytimes.com/interactive/2013/06/07/us/07nsa-timeline.html#/#time254_7504.

(ISSN: 2356 - 9492)

وفي هذا الصدد صرح جاك ل. غولدسميث، رئيس مكتب المستشار القانوني في وزارة العدل، بأن أحد جوانب ستيلر ويند غير قانوني. وفي ديسمبر ٢٠٠٥، بعد أن نشرت صحيفة نيويورك تايمز مقالاً عن المراقبة بدون إذن من قبل وكالة الأمن القومي الأميركية، اعترف الرئيس جورج بوش بالتنصت على المكالمات التي تشمل أي شخص يشتبه في أنه عضو في تنظيم القاعدة. كما ذكرت صحيفة التايمز أن وكالة الأمن القومي الأمريكية قد وصلت إلى كميات هائلة من البيانات الشخصية من شركات الهاتف.

وفي مارس ٢٠٠٦ تم تعديل قانون باتريوت وإلغاء الشرط الوارد بالمادة ٢١٥ والتي تتطلب لتسجيل المكالمات والمحادثات أن يكون للشخص صلة بالإرهاب.

وفي يناير ٢٠٠٧ أعلن المدعى العام الأمريكي البرتو ر. جونزاليس Alberto R. Gonzales انه بعد شهور من المفاوضات مع محكمة مراقبة المخابرات الاجنبية، تم وضع برامج المراقبة تحت سلطة المحكمة. ولكن قانون المراقبة الاستخباراتية تم تعديله بحيث يسمح بشكل من أشكال مراقبة الاتصالات بدون الحصول على اذن من المحكمة.

وفي فبراير ٢٠٢٠، كان من المقرر انعقاد لجنة مجلس النواب للشئون القضائية لمراجعة مشروع قانون يهدف إلى إصلاح وتمديد العمل بالمادة ٢١٥ من قانون باتريوت، فضلا عن بعض الأحكام الأخرى من محكمة المخابرات الفيدرالية، وذلك قبل انتهاء صلاحية العمل به في ١٥ مارس ٢٠٢٠. وقد تم تأجيل الاجتماع دون اعلان الأسباب.

وفي ١٥ مارس ٢٠٢٠، انتهت صلاحية المادة ٢١٥ من قانون باتريوت بعد تاريخ طويل من التجاوزات وإساءة استعمال السلطة. وبذلك انقضت المادة ٢١٥ بعد أن فشل المشرعون في التوصل إلى اتفاق بشأن الإصلاحات المقترحة لقانون مراقبة الاستخبارات الأجنبية. وجاء ذلك بعد إقرار مجلس النواب مشروع قانون إعادة تمديد قانون المراقبة الاستخباراتية، والذي بمقتضاه أن يمتد تطبيق المادة ٢١٥ لمدة ثلاث سنوات أخرى، إلى جانب ادخال بعض الإصلاحات المتواضعة. ولكن لكي يتم إقرار مشروع قانون بشكل نهائي في الولايات المتحدة الأمريكية، يجب على مجلسي النواب والشيوخ تمرير هذا

المشروع، ويجب على الرئيس التوقيع عليه، وهو ما لم يحدث مع قانون إعادة تمديد قانون المراقبة الاستخباراتية، وهذا يعني انتهاء العمل بالمادة ٢١٥ من قانون باتريوت في الولايات المتحدة الأمريكية(٦٢).

ويري جانب كبير من الباحثين الأمريكيين أن الحكومة الأمريكية تأخرت في منع وكالة الاستخبارات من تطبيق المادة ٢١٥ كوسيلة لجمع بيانات الاتصالات الخاصة بالمواطنين الأميركيين بشكل مستمر وتحت ستار الأمن القومي. وأضاف البعض أن المادة ٢١٥ تمثل انتهاك للخصوصية خاصة إذا ما قورنت بقانون حماية السجلات الشخصية(٦٣) الذي ينظم جمع وحفظ واستخدام ونشر المعلومات المتعلقة بالأفراد التي تحتفظ بها الوكالات الفيدرالية في أنظمتها سجلاتها.

أما بالنسبة للنظام المصري، فقد كان قانون الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣ لا يسمح للسلطات العامة في الدولة بالحصول على معلومات وبيانات عن المستخدمين من مقدمو خدمات الاتصالات الا بشروط محددة متعلقة بالحفاظ على الأمن القومي، ومع مراعاة حرمة الحياة الخاصة للمواطنين وفقا لما يقرره القانون.

فنصت المادة ٦٤ من القانون المشار إليه على **أن** يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز القومي لتنظيم الاتصالات والقوات المسلحة وأجهزة الأمن القومي، ولا يسرى ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية

(62) INDIA MCKINNEY AND ANDREW CROCKER, “Yes, Section 215 Expired. Now What?”, April 2020, Electronic Frontier Foundation, on: https://www.eff.org.
(63) Privacy Act of 1974, on : https://www.justice.gov/opcl/privacy-act-1974.

(ISSN: 2356 - 9492)

المطلوبة، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة.

ومن جانب آخر، لا يسمح قانون مكافحة جرائم تكنولوجيا المعلومات رقم ١٧٥ لسنة ٢٠١٨ للسلطات العامة بإلزام مقدمي خدمات الاتصالات بإتاحة البيانات الخاصة بالمستخدمين إلا في حالات وبشروط معينة. حيث تنص المادة الثانية من هذا القانون على أنه" مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي ووفقًا لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون."

ويتضح من النصوص السابقة أن الجهات التي لها الحق في الرقابة هي جهاز القوات المسلحة وأجهزة الأمن القومي والمتمثلة في رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية. والأصل أن يلتزم مقدو خدمات الاتصالات بالحفاظ على سرية بيانات المستخدمين وعدم إفشائها، في إطار الالتزام بحماية الحياة الخاصة للمواطنين. ولكن القانون – استثناءا من ذلك – فرض على مقدمي الخدمات اتاحة جميع البيانات اللازمة للسلطات العامة شريطة أن تتوافر أسباب متعلقة بالأمن القومي. والمقصود بالأمن القومي كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بالأجهزة العامة بالدولة.

كذلك يجيز قانون الإجراءات الجنائية لقاضي التحقيق أن يأمر بمراقبة الاتصالات الخاصة بأشخاص مشتبه بهم إذا كان ذلك من شأنه المساعدة في الكشف عن الجريمة. وقد نصت المادة ٩٥ من القانون المشار اليه على أن لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات لدى مكاتب البريد، وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر.

وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناءً على أمر مسبب ولمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخرى مماثلة.

وقد اشتركت المفوضية السامية للأمم المتحدة مع جامعة الأمم المتحدة في مشروع بحثي بشأن تطبيق القانون الدولي لحقوق الإنسان على النظم الوطنية المسئولة عن المراقبة الرقمية الحكومية. وفي إطار مشاورة مفتوحة، وجهت المفوضية في ٢٧ فبراير ٢٠١٤ استبيانا(٦٤) إلى الدول الأعضاء عن طريق بعثتها الدائمة في جنيف ونيويورك. وقد استقبلت ردود على هذا الاستبيان من ٢٩ دولة عضوا من جميع المناطق، وخمس منظمات دولية وإقليمية، وثلاث مؤسسات وطنية لحقوق الإنسان، و١٦ منظمة غير حكومية، ومبادرتين من القطاع الخاص. أشارت العديد من المساهمات التي تلقتها الأمم المتحدة إلى الأطر التشريعية الوطنية القائمة وإلى التدابير الأخرى المتخذة لضمان احترام وحماية الحق في الخصوصية في العصر الرقمي، وكذلك إلى المبادرات الرامية إلى وضع وتنفيذ الضمانات الإجرائية والرقابة الفعالة في النظم الداخلية. وأشارت مساهمات بعض الدول إلى التحديات التي تواجهها في حماية الحق في الخصوصية في العصر الرقمي، وقدمت اقتراحات للمبادرات على المستوى الدولي. وشملت هذه التدابير تشجيع اللجنة المعنية بحقوق الإنسان على تحديث تعليقاتها العامة ذات الصلة، ولا سيما بشأن المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية؛ وإطلاع اللجنة على مقترح إنشاء مجلس حقوق الإنسان لولاية تتعلق بالإجراءات الخاصة بشأن الحق في الخصوصية؛ وإشراك المكلفين بولايات في إطار الإجراءات الخاصة الحاليين في المبادرات المشتركة أو الفردية لمعالجة المسائل المتصلة بالحق في الخصوصية في سياق المراقبة الرقمية وتقديم إرشادات بشأن أفضل الممارسات الدولية.

كما أبرزت عدة مساهمات أن مراقبة بيانات الاتصالات الإلكترونية – عندما تتم وفقاً للقانون بما في ذلك القانون الدولي لحقوق الإنسان – يمكن أن تكون تدبيراً ضرورياً وفعالاً لأغراض إنفاذ القانون أو الاستخبارات المشروعة. غير أن الكشف عن المراقبة

(64) OHCHR, “The right to privacy in the digital age”, Report of the Office of the United Nations High Commissioner for Human Rights, www.ohchr.org.

(ISSN: 2356 - 9492)

الجماعية الرقمية أثار تساؤلات حول مدى اتساق هذه التدابير مع المعايير القانونية الدولية وما إذا كانت هناك حاجة إلى ضمانات مراقبة أقوى للحماية من انتهاكات حقوق الإنسان. وعلى وجه التحديد، يجب ألا تتداخل تدابير المراقبة بشكل تعسفي أو غير قانوني مع خصوصية الفرد أو أسرته أو مراسلاته؛ ويجب على الحكومات أن تتخذ تدابير محددة لضمان حماية القانون من هذا التدخل.

وكشف استعراض مختلف المساهمات الواردة أن معالجة مسألة المراقبة تتطلب تقييماً لما يشكل تدخلاً في الخصوصية في سياق الاتصالات الرقمية؛ وتوضيح المعنى المقصود من التدخل التعسفي وغير قانوني بشكل واضح.

المبحث الثاني

الحوسبة السحابية

إن من أهم التحديات التي تواجه الشركات والمنظمات التي تعمل بنموذج الحوسبة السحابية هي مدي قدرتها على الحفظ الآمن للبيانات. فالحوسبة السحابية تعتمد بشكل أساسي على ما يوفره مقدم الخدمة من سياسات وإجراءات لتأمين البيانات مثل التشفير والقدرة على التصدي للبرمجيات الخبيثة(٦٥).

المطلب الأول

مدلول فكرة الحوسبة السحابية (Cloud Computing)

إن فكرة الحوسبة السحابية تتبلور في توفير تطبيقات من خلال شبكة الإنترنت تتيح لمستخدميها إمكانية تخزين المعلومات ومعالجتها ونقلها ومشاركتها مع الآخرين من أي مكان وفي أي وقت ودون الحاجة إلى استخدام الحاسوب الشخصي. فهذه التقنية تتيح للمستخدمين استخدام الخدمات المعلوماتية عن طريق سيرفرات خارجية متاحة على سحابة الإنترنت مع ضمان تأمين هذه المعلومات والحفاظ عليها من الفيروسات او الاختراق من قراصنة المعلومات(٦٦).

---

(٦٥) صباح محمد كلو، " الحوسبة السحابية: مفهومها وتطبيقاتها في مجال المكتبات ومراكز المعلومات"، The SLA-AGC 21st Annual ConferenceAbu Dhabi, United Arab Emirates, 17-19 March 2015, p.16 https://www.qscience.com .

(٦٦) انظر المرجع السابق.

وتهدف هذه التكنولوجيا في الأساس إلى التيسير على المستخدمين وتوفير الوقت والجهد. ومن أهم أمثلة تطبيقات الحوسبة السحابية خدمات التخزين السحابية، والتي تعتبر من أهم الخدمات التي يتم استخدامها في الوقت الحالي مثل Google Drive وiCloud وDropbox. هذه الخدمات توفر سعة تخزينية للملفات على الإنترنت بدون الحاجة إلى وجود أقراص تخزين فعلية على جهاز الكمبيوتر الخاص بالأفراد أو الشركات، بحيث يمكن الوصول للمعلومات والبيانات من أي جهاز يتصل بالإنترنت.

وتنقسم الحوسبة السحابية إلى ثلاث تصنيفات كالآتي(٦٧):

- الحوسبة العامة، وهي التي توفر الخدمات لأي شخص على شبكة الإنترنت
- الحوسبة الخاصة، وهي شبكة خاصة أو مركز بيانات يوفر الخدمات لعدد محدود من الأشخاص.
- الحوسبة الهجين، وهي التي تحدد عملية توزيع التطبيقات المختلفة على كلا من السحابة العامة والخاصة. فهذا النوع يتيح إمكانية مشاركة المعلومات والملفات والبيانات بين النوعين من السحابات.

كما يمكن تقسيم خدمات الحوسبة السحابية إلى الآتي: (٦٨)

- خدمة البنية التحتية (Infrastructure)

في هذا النموذج تقوم الشركات والمؤسسات باستئجار أو شراء البنية التحتية المعلوماتية. وتتكون البنية التحتية من خوادم فعلية وخوادم افتراضية، بالإضافة الى توفير التخزين والشبكات. ويتطلب ذلك من المستخدمين فقط إدارة التشغيل وقواعد البيانات واستخدام التطبيقات.

- خدمة المنصات (Platform)

(67) Gurudatt Kulkarni, Jayant Gambhir, Rajnikant Palwe, Marathwada Mitra Mandal ‘s Polytechnic, Pune, " Cloud Computing-Software as Service", International Journal of Computer Science & Information Technology Research Excellence Vol. 2, Issue 1, Jan-Feb 2012.

(٦٨) انظر المرجع السابق.

(ISSN: 2356 - 9492)

هو نموذج للحوسبة السحابية يقوم من خلاله مقدم الخدمات بتوفير الأجهزة وأدوات البرمجيات للمستخدمين عبر الإنترنت. عادةً ما تكون هذه الأدوات مطلوبة لتطوير التطبيقات. ويقوم مزود الخدمة باستضافة الأجهزة والبرامج على بنيته التحتية الخاصة. ونتيجة لذلك، فإن مزود الخدمة يجعل المستخدمين غير مضطرين إلى استخدام أجهزة وتحميل برامج خاصة بهم لتشغيل تطبيق جديد.

- خدمة البرمجيات (Software)

تسمح هذه الخدمة للمستخدمين باستخدام التطبيقات المختلفة عن بعد عن طريق الخدمات السحابية. ويتم من خلالها الاشتراك في تطبيق معد سلفا ويتم توفيره للعملاء عبر الإنترنت، ويقتصر دور المستخدم فيه على ضبط اعدادات الخدمة.

المطلب الثاني

مخاطر الحوسبة السحابية على الحياة الخاصة للأفراد

نظرًا لأن خدمات الحوسبة السحابية تقوم بمعالجة بيانات المستخدمين على الأجهزة التي ليست ملكهم ولا سيطرة لهم عليها، فقد يؤدي ذلك الى سوء استغلال بياناتهم الشخصية وانتهاك خصوصيتهم. لذلك فإن الحفاظ على حماية البيانات الشخصية والخصوصية للمستخدمين يعد من أهم التحديات التي تواجه التشريعات الحالية في هذا المجال.

إن تكنولوجيا الحوسبة السحابية التي توفر خدمات متطورة للعملاء، هي في الأساس مجموعة من البرامج الافتراضية التي يستخدمها مزودو الخدمات، مثل Amazon وGoogle وWindows وDropbox، لتقديم الخدمات للمستفيدين. ومع ذلك، لا تزال الأساليب المستخدمة لتأمين البيانات على السحابة غير كافية لضمان حماية الخصوصية بشكل كامل في جميع الحالات.

وفي هذا الإطار يمكن تقسيم عوامل تهديد الخصوصية في مجال الحوسبة السحابية إلى عوامل داخلية وعوامل خارجية[٦٩]. وتنبثق العوامل الداخلية من فكرة أساسية تتمثل

(69) Del Mar López Ruiz M., Pedraza J. (2016) Privacy Risks in Cloud Computing. In: Kołodziej J., Correia L., Manuel Molina J. (eds) Intelligent

في أن مزودو خدمات الحوسبة السحابية هم من يتولون مسئولية تحديث وصيانة البرمجيات المشغلة للخدمات، وبالتالي فيكون لهم سيطرة كاملة على جميع البيانات والمعلومات التي يتم تحميلها عبر التطبيقات. كذلك يمكن لمزودو الخدمات جمع البيانات الوصفية حول من يصل إلى البيانات وأي معلومات شخصية إضافية أخرى. وهنا تصبح الضمانة الوحيدة لحماية البيانات الشخصية هو ما يتوافر من الثقة في مزود الخدمة.

بالإضافة إلى ذلك، فان الشركات التي تقدم خدمات الحوسبة السحابية قد تتردد في توفير آليات قوية لتأمين البيانات الشخصية للعملاء بسبب اعتبارات ارتفاع الأسعار. فعلى سبيل المثال، يعتقد Soghoian[٧٠] أن السبب المحتمل الذي جعل شركة جوجل Google تستغرق عدة سنوات لتقديم "بروتوكول النقل الآمن للنصوص المترابطة" (Hypertext Transfer Protocol Secure)، هو مسألة التكلفة لأن التشفير يتطلب قوة معالجة وذاكرة. وهذا البروتوكول ينشئ قناة تشفير مؤمنة بين المستخدم ومخدم الانترنت لنقل البيانات بشكل آمن، كما أنه يضمن حماية معقولة من مخاطر التصنت والقرصنة.

ويعد أيضا فقدان البيانات أو تسربها من أهم المشكلات التي تواجه مزودو الخدمات. ويرجع ذلك في أغلب الحالات إلى الحذف العرضي الذي يحدث دون قصد نتيجة لتدخل العامل البشري، وآليات التوثيق غير المتناسقة، وسوء إدارة مفاتيح التشفير، والعديد من الأسباب الأخرى المتعلقة بتشغيل التطبيقات.

أما عن العوامل الخارجية، ففي بعض الحالات قد تكون تطبيقات عملاء بعض مزودو الخدمات ومنافسيهم مخزنة ويتم تشغيلها على نفس الأجهزة، ويقوم أحد الجانبين

Agents in Data-intensive Computing. Studies in Big Data, vol 14. Springer, Cham. https://doi.org/10.1007/978-3-319-23742-8_8.

(70) Soghoian, C.: Caught in the cloud: privacy, encryption, and government back doors in the Web 2.0 Era. J. Telecommun. High Tech. L 8, 359–424 (2009).

(ISSN: 2356 - 9492)

بالإفراط في تحميل البيانات على الأجهزة والسحابة من أجل جعل خدمة منافسيهم غير متوفرة. واستخدام هذه الآلية قد يعرض بيانات الشركة المنافسة للفقدان[٧١].

كذلك قد تُسبب واجهات برمجة التطبيقات (Application Programming Interface API)[٧٢] مشكلات متعلقة بتأمين البيانات. فمزودو الخدمات السحابية يضطرون أن يجعلوا واجهات برمجة التطبيقات الخاصة بهم علنية حتى يتمكن العملاء من استخدام خدماتهم. وفي مجال خدمات الحوسبة السحابية، يعتبر عدد واجهات برمجة التطبيقات أعلى من ذلك المستخدم في الخدمات المعلوماتية الأخرى وذلك بسبب القدرة الاستيعابية الكبيرة لها. وهذا يسمح أيضا لقراصنة المعلومات بمعرفة واجهات برمجة التطبيقات التي تعطي الكثير من المعلومات حول بنية السحابة.

وهناك من العوامل الخارجية ما يرجع للمستخدمين أنفسهم، حيث تتسم معظم التطبيقات التي تعمل في السحب بضعف التأمين بسبب أنها لم تكن مصممة في الأساس بهدف التأمين. وعلاوة على ذلك، هناك العامل البشري الذي يمكن أن يكون ضحية للاحتيال أو التلاعب مما يؤدي إلى فقدان بياناته التأمينية. فقد يتعرض البعض لقرصنة[٧٣] البريد الالكتروني أو الصفحة الشخصية على مواقع التواصل الاجتماعي، وهو ما يعد خرقا للخصوصية وأحيانا يرتبط الأمر بخسائر مادية أيضا عند اختراق البيانات البنكية عن طريق الإنترنت. ويعتبر التعرض لمثل هذه القرصنة بمثابة جرس إنذار للتأكد من سلامة برنامج الحماية من الفيروسات المستخدم. ويُسهل الاعتماد على برامج مجانية يتم تحميلها من الإنترنت عمل القراصنة كونه لا يوفر الحماية المطلوبة للبيانات.

(71) Gul, I., Ur Rehman, A., Islam, M.H.: Cloud computing security auditing. In: The 2nd International Conference on Next Generation Information Technology (ICNIT), Gyeongju (2011).

(72) Behl, A.: Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation. In: World Congress on Information and Communication Technologies (WICT), pp. 217–222 (2011).

(٧٣) القرصنة هي اختراق لأجهزة الحاسوب عبر شبكة الإنترنت ويقوم بهذه العملية شخص أو مجموعة من الأشخاص لديهم خبرة واسعة في برامج الحاسوب، إذ يمكنهم بواسطة برامج مساعدة الدخول إلى حاسوب أخر والتعرف على محتوياته.

ومن جهة أخرى يعد موقع السحابة أحد أهم المشكلات التي تواجه مستخدمي خدمات الحوسبة السحابية، حيث إن المستخدمين في كثير من الأحيان لا يعرفون أين يتم تخزين المعلومات الخاصة بهم. فمراكز البيانات التي يتم تخزين بيانات الشركات وعملائها عليها تقع عادة في مواقع جغرافية غير محددة وتخضع لقوانين مختلفة.

ونجد أن النصوص القانونية المنظمة للحق في الخصوصية في معظم البلدان لم تتصد للإشكاليات المتعلقة بالطابع الدولي للخدمات المعتمدة على تقنيات الإنترنت. فقضايا حماية البيانات الخاصة المخزنة على السحب قد لا تقع في نطاق ولاية قضائية واحدة، وذلك إذا كانت السحابة تقع في موقع جغرافي مختلف عن موقع الشركة صاحبة البيانات. كذلك فان القوانين المنظمة للحق في الخصوصية تختلف في مضمونها بحسب كل بلد، وحتى إذا تمكن الأشخاص المعنيين من تقديم أدلة كافية حول انتهاك الخصوصية، غالباً ما يكون من الصعب متابعة الإجراءات القضائية خارج موطن الضحية بالإضافة الى التكلفة المرتفعة(٧٤).

لهذا السبب، تظهر مسألة تنظيم الحق في احترام الخصوصية في مواجهة الابتكار التكنولوجي كإحدى القضايا القانونية البارزة في بداية القرن الحادي والعشرين.

فهناك مفهوم جديد للخصوصية في العالم الرقمي، حيث يكون المعيار المتبع هو ما إذا كانت البيانات الشخصية قد تمت معالجتها بطريقة تتفق مع النظام المخصص لها من عدمه. بمعنى أخر تتجه الدراسات الحديثة نحو ادخال مبدأ الخصوصية في نطاق الحماية عند تصميم البرامج المعلوماتية. وبذلك يتم خلق نظام وقائي في التطبيقات والبرامج الالكترونية تعزز قدرتها على حماية الخصوصية في العصر الرقمي.

وسوف تقدم البرامج التي تأخذ في الاعتبار فكرة الخصوصية في مرحلة الابتكار التكنولوجي مثالا نموذجيا قد يحقق طفرة غير مسبوقة في مجال الخصوصية المعلوماتية. فمن الضروري أن يتم مناقشة اعداد بروتوكول دولي يلزم كبرى الشركات في مجال تكنولوجيا المعلومات بدمج الخصوصية في الابتكارات التكنولوجية كوسيلة

(74) Del Mar López Ruiz M., Pedraza J. (2016), *Ibid*.

(ISSN: 2356 - 9492)

لترجمة الحق في الخصوصية في العالم الرقمي، ومراقبة استخدام النظام للبيانات الشخصية من قبل هذه الشركات.

الفصل الثاني

تنظيم الحق في الخصوصية والقيود الواردة عليه في التشريعات المصرية

بدأت مصر في الآونة الأخيرة في تبني سياسات تشريعية تعمل على تحديث النظام التشريعي ووضع الممارسات المتعلقة بتكنولوجيا المعلومات تحت مظلة التنظيم القانوني الداخلي. ويأتي ذلك في إطار رؤية الحكومة المصرية من ضرورة مواكبة التطورات الحديثة التي قد تؤثر بشكل واضح على حياة المواطنين اليومية. وجاء التنظيم القانوني للحقوق المرتبطة بالتطور التكنولوجي الحديث مراعيا الموازنة بين مصلحة المواطنين في ممارسة حقوقهم وحرياتهم، وبين مصلحة المجتمع وما يحفظ سلمه وأمنه. وسوف نعرض لأهم هذه التشريعات في مبحث أول. ثم نتناول بالتفصيل أحكام قانون حماية البيانات الخاصة الذي صدر لينظم الحق في سرية المعلومات والبيانات الشخصية وضمانات عدم الاعتداء عليها وجاء ليتوج مجهودات الدولة في مواكبة التطورات المستحدثة عالميا في مجال حماية الحق في الخصوصية المعلوماتية، وذلك في مبحث ثانٍ.

المبحث الأول

التنظيم التشريعي للحق في الخصوصية المعلوماتية في القانون المصري بشكل عام

اتساقا مع التزامات مصر الدولية وتماشيا مع النصوص الدستورية التي تؤكد على حرمة الحياة الخاصة، بدأت الدولة تتجه نحو تعديل تشريعاتها القائمة لتصبح صالحة للتطبيق على الممارسات المرتبطة بتكنولوجيا المعلومات. بالإضافة الى ذلك، فقد أصدر المشرع المصري حزمة من التشريعات الحديثة التي استهدفت معالجة الجرائم المعلوماتية والإلكترونية وحماية البيانات الخاصة. وسوف نتناول في هذا المبحث وسائل الحماية القانونية للحياة الخاصة في إطار التشريعات المصرية القائمة وما استحدث منها.

المطلب الأول

الحق في الخصوصية في قانون العقوبات المصري

تجرم المادة ٣٠٩ من قانون العقوبات المساس بحرمة الحياة الخاصة عن طريق التنصت أو التسجيل، فتنص على أن " يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

ب- التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص فى مكان خاص".

وقد حاول المشرع استيعاب التطورات التكنولوجية الحديثة باستخدام عبارة "جهاز من الأجهزة أيا كان نوعه" حتى يشمل كافة الأجهزة التي قد تظهر في المستقبل وتستخدم في الحصول على المعلومات أو البيانات واستخدامها بشكل غير قانوني.

ولم يقتصر التجريم على الشخص الذي ارتكب الأفعال المشار اليها وانما شمل المشرع بالتجريم ايضاً كل من سهل أو شارك في ارتكاب تلك الأفعال. فتنص المادة ٣٠٩ مكرر على أن "يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلا أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن".

كما جاءت المادة ١٨٨ مكرر بنص يجرم نشر الصور والفيديوهات الخاصة بشخص آخر دون الحصول على إذن. ونصت على عقوبة الحبس لمدة لا تجاوز سنة وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرين ألف جنيه أو بإحدى هاتين العقوبتين لكل من ينشر بسوء قصد أخباراً أو بيانات أو إشاعات كاذبة أو أوراقاً مصطنعة أو مزورة أو منسوبة كذباً إلى الغير، إذا كان ذلك من شأنه أن يؤدي الى تكدير السلم العام أو إثارة الفزع بين الناس أو إلحاق الضرر بالمصلحة العامة.

(ISSN: 2356 - 9492)

المطلب الثاني

القانون رقم ١٨٠ لسنة ٢٠١٨ بشأن تنظيم الصحافة والاعلام والمجلس الأعلى لتنظيم الاعلام

صدر قانون تنظيم الصحافة إعمالاً للمادة ٧٠ من دستور مصر الحالي التي تنص على أن حرية الصحافة والطباعة والنشر الورقي والمرئي والمسموع والإلكتروني مكفولة، وللمصريين من أشخاص طبيعية أو اعتبارية، عامة أو خاصة، حق ملكية وإصدار الصحف وإنشاء وسائل الإعلام المرئية والمسموعة، ووسائط الإعلام الرقمي.

وقد حرص المشرع في هذا القانون على إعمال الموازنة بين الحق في حرية الرأي والتعبير، والذي يعد من أهم الحقوق الدستورية والدولية للصحفيين والأفراد، وبين الحق في حرمة الحياة الخاصة وعدم جواز انتهاك خصوصية الأفراد تحت شعار حرية الرأي والتعبير.

فتنص المادة ٢ من القانون المذكور علي أن كفالة الدولة لحرية الصحافة والإعلام والطباعة والنشر الورقي والمسموع والمرئي والإلكتروني. كما تحظر المادة ٣ فرض أي رقابة على الصحف ووسائل الإعلام المصرية أو مصادرتها أو وقفها أو اغلاقها. وحرصاً على حماية الحق في حرية الرأي والتعبير، بوصفه أحد أهم الحقوق الدستورية والدولية للأفراد، فقد نصت المادة ٨ على عدم جواز مساءلة الصحفيين أو الإعلاميين قانوناً عن أراءهم أو المعلومات الصحيحة التي تصدر عنهم.

ويقابل تلك المواد المادة (١٩) من العهد الدولي للحقوق المدنية والسياسية الصادر من الجمعية العامة للأمم المتحدة والذي انضمت إليه مصر في ١٩٩٧ وتم التصديق عليه بموجب القرار الجمهوري رقم ٥٣٦ لسنة ١٩٨١، والتي تنص علي أنه "١- لكل إنسان حق في اعتناق آراء دون مضايقة. ٢- لكل إنسان الحق في حرية التعبير. ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها. ٣- تستتبع ممارسة الحقوق المنصوص عليها في الفقرة ٢

من هذه المادة واجبات ومسئوليات خاصة. وعلى ذلك يجوز إخضاعها لبعض القيود، ولكن شريطة أن تكون محددة بنص القانون وأن تكون ضرورية:

أ) لاحترام حقوق الآخرين أو سمعتهم،

ب) لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

وفي ذلك الشأن قضت المحكمة الدستورية العليا(٧٥) بأن "حرية التعبير التي كفلها الدستور، هي القاعدة في كل تنظيم ديمقراطي، لا يقوم إلا بها، ولا يعدو الإخلال بها أن يكون إنكارا لحقيقة أن حرية التعبير لا يجوز فصلها عن أدواتها، وأن وسائل مباشرتها يجب أن ترتبط بغاياتها، فلا يعطل مضمونها أحد، ولا يناقض الأغراض المقصودة من إرسائها، ولعل أكثر ما يهدد حرية التعبير أن يكون الإيمان بها شكلية أو سلبية، بل يتعين أن يكون الإصرار عليها قبولا بتبعاتها، وألا يفرض أحد على غيره صمته، ولو بقوة القانون".

وحيث إنه بالرغم ما لحرية التعبير من مرتبة عليا في مدارج النظام العام المصري، فانها ليس لها من ذاتها ما يعصمها من التقييد، فهي ليست من الحريات المطلقة، ذلك أن أثرها لا يقتصر علي صاحب الرأي وحده بل يتخطاه الي غيره، وقد يشمل المجتمع بأسره، ومن ثم فانه يجوز تقييدها درئاً لانتهاك حقوق الاخرين وحياتهم الخاصة.

وقد أكدت المحكمة الإدارية العليا ذات المبدأ في حكمها الصادر في ٢٦ سبتمبر ٢٠٢٠(٧٦)، حيث قضت بأنه "إذا كان الدستور قد انحاز إلى الحرية الشخصية في التعبير في كل أمر يتصل بالشئون العامة، بحسبان أنه لا يجوز لأحد أن يفرض على غيره صمتاً ولو كان معززاً بالقانون وأن حوار القوة إهدار لسلطان العقل، إلا أنه يتعين أن تكون ممارسة الحرية الشخصية في التعبير في إطارها المشروع دون إهانة أو إساءة أو تطاول، بحسبان أن حرية التعبير عن الرأي لا يقتصر أثرها على صاحب الرأي وحده، بل يتعداه إلى غيره من أفراد المجتمع، ومن ثم لم يطلق الدستور هذه الحرية،

(٧٥) المحكمة الدستورية العليا، الدعوى رقم ٢ لسنة ١٦ قضائية دستورية، بجلسة ١٩٩٦/٢/٣.
(٧٦) حكم المحكمة الإدارية العليا - الدائرة الرابعة - في الطعن رقم ٨٦٥٨٤ لسنة ٦٤ ق، جلسة ٢٠٢٠/٦/٢٦.

(ISSN: 2356 - 9492)

وإنما أباح للمشرع تنظيمها بوضع القواعد والضوابط التي تبين كيفية ممارسة الحرية بما يكفل صونها في إطارها المشروع دون أن تجاوزه إلى الإضرار بالغير أو بالمجتمع، فليس جائزاً أن يكون سوء القصد قد خالطها، فحرية التعبير عن الرأي حق دستوري إلا أن ما رمى إليه الدستور هو ألا يكون الرأي الشخصي أو النقد منطوياً على أراء تنعدم قيمها الاجتماعية، كتلك التي تكون غايتها الوحيدة شفاء الأحقاد والضغائن الشخصية، أو التي تكون منطوية على الفحش أو محض التعرض بالسمعة. كما لا تمتد الحماية الدستورية إلى آراء تكون لها بعض القيمة الاجتماعية، ولكن جرى التعبير عنها على نحو يصادر حرية النقاش أو الحوار، كتلك التي تتضمن الحض على أعمال غير مشروعة تلابسها مخاطر واضحة تتعرض لها مصلحة حيوية.".

كما قضت محكمة النقض(٧٧) في هذا الصدد بأن حرية الرأي والفكر من النعم التي أنعم الله بها على الإنسان وبها امتاز على كثير من المخلوقات، وهي المدخل الحقيقي لممارسة الكثير من الحريات والحقوق العامة الفكرية والثقافية وغيرها كحق النقد والبحث التاريخي، وقد كفل الدستور هذه الحرية إلا أنها ليست حرية مطلقة ذلك أنه قيدها بأن تكون في حدود القانون، أي في حدود احترام حريات الآخرين، وهى قيود تستلزمها الوقاية من سطوة الأقلام التي تتخذ من الصحف أداة للمساس بالحريات أو النيل من كرامة الشرفاء، لأن هذه الحرية لا يمكن قيامها بالنسبة لجميع الأفراد إلا في حدود احترام كل منهم لحريات غيره.

وإعمالاً لذلك جاءت بعض الاستثناءات على حرية الرأي والتعبير في قانون تنظيم الصحافة رقم ١٨٠ لسنة٢٠١٨، وذلك لحماية حق الأفراد في عدم انتهاك خصوصيتهم. فتنص المادة ١٧علي أن يلتزم الصحفى أو الإعلامى فى أدائه المهنى بالمبادئ والقيم التى تضمنتها نصوص الدستور. كما نصت على التزام الصحفيين بأحكام القانون وميثاق الشرف المهنى والسياسة التحريرية للصحيفة أو الوسيلة الإعلامية المتعاقد معها، وبآداب المهنة وتقاليدها، بما لا ينتهك حقًا من حقوق المواطنين، أو يمس حرياتهم.

(٧٧) طعن نقض رقم ١٤٩٩٢ لسنة ٧٨ قضائية – جلسة ٢٠١٧/٥/٨.

وفيما يتعلق بحماية الحق في الخصوصية، فقد حظرت المادة ٢٠ التعرض للحياة الخاصة للمواطنين في أي وسيلة من وسائل النشر أو البث. ويحمد للمشرع عدم تحديد وسائل النشر حتى يشمل نطاقها كافة وسائل النشر المستحدثة والالكترونية.

المطلب الثالث

تنظيم جرائم المعلومات بموجب القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم المعلومات

صدر القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم المعلومات بعد انتشار ظاهرة استخدام وسائل التكنولوجيا في ارتكاب الجرائم الالكترونية التي تهدد أمن المجتمع. وقد جاء القانون أيضا ليحقق التوازن بين حرية الرأي والتعبير وبين مواجهة الجرائم والأفعال المتعلقة بتقنية المعلومات والحد من آثارها السلبية لا سيما ما يمثل منها انتهاكاً لخصوصية الآخرين. وتأتي القيود الواردة بالقانون متوافقة مع المادة ١٩ من العهد الدولي للحقوق المدنية والسياسية التي تجيز تقييد الحق في حرية الرأي والتعبير بالقدر الذي يضمن عدم مساسه بحقوق الآخرين أو سمعتهم.

فينص القانون على التزام المسئولين برقابة البيانات والمعلومات، وينظم قواعد تأمين البيانات والفضاء المعلوماتي والبرامج والأنظمة والشبكات الواردة فيه. كما يضع نظامًا لتأمين مواقع تشغيل المعلومات والدخول على شبكة المعلومات الدولية.(٧٨)

فالهدف الرئيسي من القانون مكافحة الجرائم ذات الصلة بنظم المعلومات والشبكات حفاظًا على حقوق مستخدمي شبكة المعلومات وحماية للأمن القومي والصالح العام.

ويضع القانون تعريفًا للعديد من المصطلحات الهامة، مثل أدوات التشغيل وأشكال الجرائم الإلكترونية، مثل القرصنة والاختراق والبرمجيات الخبيثة.

كما ينص القانون على إنشاء الجهاز القومي لأمن المعلومات والذي تتضمن سلطاته اعداد الاستراتيجية المتعلقة بأمن المعلومات، بالإضافة إلى تشجيع ثقافة أمن المعلومات ومنح التراخيص لمقدمي الخدمات الإلكترونية.

(٧٨) الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات: https://mcit.gov.eg.

(ISSN: 2356 - 9492)

ويتضمن القانون أحكاماً متعددة تكفل حماية حرمة الحياة الخاصة ضد جرائم تقنية المعلومات. فقد جرم القانون أي فعل من شأنه إحداث ضرر أو إبطاء البريد الإلكتروني أو الموقع أو الحساب الشخصي لأي شخص، فتنص المادة ١٨ على عقوبة الحبس مدة لا تقل عن شهر، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، لكل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس.

وقد حرص القانون على أن ينص بشكل صريح على تجريم أي فعل يشكل اعتداء على حرمة الحياة الخاصة. فتنص المادة ٢٥ من هذا القانون على عقوبة الحبس مدة لا تقل عن ستة أشهر، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، لكل 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 شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.

ويتضح من النص السابق أن استخدام البيانات الشخصية أو الأخبار أو الصور وما في حكمها عن طريق نشرها أو منحها للأنظمة أو المواقع الإلكترونية أو بإحدى وسائل تقنية المعلومات، يعد جريمة في حالة استخدامها دون اذن الشخص المعني وبشكل ينتهك خصوصيته. وقد جعل القانون الأفعال السابقة جرائم معاقب عليها سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.

وكذلك جرم القانون في المادة ٢٦ تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه. وقد جعل القانون عقوبة الأفعال السابقة الحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات والغرامة التي لا تقل عن

مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين. كذلك اشترط المشرع لاعتبار معالجة البيانات الشخصية جريمة، أن يكون الهدف من المعالجة ربطها بمحتوي منافٍ للأداب أو استخدامها بشكل يمس باعتبار الشخص المعني أو بشرفه. فيجب أن يتوافر شرط العمد وقصد ارتكاب الأفعال المنصوص عليها لتتوافر أركان الجريمة.

وقد اعتمد القانون في صياغته على توصيات الاتحاد الدولي للاتصالات فيما يخص الأمن السيبراني ومسودة قانون مركز دعم اتخاذ القرار ومسودة قانون إدارة التشريع لوزارة العدل والقانون الهندي والاتفاقية الأوروبية لمكافحة جرائم الانترنت والمعروفة باتفاقية بودابست.

وقد أفلح المشرع في استجابته لمتطلبات المجتمع المدني، بوضع قانون شامل يحتوي على أكثر من ٧٠ مادة تضمن حماية المستخدمين للشبكات المعلوماتية من مخاطر التلاعب ببياناتهم الخاصة أو الاعتداء على حياتهم الشخصية، وذلك مع الأخذ في الاعتبار مقتضيات الأمن القومي وفي إطار القواعد الواردة في المواثيق الدولية.

المبحث الثاني

تنظيم حماية البيانات الخاصة بموجب القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية

أدت ثورة تكنولوجيا المعلومات والاعتماد على شبكة المعلومات الدولية بشكل واسع – من قبل الحكومات والأفراد على حد سواء – إلى ارتفاع نسبة المخاطر المصاحبة لاستخدام وسائل تكنولوجيا الاتصالات على اختلاف أشكالها، وخاصة المخاطر المتعلقة بانتهاك الحق في الخصوصية، والتي تتجسد في أغلب الأحوال في الاعتداء على الحق في سرية المعلومات والبيانات الشخصية.

ويتضح من الاحصائيات الرسمية في مصر، أن هناك أكثر من خمسين مليون مواطن يستخدم الإنترنت خلال عام ٢٠٢٠، وهو ما يعادل نصف سكان مصر تقريبًا،

(ISSN: 2356 - 9492)

كما قُدر حجم التجارة الإلكترونية في مصر في ذات العام الى نحو ملياري دولار[٧٩]، وهذه الأرقام تؤكد ضرورة تدخل المشرع المصري لحماية المواطنين من الاعتداء على بياناتهم الشخصية.

ومن هذا المنطلق، فإن وجود إطار تشريعي مناسب لفرض تلك الحماية أضحى مكونا رئيسيا في التطور التشريعي لأي دولة. لذلك. إمعانا في ضمان حماية وكفالة حرمة الحياة الخاصة للمواطنين، أفرد المشرع قانوناً خاصاً لمواجهة جرائم استغلال البيانات الشخصية المعالجة الكترونيا، لما تشكله من تهديد كبير لحرمة الحياة الخاصة. فصدر القانون رقم ١٥١ لسنة ٢٠٢٠ في شأن حماية البيانات الشخصية ليعاقب على الجرائم الماسة بالبيانات الشخصية للمصريين أو الأجانب المقيمين داخل جمهورية مصر العربية. وجاء القانون المشار اليه متوجا للجهود المصرية الساعية لتعزيز حماية حقوق الإنسان في البلاد. وقد جاء القانون في ٤٩ مادة بخلاف مواد الإصدار، مقسّمًا إلى أربعة عشر فصلاً تناولت جميع أحكامه وتصنيفات المخاطبين بها وحقوقهم وواجباتهم.

المطلب الأول

مفهوم انتهاك البيانات الشخصية وفقاً للقانون رقم ١٥١ لسنة ٢٠٢٠

وضع قانون حماية البيانات الشخصية إطار محدد للحق في الخصوصية المعلوماتية، وبين الأفعال التي تشكل اعتداء على البيانات الخاصة للأفراد. ونلاحظ أن المشرع المصري اهتدى بلائحة الاتحاد الأوروبي لحماية البيانات الشخصية[٨٠] في صياغته لبعض التعريفات المستخدمة في نصوص هذا القانون. فنجد أنه قد عرف

(٧٩) وفقا للأرقام المعلنة من وزارة الاتصالات المصرية في عام ٢٠٢٠، راجع الموقع الرسمي لمركز المعلومات ودعم اتخاذ القرار – مجلس الوزراء، مقالة للقاضي / محمد جميل خلف الله، " الإطار التشريعي لحماية البيانات الشخصية في القانون المصري": https://idsc.gov.eg

(80) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) on: https://eur-lex.europa.eu

البيانات الشخصية في المادة الأولي منه بأنها "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية".

كما عرف المشرع خرق وانتهاك البيانات الشخصية بأنه "كل دخول غير مرخص به إلى بيانات شخصية أو وصول غير مشروع لها، أو أي عملية غير مشروعة لنسخ أو إرسال أو توزيع أو تبادل أو نقل أو تداول يهدف إلى الكشف أو الإفصاح عن البيانات الشخصية أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها".

ويتضح من النص السابق أن اللامشروعية في نطاق الممارسات المعلوماتية يمكن أن تأخذ عدة أشكال، نعرض لها فيما يلي:

١- استخدام أساليب غير مشروعة للحصول على البيانات والمعلومات

تتعدد الأساليب غير المشروعة التي تستخدم للحصول على المعلومات والبيانات الشخصية. ويعد استخدام القرصنة المعلوماتية من أشهر الوسائل غير المشروعة للحصول على المعلومات. ويستخدم قراصنة المعلومات عادة برامج خاصة يتم إدخالها على أجهزة الحاسوب بواسطة شبكة الانترنت للتمكن من الوصول للملفات الخاصة المحفوظة عليه. ومن المستقر عليه أن معيار عدم مشروعية تجميع البيانات الشخصية هو عدم علم الشخص المعني.

٢-جمع البيانات المحظورة

قد يحظر القانون جمع بعض البيانات أو يضع ضوابط للتعامل معها. والمقصود بالبيانات المحظورة هي تلك التي يسمح فقط لعدد محدود من الأشخاص بالإطلاع عليها، وهم عادة الذين يستخدمونها لأداء واجباتهم الوظيفة. على سبيل المثال، المعلومات السرية المتعلقة بالتحقيقات الجنائية أو الوثائق المتعلقة بأمن الدولة أو المعلومات الحربية وغيرها.

٣- إساءة استعمال البيانات التي تم تخزينها

(ISSN: 2356 - 9492)

الأصل أن تتم عمليات تجميع وتخزين ومعالجة البيانات الشخصية لأهداف محددة وواضحة ومعينة سلفا. فاذا تم استخدام هذه البيانات من قبل الشخص المصرح له بالتعامل عليها في غير الأهداف المحددة لها، أصبح تصرفه غير مشروع.

٤- الكشف غير المشروع للبيانات والمعلومات

يقصد بالكشف غير المشروع للبيانات، إفشائها أو نقلها من قبل المسئول عنها بمناسبة تخزينها أو معالجتها، إلى شخص أو جهة غير مرخص لها بتلقي تلك البيانات أو المعلومات. فاذا كان الشخص قد رخص له بتخزين أو معالجة البيانات فذلك لا يعني أنها أصبحت قابلة للتداول.

٥- اتلاف وتعديل البيانات الشخصية

الاتلاف يعني تعييب الشئ بطريقة تجعله غير صالح للاستخدام للهدف المرجو منه، وبذلك يتحقق الاعتداء الذي يجرمه القانون. وقد أوضحت دراسة تمت في الولايات المتحدة الأمريكية عام ١٩٩٦[٨١]، برعاية مكتب التحقيقات الفدرالي، أن حوالي ٤١٪ من الأنظمة المعلوماتية لدى الجهات الحكومية تعرضت إلى عمليات إتلاف على مدار عام ١٩٩٥. والاتلاف قد يكون كامل وذلك عن طريق محو كافة البيانات، وقد يكون جزئي باستعمال أحد البرامج أو الفيروسات التي من شأنها إحداث خلل أو مسح جزئي للبيانات والمعلومات.

أما التلاعب فيتحقق بالدخول الى أي جهاز حاسوب وإدخال معلومات خاطئة أو ادخال تعديلات على البرامج وقواعد البيانات بقصد إحداث خلل في برامج التشغيل أو الدخول على البرامج والوصول للمعلومات بشكل غير مرخص به. أما مجرد جمع وتخزين وتبادل أو تداول المعلومات لا يعد جريمة في حد ذاته. ويضع المشرع المصري شرطين حتى تشكل الأفعال المشار اليها انتهاك للبيانات الشخصية، وذلك إذا تم الدخول بشكل مخالف للقانون، كأن يتم بدون إذن أو رضاء صاحب الشأن، ومن ناحية أخرى،

(٨١) بوليين أنطونيوس أيوب، "الحماية القانونية للحياة الشخصية في مجال المعلوماتية"، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٩، ص ٤٣٠.

إذا توافر سوء القصد لدى الشخص المسؤول عن تخزين ونقل ومعالجة البيانات، بحيث يتضح أن هدفه كشف أو اتلاف أو تعديل تلك البيانات.

المطلب الثاني

شروط جمع ومعالجة البيانات الشخصية

حدد قانون حماية البيانات الشخصية شروط جمع ومعالجة وإتاحة البيانات الشخصية، حيث اشترط المشرع المصري ضرورة الحصول على موافقة صريحة من الشخص المعني بالبيانات حتى يمكن جمعها ومعالجتها وإفشائها بأي وسيلة من الوسائل. إلا أن القانون لم يتطرق لتعريف الرضاء على استعمال ومعالجة البيانات، على الرغم من أهمية بيان طبيعة الموافقة على معالجة البيانات الشخصية لما قد يسببه من نزاعات قد تصل أحيانا إلى القضاء. وقد عرفت لائحة الاتحاد الأوروبي لحماية البيانات الشخصية "الرضاء" بأنه أي إشارة حرة ومحددة لا لبس فيها تعبر عن رغبات الشخص المعني بالبيانات، والتي يدل بها، ببيان أو بعمل إيجابي واضح، على الموافقة على معالجة البيانات الشخصية المتعلقة به أو بها.

كما ووضحت لائحة الاتحاد الأوروبي شروط الموافقة على معالجة البيانات الشخصية بشكل مفصل، حيث تنص المادة ٧ من اللائحة[٨٢] على أنه عندما تعتمد المعالجة على الموافقة، يجب أن يكون المتحكم قادرًا على إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية. وإذا جاءت موافقة الشخص المعني بالبيانات في شكل كتابي يتعلق أيضا بمسائل أخرى، يجب أن تتم الموافقة على المعالجة بطريقة يمكن تمييزها بوضوح عن المسائل الأخرى في شكل مفهوم ويسهل الوصول إليه، وباستخدام لغة واضحة. وأي جزء من الإعلان عن الموافقة يتضمن انتهاكا لنصوص اللائحة لا يكون ملزما. ويحق لمورد البيانات سحب موافقته في أي وقت، ولا يؤثر

(82) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Ibid*.

(ISSN: 2356 - 9492)

سحب الموافقة على مشروعية المعالجة التي تمت استنادا على الموافقة قبل سحبها. كما يجب أن تكون إجراءات سحب الموافقة يسيرة بقدر سهولة إعطاء الموافقة.

وقد أضافت المادة ٣ من قانون حماية البيانات الشخصية مجموعة من الشروط الأخرى الواجب توافرها – بخلاف موافقة صاحب البيانات – حتى يمكن جمع البيانات الشخصية ومعالجتها والاحتفاظ بها، وتتمثل هذه الشروط فيما يلي:

١- أن يتم جمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

٢- أن تكون صحيحة وسليمة ومؤمنة.

٣- أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.

٤- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

وإمعاناً في حماية البيانات الشخصية للأفراد، فقد ألزم القانون كل من المتحكم والمعالج للبيانات بأن يبلغ مركز حماية البيانات الشخصية في حال علمهم أو علم أحدهم – بحسب الأحوال – بوجود خرق أو انتهاك للبيانات الشخصية وذلك خلال اثنين وسبعين ساعة من العلم. أما إذا كان هذا الخرق أو الانتهاك متعلق باعتبارات حماية الأمن القومي فيجب أن يتم إبلاغ المركز فورياً، وعلى أن يقوم المركز بدوره بإبلاغ جهات الأمن القومي بالواقعة بشكل فوري.

كذلك قرر المشرع في قانون حماية البيانات رقم ١٥١ لسنة ٢٠٢٠، مجموعة من الشروط التي يجب على كل من المعالج والمتحكم وحائز البيانات مراعاتها عند طلب اتاحة البيانات الشخصية. حيث تنص المادة ١٠ من القانون المذكور على ضرورة أن تتم عملية اتاحة البيانات بناءاً على التقدم بطلب كتابي من ذي صفة لتنفيذ الإتاحة والاحتفاظ بها. ويتم البت في الطلب ومستنداته خلال ستة أيام عمل من تاريخ تقديمه إلى المختص، وعند صدور قرار بالرفض يجب أن يكون الرفض مسببًا، ويعتبر مضي المدة المشار إليها دون رد في حكم الرفض.

كما قرر المشرع حماية خاصة للبيانات الشخصية الحساسة، حيث حظر قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، جمع أي بيانات شخصية حساسة لأي مواطن ونقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من مركز

حماية البيانات الشخصية. وقد جاء هذا النص تأكيداً على حرص المشرع المصري علي توفير أقصى حماية لحرمة الحياة الخاصة للمواطنين بما يتوافق مع النصوص الدستورية وبما يتسق مع التزامات مصر الدولية.

وقد عرف القانون "البيانات الشخصية الحساسة" بأنها البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفى جميع الأحوال تعد البيانات الخاصة بالأطفال من البيانات الشخصية الحساسة.

وقد ألزمت المادة ١٢ من القانون كلٍ من المتحكم أو المعالج سواء كان شخصًا طبيعيا أو اعتباريًا بضرورة الحصول على موافقة كتابية وصريحة من الشخص المعنى في حالة إجراء أي عملية من العمليات المشار اليها في الفقرة السابقة. وإمعانا في الحفاظ على حقوق الاطفال، فقد حظر القانون أن تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر مشروطة بتقديم بيانات شخصية للطفل تزيد على ما هو ضروري للمشاركة في ذلك. وإن كان هذا النص يشوبه بعض الغموض، حيث لم يوضح المشرع المقصود بالقدر الضروري من المعلومات اللازم للمشاركة في الألعاب أو المسابقات وغيرها، تاركاً بذلك مجالاً لتفسير النص وفقاً لكل حالة مما قد يؤدي الي خلل في التطبيق. ولكن من ناحية أخري فقد اشترط المشرع موافقة ولي الأمر لإجراء أي عملية مما ذُكر تتعلق ببيانات الأطفال.

وقد اتبعت لائحة الاتحاد الأوروبي ذات معيار المشرع المصري فيما يتعلق بالموافقة على معالجة بيانات الأطفال. حيث نصت المادة ٨ من اللائحة[٨٣] على أنه في حالة الحصول على موافقة الشخص المعني بالبيانات، تكون معالجة البيانات الشخصية للطفل قانونية عندما يكون الطفل في السادسة عشرة من عمره على الأقل. وفي حالة عدم بلوغ الطفل سن السادسة عشر، لا تكون هذه المعالجة قانونية إلا إذا أذن ولي أمر الطفل بذلك.

(٨٣) نفس المرجع.

(ISSN: 2356 - 9492)

كما نظم قانون حماية البيانات موضوع التسويق الالكتروني الحر، الذي يعرف بأنه إرسال أي رسالة أو بيان أو محتوي إعلاني أو تسويقي بأي وسيلة تقنية أيًا كانت طبيعتها أو صورتها، تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلي أشخاص بعينهم.

وقد حظر قانون حماية البيانات الشخصية إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات، إلا بتوافر مجموعة من الشروط هي:

- ضرورة الحصول على موافقة من الشخص المعني بالبيانات.
- ضرورة أن يتضمن الاتصال هوية منشئه ومرسله.
- أن يكون للمرسل عنوان صحيح وكاف للوصول إليه.
- الإشارة إلى أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر.
- وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسال البيانات.

- **شروط تجميع ومعالجة البيانات الشخصية عبر الحدود**

يقصد بحركة البيانات الشخصية عبر الحدود – وفقاً لما جاء بقانون حماية البيانات الشخصية – نقل البيانات أو إتاحتها أو تسجيلها أو تخزينها أو تداولها أو نشرها أو استخدامها أو عرضها أو إرسالها أو استقبالها أو استرجاعها أو معالجتها، من داخل النطاق الجغرافي لجمهورية مصر العربية إلى خارجه أو العكس.

وقد حظر القانون رقم ١٥١ لسنة ٢٠٢٠، في المادة ١٤ منه، إجراء عمليات نقل البيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلي دولة أجنبية أو تخزينها أو مشاركتها، إلا بعد توفير مستوي الحماية المقرر لحماية البيانات الشخصية في القانون المشار اليه، وبترخيص أو تصريح من مركز حماية البيانات الشخصية. وقد وضع المشرع ثلاثة شروط يجب توافرها ليتمكن المتحكم أو المعالج، بحسب الأحوال، من إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية بعد أن يتم الترخيص له من مركز حماية البيانات الشخصية، وتتمثل تلك الشروط في الآتي:

١- أن تتفق طبيعة عمل كل من المتحكمين أو المعالجين، أو أن يتحد الغرض الذي يحصلان بموجبه على البيانات الشخصية.

٢- أن تتوافر مصلحة مشروعة لدي كل من المتحكمين أو المعالجين للبيانات الشخصية أو لدي الشخص المعني بالبيانات.

٣- ألا يقل مستوي الحماية القانونية والتقنية للبيانات الشخصية لدي المتحكم أو المعالج، الموجودة بالخارج، عن المستوي المتوافر في جمهورية مصر العربية.

ومع ذلك فقد استثني القانون حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه، علي نقل أو مشاركة أو تداول أو معالجة بياناته الشخصية إلي دولة لا يتوافر فيها مستوي الحماية المطلوب قانوناً، وذلك في حالات محدده، هي:

١- المحافظة علي حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له.

٢- تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة أو الدفاع عنه.

٣- إبرام عقد، أو تنفيذ عقد مبرم بالفعل، أو سيتم إبرامه بين المسئول عن المعالجة والغير، وذلك لمصلحة الشخص المعني بالبيانات.

٤- تنفيذ إجراء خاص بتعاون قضائي دولي.

٥- وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة.

٦- إجراء تحويلات نقدية إلي دولة أخري وفقًا لتشريعاتها المحددة والسارية.

٧- إذا كان النقل أو التداول يتم تنفيذًا لاتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفًا فيه.

المطلب الثالث

مركز حماية البيانات الشخصية

مركز حماية البيانات الشخصية هو هيئة عامة اقتصادية تنشأ بمقتضي نص المادة ١٩ من القانون رقم ١٥١ لسنة ٢٠٢٠، وتتبع الوزير المختص ويكون لها الشخصية الاعتبارية، ويكون مقرها الرئيسي بمحافظة القاهرة أو إحدى المحافظات المجاورة لها.

(ISSN: 2356 - 9492)

وينص القانون على أن المركز يهدف إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها. ويرجع الهدف من انشاء هذا الكيان إلى أنه لا يمكن للإطار التشريعي لحماية البيانات أن يكون كاملا دون وجود آلية قوية تشمل انشاء سلطة أو هيئة تتمتع بالصلاحيات والموارد لضمان التنفيذ الفعال لنصوص القانون. ونعرض فيما يلي للهيكل القانوني لمركز حماية البيانات الشخصية وأهم الاختصاصات التي يضطلع بها.

أولا: الهيكل القانوني لمركز حماية البيانات الشخصية

يلتزم الممثل القانوني للشخص الاعتباري لأي متحكم أو معالج بأن يعين داخل كيانه القانوني وهيكله الوظيفي موظفًا مختصًا مسئولاً عن حماية البيانات الشخصية. ويتم تقييد مسئولي حماية البيانات الشخصية بسجل ينشأ بمركز حماية البيانات الشخصية. ويكون الشخص الطبيعي المتحكم أو المعالج هو المسئول عن تطبيق أحكام القانون وقرارات مركز حماية البيانات الشخصية ومراقبة الإجراءات المعمول بها داخل كيانه والإشراف عليها، بالإضافة الى تلقي الطلبات المتعلقة بالبيانات الشخصية.

وقدد حدد القانون رقم ١٥١ لسنة ٢٠٢٠ مجموعة من الاختصاصات المخولة لمسئولي حماية البيانات الشخصية وهي كالتالي:

- إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها.
- العمل كنقطة اتصال مباشرة مع المركز وتنفيذ قراراته، فيما يخص تطبيق أحكام هذا القانون.
- تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في هذا القانون.
- إخطار المركز في حال وجود أي خرق أو انتهاك للبيانات الشخصية لديه.
- الرد على الطلبات المقدمة من الشخص المعني بالبيانات أو كل ذي صفة، والرد على المركز في التظلمات المقدمة إليه من أي منهما وفقا لأحكام هذا القانون.

– متابعة القيد والتحديث لسجل البيانات الشخصية لدي المتحكم أو سجل عمليات المعالجة لدي المعالج، بما يكفل ضمان دقة البيانات والمعلومات المقيدة به.

– إزالة أي مخالفات متعلقة بالبيانات الشخصية داخل كيانه، واتخاذ الإجراءات التصحيحية حيالها.

– تنظيم البرامج التدريبية اللازمة لموظفي كيانه، لتأهيلهم بما يتناسب مع متطلبات قانون حماية البيانات الشخصية.

ثانيا: اختصاصات مركز حماية البيانات الشخصية

حدد القانون أيضا أهم الاختصاصات التي يضطلع بها المركز في إطار تحقيق أهدافه. ومن بين أهم هذه الاختصاصات – التي وردت على سبيل المثال لا الحصر – ما يلي:

– وضع وتطوير السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية، والقيام على تنفيذها.

– توحيد سياسات وخطط حماية ومعالجة البيانات الشخصية داخل الجمهورية.

– وضع وتطبيق القرارات والضوابط والتدابير والإجراءات والمعايير الخاصة بحماية البيانات الشخصية.

– وضع إطار إرشادي لمدونات السلوك الخاصة بحماية البيانات الشخصية، واعتماد مدونات السلوك الخاصة بحماية البيانات الشخصية بالجهات المختلفة.

– التنسيق والتعاون مع جميع الجهات والأجهزة الحكومية وغير الحكومية في ضمان إجراءات حماية البيانات الشخصية، والتواصل مع جميع المبادرات ذات الصلة.

– دعم تطوير كفاءة الكوادر البشرية العاملة في جميع الجهات الحكومية وغير الحكومية القائمة على حماية البيانات الشخصية.

– إصدار التراخيص أو التصاريح والموافقات والتدابير المختلفة المتعلقة بحماية البيانات الشخصية وتطبيق أحكام هذا القانون.

– اعتماد الجهات والأفراد، ومنحهم التصاريح اللازمة التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات الشخصية.

(ISSN: 2356 - 9492)

– تلقي الشكاوى والبلاغات المتعلقة بأحكام هذا القانون، وإصدار القرارات اللازمة في شأنها.

– إبداء الرأي في مشروعات القوانين والاتفاقيات الدولية التي تنظم البيانات الشخصية أو تتعلق أو تنعكس نصوصها بصورة مباشرة أو غير مباشرة عليها.

– الرقابة والتفتيش على المخاطبين بأحكام هذا القانون، واتخاذ الإجراءات القانونية اللازمة.

– التحقق من شروط حركة البيانات عبر الحدود، واتخاذ القرارات المنظمة لها.

– تنظيم المؤتمرات وورش العمل والدورات التدريبية والتثقيفية، وإصدار المطبوعات لنشر الوعي والتثقيف للأفراد والجهات حول حقوقهم فيما يتعلق بالتعامل على البيانات الشخصية.

– تقديم جميع أنواع الخبرة والاستشارات المتعلقة بحماية البيانات الشخصية، وعلى الأخص لجهات التحقيق والجهات القضائية.

– إبرام الاتفاقيات ومذكرات التفاهم والتنسيق والتعاون وتبادل الخبرات مع الجهات الدولية ذات الصلة بعمل المركز وفقًا للقواعد والإجراءات المقررة في هذا الشأن.

– إصدار الدوريات الخاصة بتحديث إجراءات الحماية بما يتوافق مع أنشطة القطاعات المختلفة وتوصيات المركز في شأنها.

– إعداد وإصدار تقرير سنوي عن حالة حماية البيانات الشخصية في جمهورية مصر العربية.

كما يختص المركز بإصدار عدة أنواع من التراخيص والتصاريح والاعتمادات وتحديد أنواعها، ووضع الشروط الخاصة بمنح كل نوع منها وذلك وفقاً لما ستحدده اللائحة التنفيذية للقانون عقب صدورها، وتتمثل أنواع التراخيص والتصاريح والاعتمادات التي يصدرها المركز في الآتي:

– إصدار الترخيص أو التصريح للمتحكم أو المعالج لإجراء عمليات حفظ البيانات، والتعامل عليها ومعالجتها وفقًا لأحكام قانون حماية البيانات الشخصية.

– إصدار التراخيص أو التصاريح الخاصة بالتسويق الإلكتروني المباشر.

- إصدار التراخيص أو التصاريح الخاصة بالمعالجات التي تقوم بها الجمعيات أو النقابات أو النوادي للبيانات الشخصية لأعضاء تلك الجهات وفي إطار أنشطتها.
- إصدار التراخيص أو التصاريح الخاصة بوسائل المراقبة البصرية في الأماكن العامة.
- إصدار التراخيص أو التصاريح الخاصة بالتحكم ومعالجة البيانات الشخصية الحساسة.
- إصدار التصاريح والاعتمادات الخاصة بالجهات والأفراد التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات الشخصية، وإجراءات الامتثال لها.
- إصدار التراخيص والتصاريح الخاصة بنقل البيانات الشخصية عبر الحدود.

كما يجوز للمركز إلغاء الترخيص أو التصريح أو الاعتماد بعد إصداره في حالة مخالفة شروط الترخيص أو التصريح أو الاعتماد، أو عدم سداد رسوم التجديد أو تكرار عدم الامتثال لقرارات المركز أو في حالة التنازل عن الترخيص أو التصريح أو الاعتماد للغير دون موافقة المركز وكذلك في حالة صدور حكم بإفلاس المتحكم أو المعالج.

ونخلص مما سبق إلى أن مركز حماية البيانات الشخصية يسعى إلى توحيد سياسة حماية البيانات الشخصية في جمهورية مصر العربية، وذلك بالتعاون مع كافة الأجهزة والجهات الحكومية وغير الحكومية لضمان توفير أقصى حماية للبيانات الشخصية. بالإضافة إلى وضع خطط لتطوير الكفاءات البشرية في هذا المجال. فضلا عن توحيد جهة إصدار التراخيص والموافقات المتعلقة بحماية البيانات وتلقي الشكاوى المتعلقة بتطبيق قانون حماية البيانات، وممارسة سلطة الرقابة على المخاطبين بأحكام القانون المذكور.

خاتمة

تعد الخصوصية حقا أساسيا من حقوق الإنسان، بمقتضاه يجب اتاحة المجال للأفراد للحفاظ على عدم التدخل غير المطلوب من الغير في حياتهم الخاصة[٨٤]. وقد

(٨٤) د. شريف يوسف خاطر، "حماية الحق في الخصوصية المعلوماتية - دراسة تحليلية لحق الإطلاع على البيانات الشخصية (دراسة مقارنة)"، دار الفكر والقانون ٢٠١٥.

(ISSN: 2356 - 9492)

تطور الحق في الخصوصية على المستوى الدولي والإقليمي، حيث أكدت مختلف الصكوك الدولية لحقوق الإنسان على حظر أي تدخل تعسفي في خصوصية الشخص، أو أسرته أو بيته أو مراسلاته. كما تضمنت دساتير غالبية الدول النص على الحق في صون وحماية حرمة الحياة الخاصة. وتختلف الدول في مدى اعترافها بأهمية الحق في الخصوصية عن طريق التوسيع أو التضييق من نطاق القانون العام المنظم لمسألة انتهاك سرية المعلومات أو الحق في حماية الحياة الخاصة. ويبرز الحق في الخصوصية في بعض البلدان بوصفه قيمة دينية. وبالتالي فإن هذا الحق ليس فقط حق إنساني يحظى بحماية دستورية، انما هو حق يدعم حقوق أخرى للإنسان ويشكل الأساس لأي مجتمع ديمقراطي(٨٥).

وقد أثر التطور التكنولوجي بشكل كبير على الحق في الخصوصية. فمن ناحية أصبحت الدول قادرة على تطوير مرافق لحفظ السجلات، كما ساعدت البرامج الحاسوبية في تعزيز جمع البيانات الشخصية وتخزينها وتبادلها بشكل هائل(٨٦). وقد أدى ذلك الى توفر كمية هائلة من بيانات المواطنين لدى أجهزة الدولة المختلفة.

وتأتي المراقبة الحكومية على قمة الأساليب التي تلجأ اليها الحكومات لدوافع متعددة – منها مكافحة الجرائم شديدة الخطورة والحفاظ على الأمن القومي ومراعاة الصالح العام – دون وجود ضمانات قانونية كافية لحماية الحق في الخصوصية. لذلك بدأ المجتمع الدولي في دعوة الدول إلى تقييد آلية المراقبة بقدر الإمكان، ووضع قواعد قانونية من شأنها تعزيز الضمانات وتشديد القيود على استخدام أنظمة المراقبة، وإيجاد آليات للرقابة الفعالة على الجهات المعنية، وصدور الإذن من الكيانات الرقابية، وذلك بالشكل الذي يعزز حماية الحق في الخصوصية.

---

(٨٥) تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، السيد مارتين شاينين، مجلس حقوق الإنسان الدورة الثالثة عشرة البند ٣ من جدول الأعمال تعزيز وحماية كافة حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية، ص ٧: http://hrlibrary.umn.edu/arabic/AR-HRC/AHRC13-127.pdf

(٨٦) د. محمود عبد الرحمن محمد، "نطاق الحق في الحياة الخاصة"، الطبعة الاولى، منشوارت دار النهضة العربية، القاهرة، ١٩٩٤، ص ٧٦.

ومن جانب آخر، فإن الحق في حماية البيانات الشخصية يرتبط ارتباطا وثيقا بالحق في الخصوصية. وقد أشارت دساتير معظم الدول إلى الحق في الخصوصية كحق دستوري أصيل. ولكن هناك اختلاف حول مدلول "مبدأ الخصوصية"، حيث يختلف معنى الخصوصية من بلد لآخر وفقا لاختلاف الثقافات، والعوامل البيئية، والتاريخية، وغيرها. ومع ذلك، ففي عصر المعلوماتية تعترف معظم الدول بالحق في حماية البيانات الشخصية، لما تحمله من أهمية كبيرة في المجتمع الرقمي الحديث. كما تسعى الدول إلى تطوير الأطر التشريعية لحماية مستخدمي شبكة المعلومات الدولية من التلاعب ببياناتهم الشخصية.

ومن خلال دراسة الأنظمة القانونية المختلفة، نجد أنه لا يمكن ضمان الخصوصية بشكل كامل من خلال فرض أطر قانونية وتنظيمية محلية ودولية فقط. لذلك بدأ التوجه إلى ضرورة تأسيس فكرة الخصوصية ودمجها في عمليات التصميم الهندسي والتكنولوجي ليظهر مبدأ "الخصوصية حسب التصميم" بوصفه نموذج عملي لمراعاة القيم الإنسانية بشكل قابل للتحديد الدقيق خلال العمليات الهندسية برمتها. ويتبلور الهدف الأساسي "للخصوصية حسب التصميم" في ضمان الخصوصية والسيطرة الشخصية على المعلومات من قِبل المستخدمين. وتستند "الخصوصية حسب التصميم" إلى المبادئ التالية[٨٧]:

- الاستباقية لا رد الفعل؛
- الوقاية غير العلاجية؛
- اعتبار الخصوصية جزءا لا يتجزأ من التصميم؛
- حماية التشفير من المصدر إلى الوجهة " end – to – end protection"؛
- الشفافية

(87) Ann Cavoukian, "Privacy by Design - The 7 Foundational Principles", PhD, Information and Privacy Commissioner, Ontario, Canada, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

(ISSN: 2356 - 9492)

وينبغي أن تساعد هذه المبادئ على تطوير الكثير من التطبيقات من حيث الحفاظ على الخصوصية وحماية البيانات الشخصية، ولكنها تحتاج إلى أسس قوية ورقابة قانونية لتطبيقها بشكل سليم.

وفي أواخر عام ٢٠٠٩[٨٨]، أشارت نتائج المشاورات العامة التي أجرتها المفوضية الأوروبية – بشأن الكيفية التي يمكن بها للإطار القانوني الحالي لحماية البيانات أن يعالج على أفضل نحو تحديات العولمة والتغير التكنولوجي – إلى أن مفهوم "الخصوصية حسب التصميم" قد يُستحدث كمبدأ جديد، خاصة في بعض المجالات الأكثر استخداما مثل، مواقع شبكات التواصل الاجتماعي أو الحوسبة السحابية، وتوسيع نطاق وضع الاعدادات على الخصوصية بشكل تلقائي "Privacy by default ".

وفي هذا الإطار نعرض لبعض القواعد الواجب اتباعها لضمان تغطية الأنظمة القانونية لجانب أكبر من التطبيقات المعتمدة على تكنولوجيا المعلومات وخدمات الحوسبة السحابية وضمان فاعلية أكبر في حماية الحق في الخصوصية[٨٩]:

١- مسئولية مستخدمو خدمات الحوسبة السحابية

يجب أن يتم وضع آليات قانونية تضمن التزام العميل – كمتحكم في مضمون المعلومات التي يتم تخزينها على السحابة – بتشريعات حماية البيانات وخضوعه لجميع الالتزامات القانونية التي تفرضها تشريعات الدولة التي يخضع لها. كذلك يجب على العميل اختيار مزود خدمات الحوسبة السحابية الذي يضع قواعد تعاقدية تضمن الامتثال لتشريعات حماية البيانات بما يتفق مع القوانين المحلية التي يخضع لها.

(88) Del Mar López Ruiz M., Pedraza J. (2016) Privacy Risks in Cloud Computing. In: Kołodziej J., Correia L., Manuel Molina J. (eds) Intelligent Agents in Data-intensive Computing. Studies in Big Data, vol 14. Springer, Cham. https://doi.org/10.1007/978-3-319-23742-8_8.

(89) Del Mar López Ruiz M., Pedraza J. (2016) Privacy Risks in Cloud Computing. In: Kołodziej J., Correia L., Manuel Molina J. (eds) Intelligent Agents in Data-intensive Computing. Studies in Big Data, vol 14. Springer, Cham. https://doi.org/10.1007/978-3-319-23742-8_8.

٢- ضمانات التعاقد من الباطن

يجب أن يتم النص على أحكام للمتعاقدين من الباطن في أي عقد بين مزود السحابة وعملاء خدمات الحوسبة السحابية. وينبغي أن يحدد العقد أنه لا يجوز تكليف المتعاقدين من الباطن بمعالجة البيانات من قبل مزودي الخدمات، إلا بعد موافقة صاحب البيانات مع احتفاظ الأخير في جميع الأحوال بإمكانية الاعتراض على التغييرات التي يحدثها المتعاقد من الباطن أو إنهاء العقد.

كذلك يجب أن يكون هناك التزام واضح من مزودي خدمات الحوسبة السحابية بتسمية جميع المتعاقدين من الباطن. ويجب أن تعكس العقود المبرمة مع المتعاقدين من الباطن الشروط المتعاقد عليها بين مزودي الخدمات السحابية والعملاء. وعلاوة على ذلك، يجب أن تكون هناك آليات تسمح لمستخدمي الخدمات باللجوء للقضاء في حالة مخالفة البنود التعاقدية من قبل المتعاقدين من الباطن لمزودي الخدمات.

٣- تعزيز الضمانات التعاقدية بين مزودي الخدمات السحابية ومستخدمي الخدمات

يجب أن توفر العقود مع مقدمي الخدمات بصفة عامة ضمانات كافية من حيث الأمن التقني والتدابير التنظيمية. كما ينبغي أن يُفصّل العقد التعليمات الموجهة للعملاء بما في ذلك موضوع الخدمة وإطارها الزمني، ومستويات الخدمة الموضوعية والقابلة للقياس والعقوبات المالية أو غيرها في حالة مخالفة الشروط. ويتعين أن تحدد نصوص العقد التدابير الأمنية الواجب الامتثال لها للحماية من مخاطر معالجة البيانات، بما يتماشى مع القواعد الواردة في القانون الوطني للعميل.

وبالنسبة للمصرح لهم بالوصول إلى بيانات العملاء، فيجب أن يتم إدراج شرط السرية في العقد في مواجهة مقدم الخدمة وموظفيه، بحيث يقتصر الحق في الوصول للخدمة على الأشخاص المخولين بذلك فقط.

أما عن الإفصاح عن البيانات لأطراف ثالثة، فيجب أن يتم تنظيم ذلك في العقد، بحيث يُلزم مقدم الخدمة بتسمية جميع المتعاقدين معه من الباطن الذين يساهمون في توفير خدمة السحابة المعنية وجميع المواقع التي قد يتم فيها تخزين البيانات أو معالجتها من قبل مزودي الخدمات أو المتعاقدين معهم. كذلك يجب أن يتضمن العقد آليات

(ISSN: 2356 - 9492)

تضمن وصول العميل إلى المعلومات عن أي تغييرات من أجل تمكينه من الاعتراض على تلك التغييرات أو إنهاء العقد. ويتعين أن يشتمل العقد على بند يلزم مقدم الخدمة بإخطار العميل بأي طلب للكشف عن البيانات الشخصية من قبل سلطات إنفاذ القانون، ما لم يكن هذا الكشف محظورا بموجب القانون. بالإضافة إلى التزام مقدم الخدمة برفض أي طلبات للكشف عن البيانات إذا كانت غير ملزمة قانونا.

ومن الضروري أيضا أن تشتمل بنود العقد على نص يُلزم مقدم الخدمة بكفالة حق العميل في مراقبة عمليات معالجة البيانات الخاصة به، وتسهيل وصوله لها وتصحيحها أو محوها، بالإضافة إلى التزام مزود الخدمة بإخطار العميل بأي اختراق لبياناته الشخصية فور حدوث ذلك.

وفي حالة نقل البيانات عبر الحدود، يتعين أن يضمن العقد أن تتم عملية النقل بشكل قانوني وفقا لقواعد القانون الوطني للعميل. كذلك يجب أن يضمن العقد منع نقل البيانات أو المعلومات إلى البلدان التي يحددها العميل، إذا كان ذلك ممكنا. وتتطلب عمليات نقل البيانات عبر الحدود إلى تطبيق ضمانات أعلى للخصوصية نظرا لتباين القواعد القانونية المنظمة لها من بلد لآخر. ويعد اللجوء للشروط التعاقدية القياسية من أشهر الممارسات المتبعة للحد من مخاطر انتهاك خصوصية البيانات في هذه الحالة.

وأخيرا، ينبغي أن يشتمل العقد على تدابير تقنية وتنظيمية تهدف إلى معالجة المخاطر الناجمة عن نقص الرقابة التي تبرز بشكل واضح في بيئة الحوسبة السحابية. وتعمل هذه التدابير على ضمان النزاهة والسرية والشفافية.

ومن جانب آخر فان أي قانون ينظم حماية البيانات الشخصية يجب أن ينص على مجموعة من الحقوق الأساسية للمستخدم، بحيث لا تترك لتقدير الكيانات التي تستخدم البيانات، ووفقا للائحة الاتحاد الأوروبي لحماية البيانات الشخصية[٩٠] يمكن إجمال هذه الحقوق كالآتي:

(90) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

١- الحق في الوصول إلى البيانات

فينبغي أن يكون لصاحب البيانات الحق في الوصول إلى بياناته الشخصية التي تم جمعها، وممارسة هذا الحق بسهولة وعلى فترات زمنية معقولة، من أجل أن يكون على علم بمشروعية المعالجة والتحقق منها. ويشمل ذلك حق الأشخاص في الوصول إلى البيانات المتعلقة بصحتهم، مثل البيانات المسجلة في سجلاتهم الطبية التي تحتوي على معلومات مثل التشخيصات ونتائج الفحص والتقييمات التي يجريها الأطباء المعالجون. وينبغي ألا يؤثر هذا الحق سلبا على حقوق الآخرين أو حرياتهم، بما في ذلك الأسرار التجارية أو الملكية الفكرية، ولا سيما حق المؤلف الذي يحمي البرنامج. غير أن نتيجة هذه الاعتبارات لا ينبغي أن تكون رفض تقديم جميع المعلومات إلى صاحب البيانات.

٢- الحق في الاعتراض على معالجة البيانات الشخصية

يحق للمستخدم أن يعترض، في أي وقت على معالجة البيانات الشخصية المتعلقة به حتى وإن كانت المعالجة مشروعة ويشمل هذا الحق الاعتراض على الآليات الأوتوماتيكية في صنع القرار.

وفي حالة اعتراض المستخدم لا يحق للمتحكم القيام بمعالجة بياناته الشخصية إلا إذا أظهر أسبابا مشروعة ومقنعة للمعالجة وكانت تتجاوز مصالح وحقوق وحريات المستخدم، ويكون ذلك على سبيل المثال في حالات المعالجة الضرورية لمقتضيات الصالح العام.

٣- الحق في محو أو حذف البيانات الشخصية "الحق في النسيان"،

يحق للمستخدم أن يطلب حذف جميع بياناته الشخصية عند مغادرته التطبيق أو الخدمة الالكترونية. وقد حددت اللائحة الأوربية لحماية البيانات الحالات التي يحق للفرد فيها محو بياناته الشخصية، وهي كالتالي:

- إذا لم تعد البيانات الشخصية ضرورية للغرض الذي تم تجميعها أو معالجتها بواسطة المؤسسة من أجله في الأساس.

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Ibid*.

(ISSN: 2356 - 9492)

– إذا كانت المنظمة التي تعالج البيانات تعتمد موافقة الفرد كأساس قانوني لمعالجة بياناته، وقام المستخدم بسحب موافقته.

– إذا كانت المنظمة التي تعالج البيانات تعتمد على فكرة المصالح المشروعة كمبرر لمعالجة بيانات الفرد، واعترض المستخدم على هذه المعالجة، وليس هناك مصلحة مشروعة طاغية للمنظمة تجبرها على مواصلة المعالجة.

– أن تقوم مؤسسة بمعالجة البيانات الشخصية لأغراض التسويق المباشر واعترض المستخدم على هذه المعالجة.

– إذا عالجت منظمة البيانات الشخصية للشخص بشكل غير قانوني.

– كما تلتزم المنظمة التي تعالج البيانات بمحو البيانات الشخصية في حالة وجوب الامتثال لحكم قضائي أو التزام قانوني.

– أن تقوم مؤسسة بمعالجة البيانات الشخصية للطفل لأغراض تقديم الخدمات المعلوماتية الخاصة بها.

ومع ذلك، قد يتجاوز حق المؤسسة في معالجة بيانات شخص ما حقه في المحو أو النسيان. وقد أقرت اللائحة الأوروبية لحماية البيانات الشخصية بعض الحالات التي يعلو فيها الحق بالاحتفاظ بالبيانات الشخصية لدى الجهة المعالجة لها على الحق في المحو، وتتمثل هذه الحالات في الآتي:

– إذا كانت البيانات تستخدم لممارسة الحق في حرية التعبير والإعلام.

– إذا كانت البيانات تستخدم للامتثال لحكم قضائي أو التزام قانوني.

– إذا كانت البيانات تستخدم لأداء مهمة يقتضيها الصالح العام أو من مقتضيات مهام السلطة العامة.

– إذا كانت البيانات التي يجري معالجتها ضرورية لأغراض الصحة العامة وتخدم المصلحة العامة.

– إذا كانت البيانات التي يجري تجهيزها ضرورية لإجراء الطب الوقائي أو المهني. ولا ينطبق هذا إلا عندما تتم معالجة البيانات من قبل أخصائي صحي يخضع لالتزام قانوني بالسرية المهنية.

– إذا كانت البيانات المعالجة تمثل معلومات هامة تخدم المصلحة العامة أو البحث العلمي أو الأغراض الإحصائية أو البحوث التاريخية، ويكون من المرجح أن يؤدي محو البيانات إلى إعاقة أو وقف التقدم نحو تحقيق الهدف من المعالجة.

– إذا كانت البيانات تستخدم لتقديم دفاع قانوني أو لرفع دعوى قضائية.

وعلاوة على ذلك، يمكن للمنظمة التي تعالج البيانات أن تطلب "رسما معقولا" للمحو.

٤– حق المستخدمين في تصحيح أو تعديل البيانات الشخصية غير الدقيقة

فيكون من حق المستخدم أن يطلب تصحيح أو تعديل البيانات الشخصية غير الدقيقة عنه دون تأخير لا مبرر له من جانب المعالج للبيانات. ومع مراعاة أغراض المعالجة، يحق للمستخدم أن يستكمل بياناته الشخصية غير المكتملة، حتى ولو عن طريق إضافة بيان تكميلي.

٥– الحق في تلقي معلومات واضحة ودقيقة من الكيانات التي تتولى معالجة بيانات المستخدمين

فسواء قامت هذه الكيانات بتجميع المعلومات بشكل مباشر من المستخدم أو من أطراف ثالثة يجب أن تلتزم بتحري الدقة في البيانات المقدمة للمستخدم. ويجب أن تكون كافة المعلومات المقدمة للمستخدم في شكل موجز وواضح ومع إمكانية النفاذ اليها بسهولة. ويجب أيضا أن تشتمل هذه المعلومات على تفاصيل البيانات التي يتم معالجتها والأغراض التي سوف تستخدم فيها ومدة الاحتفاظ بها. كذلك يجب توفير بيانات الاتصال بهذه الكيانات لتمكين المستخدمين من الاتصال بهم في حالة وجود شكاوى.

٦– الحق في الاستفسار الذي يسمح للمستخدم بالحصول على معلومات حول أسباب المعالجة التلقائية للبيانات الشخصية والنتائج المترتبة على تلك المعالجة.

وننتهي مما سبق إلى ضرورة تدخل المشرع لحماية الحق في الخصوصية بشكل شامل بنصوص قانونية دقيقة ومتناسبة مع المعايير الدولية لحماية هذا الحق. لذلك يجب على كافة الدول الاتجاه نحو سن تشريعات لحماية الحق في الخصوصية

(ISSN: 2356 - 9492)

المعلوماتية تضمن وجود حماية قانونية واضحة للأفراد، وتمنع الإفراط في جمع المعلومات الشخصية، وتكفل اتخاذ تدابير تضمن دقة المعلومات، وتضع حدودا لاستخدام المعلومات وتخزينها وتبادلها، وتلزم بإخطار الأفراد بكيفية استخدام المعلومات الخاصة بشكل آمن.

كما يجب إنشاء جهات رقابة قوية ومستقلة لمراجعة سياسات وممارسات الجهات الحكومية وضمان وجود رقابة قوية على استخدام تقنيات المراقبة ومعالجة المعلومات الشخصية وتطبيق مبادئ التناسب والضرورة. ويجب ألا يكون هناك نظام سري للمراقبة لا يخضع لاستعراض هيئة رقابية، بالإضافة الى ضرورة الحصول على إذن من هيئة مستقلة في جميع التدخلات المتعلقة بالبيانات الشخصية للأفراد.

كذلك يجب أن يتضمن أي برنامج مراقبة قائم على قوائم الفئات التي تخضع للمراقبة أو على المعلومات المتعلقة بالملامح الشخصية، الضمانات المتعلقة بمراعاة الإجراءات القانونية الواجبة لجميع الأفراد، بما في ذلك الحق في التعويض عن الضرر. ويجب تعزيز مبدأ الشفافية حتى يتم إعلام الأفراد بسبب وكيفية إضافتهم إلى قوائم المراقبة، أو كيفية وضع المعلومات عن ملامحهم الشخصية، وبآليات الطعن المتاحة لهم.

ومن الضروري أيضا وضع قواعد دولية أكثر فعالية تحد من وصول الحكومات إلى المعلومات التي تحتفظ بها أطراف ثالثة، بالإضافة الى تشديد الضمانات الدستورية المقررة داخل الدول. فقد تخضع أطراف ثالثة لقوانين أجنبية تتطلب الإفصاح عن بعض المعلومات التي تشكل انتهاك للحق في الخصوصية في القوانين الداخلية للدول. فحكومة الولايات المتحدة الأمريكية، على سبيل المثال، قد تمكنت عن طريق وزارة المالية من رصد المعاملات المالية الأجنبية عبر شبكة جمعية الاتصالات المالية بين المصارف على مستوى العالم (سويفت)[٩١]، وذلك بهدف العثور على المشتبه بهم في الانتماء لجماعات إرهابية. وقد تقدمت جماعات حقوق الإنسان بشكاوى قانونية في أكثر

(٩١) وهي الجمعية التعاونية البلجيكية المسؤولة عن تبليغ الرسائل فيما بين أكثر من ٨٠٠ ٧ مؤسسة مالية منتشرة في أكثر من ٢٠٠ بلد.

من ٢٠ محكمة محتجة بأن تلك الجمعية انتهكت القوانين المحلية المتعلقة بالخصوصية بتسليمها هذه المعلومات إلى سلطات الولايات المتحدة(٩٢).

وبالرغم من ذلك، فهناك العديد من الدول التي لا تزال لديها ضمانات دستورية قوية ومطبقة لحماية الحق في حرمة الحياة الخاصة في مواجهة الأطراف الثالثة. ففي كندا، على سبيل المثال، ينص ميثاق الحقوق والحريات على حماية خصوصية المعلومات التي تحتفظ بها الأطراف الثالثة إذا كانت تكشف تفاصيل خاصة متعلقة بأسلوب الحياة والخيارات الشخصية للأشخاص. ويتطلب تحقيق الحماية لهذا الحق اعمال التوازن بين الحفاظ على كرامة الفرد واستقلاله مع رعاية الصالح العام وإنفاذ القوانين بشكل فعال. كذلك أكدت السوابق القضائية للاتفاقية الأوربية لحقوق الإنسان أن الحق في الخصوصية يشمل المعلومات التي تحتفظ بها أطراف ثالثة. وتنص اتفاقية حماية الأفراد فيما يخص المعالجة الآلية للبيانات الشخصية، على التزام كل من القطاعين العام والخاص بحماية المعلومات التي يحتفظون بها، وتنظم الاتفاقية مشاركة المعلومات مع الوكالات الحكومية(٩٣).

ونشير في النهاية إلى أن الحق في الخصوصية لا يعد حقا مطلقا، بل مثله مثل كافة الحقوق الأساسية، تتمتع الحكومات بسلطة فرض بعض القيود المعقولة عليه. فهناك بعض الاستثناءات التي تطبقها الدول عندما يتعلق الأمر بحماية أمن الدولة أو السلامة العامة أو المصالح النقدية للدولة، أو قمع جرائم جنائية، أو حماية الأفراد، أو حقوق الآخرين وحرياتهم. ولكن تلك القيود يجب أن تخضع لعدة شروط أولها أن يكون هناك قانون يبرر تقييد الحق في الخصوصية. بالإضافة إلى أن يكون التقييد بسبب هدف مشروع للدولة. كما يجب أن يقع ضمن نطاق المعقولية، وذلك بأن تكون القيود المفروضة متناسبة مع الهدف الذي يسعى القانون إلى حمايته.

(٩٢) تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، السيد مارتين شاينين، مجلس حقوق الإنسان الدورة الثالثة عشرة البند ٣ من جدول الأعمال تعزيز وحماية كافة حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية، ص ٢٢: http://hrlibrary.umn.edu/arabic/AR-HRC/AHRC13-127.pdf

(٩٣) ذات المرجع السابق، ص ٢٣.

(ISSN: 2356 - 9492)

قائمة المراجع

أولا: المراجع العربية

- **الكتب:**

- بوليين أنطونيوس أيوب، "الحماية القانونية للحياة الشخصية في مجال المعلوماتية"، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٩.

- د. شريف يوسف خاطر، "حماية الحق في الخصوصية المعلوماتية – دراسة تحليلية لحق الإطلاع على البيانات الشخصية (دراسة مقارنة)"، دار الفكر والقانون ٢٠١٥.

- د. حسام الدين الأهواني، "الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني"، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، يناير ويوليو ١٩٩٠، العددان الأول والثاني، السنة الثانية والثلاثون.

- د. علي أحمد عبد الزغبي، " حق الخصوصية في القانون الجنائي "، المؤسسة الحديثة للكتاب، ٢٠٠٦.

- د. مصطفى احمد، "الحياة الخاصة ومسئولية الصحفي"، دار الفكر العربي، ٢٠٠١.

- د. وليد السيد سليم، "ضمانات الخصوصية في الانترنت"، الطبعة الاولى، دار الجامعة الجديدة، الاسكندرية، ٢٠١٢، ص ١٨٠.

- **الأبحاث والمقالات:**

- صباح محمد كلو، " الحوسبة السحابية: مفهومها وتطبيقاتها في مجال المكتبات ومراكز المعلومات"،

The SLA-AGC 21st Annual ConferenceAbu Dhabi, United Arab Emirates, 17-19 March 2015.

- **الأحكام القضائية:**

- محكمة النقض، الطعن رقم ١٢١٦ لسنة ٤٩ ق، جلسة ٢٧ يناير ١٩٨٣، أحكام النقض – المكتب الفني – مدني الجزء الأول، السنة ٣٤، ص ٣٣١.

- طعن نقض رقم ١٤٩٩٢ لسنة ٧٨ قضائية – جلسة ٢٠١٧/٥/٨.
- المحكمة الإدارية العليا – الطعن رقم ١٥١١٨ لسنة ٦٥ ق – جلسة ٢١/ ١٢/ ٢٠١٩.
- المحكمة الإدارية العليا – الدائرة الرابعة – في الطعن رقم ٨٦٥٨٤ لسنة ٦٤ ق، جلسة ٢٠٢٠/٦/٢٦.

- **الاتفاقيات والمعاهدات الدولية:**

- الإعلان العالمي لحقوق الإنسان، ١٩٤٨:
https://www.un.org/ar/universal-declaration-human-rights/
- العهد الدولي للحقوق المدنية والسياسية، ١٩٧٦،
https://www.ohchr.org/ar/professionalinterest/pages/ccpr.aspx
- الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم، ١٩٩٠:
https://www.ohchr.org/ar/professionalinterest/pages/cmw.aspx
- الاتفاقية المتعلقة بالجريمة الإلكترونية، المجلس الأوروبي، ٢٣ نوفمبر ٢٠٠١: https://rm.coe.int/budapest-convention-in-arabic/1680739173.
- اتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا روما في ٤ نوفمبر ١٩٥٠.
- الاتفاقية الأمريكية لحقوق الإنسان، سان خوسيه في ٢٢ نوفمبر ١٩٦٩.
- الميثاق الإفريقي لحقوق الإنسان والشعوب، ١٩٨١.
- الميثاق الإفريقي لحقوق ورفاهية الطفل، ١٩٩٠.
- إعلان القاهرة حول حقوق الإنسان في الإسلام، ٥ أغسطس ١٩٩٠.
- اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية في عام ٢٠١١.

- **التقارير الدولية:**

(ISSN: 2356 - 9492)

- تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، السيد مارتين شاينين، الجمعية العامة للأمم المتحدة، مجلس حقوق الانسان، الدورة الثالثة عشر – تعزيز وحماية كافة حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية.
http://hrlibrary.umn.edu/arabic/AR-HRC/AHRC13-127.pdf.

- **القواميس:**

- المعجم الوجيز، مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم ١٩٩٠.

ثانيا: المراجع الأجنبية:

- **الأبحاث والمقالات:**

- Behl, A., Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation. In: World Congress on Information and Communication Technologies (WICT), pp. 217–222 (2011).
- Del Mar López Ruiz M., Pedraza J. (2016) Privacy Risks in Cloud Computing. In: Kołodziej J., Correia L., Manuel Molina J. (eds) Intelligent Agents in Data-intensive Computing. Studies in Big Data, vol 14. Springer, Cham. https://doi.org/10.1007/978-3-319-23742-8_8.
- Gul, I., Ur Rehman, A., Islam, M.H.: Cloud computing security auditing. In: The 2nd International Conference on Next Generation Information Technology (ICNIT), Gyeongju (2011).
- Gurudatt Kulkarni, Jayant Gambhir, Rajnikant Palwe, Marathwada Mitra Mandal ‘s Polytechnic, Pune, " Cloud Computing-Software as Service", International Journal of Computer Science & Information Technology Research Excellence Vol. 2, Issue 1, Jan-Feb 2012.
- Harry D. Krause, “The Right to Privacy in Germany: Pointers for American Legislation?”, Duke Law Journal, Summer, 1965, Vol. 1965, No. 3 (Summer, 1965), pp. 481-530.
- Jed Rubenfeld, "The Right of Privacy", Harvard Law Review , Feb., 1989, Vol. 102, No. 4 (Feb., 1989), pp. 737-807.

- J. J. BRITZ, "TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges to the Information Profession", Department of Information Science University of Pretoria 0002 Pretoria, South Africa, on : http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html.

- Mariarosaria Taddeo, "Cyber Security and Individual Rights, striking the right balance Special issue of Philosophy & Technology – Online Security and Civil Rights", University of Warwick, 2015.

- Michael S. Josephson, "The Assault on Privacy by Arthur R. Miller", Michigan Law Review , Jun., 1971, Vol. 69, No. 7 (Jun., 1971), pp. 1389-1397.

- Neil M. Richards, "The Dangers of Surveillance", 126 Harvard Law Review 1934, 20 May 2013.

- Soghoian, C.: Caught in the cloud: privacy, encryption, and government back doors in the Web 2.0 Era. J. Telecommun. High Tech. L 8, 359–424 (2009).

- Uchenna Jerome Orji, "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?", Article In Masaryk University Journal of Law and Technology · September 2018.

- United Nations Human Rights Office of the High Commissioner, " Online expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine- learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy", 27-28 May 2020, Concept Note.

- **الرسائل العلمية:**

- Clémence CODRON, "La surveillance diffuse: entre Droit et Norme", THÈSE en Droit Public, sous la direction de Professeur Jean-Jacques Lavenue, Université de Lille 2, soutenue le 15 juin 2018.

- **الأحكام القضائية:**

- The European Court of Human Rights, Case of Roger ACMANNE and others v. BELGIUM, 10 December 1984.

(ISSN: 2356 - 9492)

- The European Court of Human Rights, Case of Storck v. Germany, Strasbourg,16 June 2005.
- Human Rights Committee, Case of M.G. v. Germany, 2006.
- Meyer v. State of Nebraska (1923), Supreme Court of The United States, 262 U.S. 390, 1923, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/Meyer%20v%20Nebraska%20%281923%29.html.
- Griswold v. Connecticut (1965), Supreme Court of The United States , 381 U.S. 479, 1965, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/griswold.html.
- Stanley v Georgia (1969), Supreme Court of The United States, 394 U.S. 557 April 7, 1969, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/stanley.html.
- Goodwin & I v United Kingdom [2002], https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life.
- European Court of Human Rights, Case of Gillan and Quinton v. The United Kingdom, 2010, https://hudoc.echr.coe.int.
- European Court of Human Rights, Case of Barbulescu v. Romania, 2017, https://hudoc.echr.coe.int.
- European Court of Human Rights, Case of S. and Marper v. The United Kingdom, 2008, https://hudoc.echr.coe.int.
- The European Court of Human Rights, CASE OF CSOMA v. ROMANIA, STRASBOURG, 15 April 2013.
- Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, paras. 26-27, and 37.

- التقارير الدولية والوثائق:

- Alan F. Westin, Daniel J. Solove, “Privacy and Freedom”, Ig Publishing, 2015, 500 P.
-
- Constitionnet, “Constitutional History of Germany”, https://constitutionnet.org/country/constitutional-history-germany.
- Executive Office of the President of the United States, “Big Data: Seizing Opportunities, Preserving Values”, May 2014, on: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

- Exploring Constitutional Conflicts, “The Right of Privacy”, University OF Missouri-Kansas City, School of Law: http://law2.umkc.edu.
- Human Rights Council, “The right to privacy in the digital age”, Report of the Office of the United Nations High Commissioner for Human Rights, Twenty-seventh session, Agenda items 2 and 3, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General.
- Krishnadas Rajagopal, “The lowdown on the right to privacy”, In The Hindi, July, on : https://www.thehindu.com.
- OHCHR, “The right to privacy in the digital age”, Report of the Office of the United Nations High Commissioner for Human Rights, www.ohchr.org.
- Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI, para.3, 4.
- Statecounter, “Social Media States Egypt”، October 2019 https://gs.statcounter.com/social-media-stats/all/egypt.
- The Boston Consulting Group, “The Internet Economy in the G-20 (The $4.2 Trillion Growth Opportunity)” Report, March 2012.
- The New York Times, “Electronic Surveillance Under Bush and Obama”, U.S. In : https://archive.nytimes.com/www.nytimes.com/interactive/2013/06/07/us/07nsa-timeline.html#/#time254_7504.
- United Nations Human Rights Office of the High Commissioner, Report of the proceedings of the online expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy (27- 28 May 2020).