حماية البيانات الشخصية أثناء المعالجة في ضوء القانون ١٥١ لسنة ٢٠٢٠ واللائحة الأوربية لعام ٢٠١٦

(دراسة مقارنة)

Protection of personal data during processing
In light of Law 151 of 2020
And the European Regulation of 2016
(Comparative Study)

إعداد

الدكتور/ خالد مصطفي على فهمي إدريس

عضو هيئة التدريس بجامعة السلام الخاصة بطنطا

البريد الإلكترونى : khalededrraas@gmail.com

ملخص:

تعاظم دور التكنولوجيا في العصر الحالي فأصبحت منصة للمعلومات والبيانات، وأصبحت البيانات الشخصية متاحة على نطاق واسع ويتم تداولها بشكل يمكن أن يضر بأصحابها، بل إن المواقع الإلكترونية لا تقدم الخدمة للمتقدم إلا بعد حصولها على كافة بياناته، وأصبحت هذه المواقع الإلكترونية تستغل هذه البيانات لأغراض أخرى غير تلك التي بثت من أجلها، مما أدى إلى انتهاك خصوصية الشخص. حيث إن حماية البيانات الشخصية لكل فرد تشكل أساساً لاحترام حقوقه وحرياته كما أنها تشكل أساساً لمجموعة من الحقوق المتعلقة به، والهدف ليس فقط حماية البيانات الشخصية، بل حماية الحقوق والحريات الأساسية لأصحاب تلك البيانات في ظل تجميع العديد من الجهات لبيانات الأشخاص بشكل يؤثر على مصالح صاحب تلك البيانات. ومن هذا المنطلق، أصدر المشرع القانون رقم ١٥١ لسنة ٢٠٢٠ لحماية البيانات الشخصية، والذي استوحاه من اللائحة الأوروبية لحماية البيانات لسنة ٢٠١٦. ويهدف القانون إلى إيجاد التوازن بين آليات حقوق الأفراد في حماية بياناتهم الشخصية، والسماح بمعالجة البيانات والمعلومات والاحتفاظ بها في الفضاء الإلكتروني، في ظل انتشار مفاهيم البيانات الضخمة والذكاء الاصطناعي. ويضع أطراً تنظيمية لتخزين البيانات الشخصية ومعالجتها ضمن قيود والتزامات واضحة، مما يساهم في تعزيز الثقة اللازمة في الانخراط في الاقتصاد الرقمي والمساهمة في تشجيع التجارة والخدمات الإلكترونية. كما يهدف القانون إلى بناء بيئة مواتية لضمان سلامة الفضاء الإلكتروني ودعم استقراره، وتحديد الالتزامات والواجبات

المفروضة على المسؤول عن البيانات الشخصية ومعالجها ومتلقيها، والعقوبات والجزاءات المفروضة على المخالفين لأحكام القانون. وينشئ القانون مركزاً لحماية البيانات الشخصية يهدف إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها. وقد تناولنا الموضوع في إطار الحماية المدنية التي وفرها المشرع في مصر أو أوروبا أو في الدول العربية والتي تهدف جميعها إلى حماية خصوصية البيانات المعالجة إلكترونياً، وفي هذا البحث تناولنا بعض جوانب الحماية القانونية للبيانات الشخصية أثناء المعالجة التي أشار إليها القانون ١٥١ لسنة ٢٠٢٠ واللائحة الأوروبية لسنة ٢٠١٦ وبعض التشريعات العربية، وذلك من خلال ثلاثة مباحث بدأناها بمبحث تمهيدي عن طبيعة البيانات الشخصية ونطاق تطبيقها، ومبحث أول عن معالجة البيانات الشخصية ومبحث ثان عن حق الشخص المعني بالبيانات في المعالجة الصحيحة لبياناته، ومن خلال البحث توصلنا إلى عدد من النتائج والتوصيات.

كلمات مفتاحية:

البيانات الشخصية ، المعالجة ، حقوق الشخص المعني ، اللائحة الأوربية لحماية البيانات، تعويض الأضرار.

Abstract:

The role of technology has increased in the current era and has become a platform for information and data, and personal data has become widely available and is circulated in a way that can harm its owners. Rather, websites do not provide the service to the applicant until they obtain all of his data, and these websites have begun to exploit this data for purposes other than those for which it was broadcast, which has led to a violation of the person's privacy. Since protecting the personal data of each individual constitutes a basis for respecting his rights and freedoms as it is the basis for a group of rights related to him, and the goal is not only to protect personal data, but to protect the basic rights and freedoms of the owners of that data in light of the collection of many parties of people's data in a way that affects the interests of the owner of that data. From this standpoint, the legislator has established Law No. 151 of 2020 to protect personal data, which was taken from the European Data Protection Regulation of 2016. The law aims to create a balance between the mechanisms of individuals' rights

to protect their personal data, and allowing the processing and retention of data and information in cyberspace, in light of the spread of the concepts of big data and artificial intelligence. It establishes regulatory frameworks for storing personal data and processing it within clear restrictions and obligations, which contributes to enhancing the necessary confidence in engaging in the digital economy and contributing to encouraging e-commerce and services. The law also aims to build a favorable environment to ensure the safety of cyberspace and support its stability, and to determine the obligations and duties imposed on the person responsible for personal data, its processor, and its recipient, and the penalties and sanctions imposed on violators of the provisions of the law. The law establishes a center for the protection of personal data that aims to protect personal data and regulate its processing and availability. Accordingly, we addressed the subject within the frameworks of civil protection provided by the legislator in Egypt, Europe or in the Arab countries, all of which aim to protect the privacy of electronically processed data. In this research, we discussed some aspects of

the legal protection of personal data during processing referred to in Law 151 of 2020, the European Regulation of 2016, and some Arab legislation. through three topics that we began with an introductory topic on the nature of personal data and the scope of its application, a first topic on the processing of personal data and a second topic on the right of the person concerned with the data to the correct processing of his data. Through the research, we reached a number of results and recommendations.

Keywords:

Personal data - Processing - Rights of the person concerned - European Data Protection Regulation - Compensation for damages.

مقدمة:

يعيش العالم اليوم في ثورة معلوماتية كبيرة نتيجة التكنولوجيا الحديثة وما تلاها من ثورة كبيرة في نظم الاتصالات والمعلومات، وعلى الرغم من النتائج العظيمة التي أصبح العالم معها وكأنه قرية كونية صغيرة، الأمر الذي ساهم في اختصار الوقت والمكان والتعامل السريع مع البيانات والمعلومات، إلا أنه قد نتج الكثير من الانعكاسات السلبية والمخاطر التي باتت تهدد الأمن القومي بعد أن أصبحت البيانات الشخصية متاحة بواسطة التكنولوجيا الحديثة وصار تداولها بين المستخدمين للشبكة العنكبوتية يتم بيسر الأمر الذي من شأنه الاضرار بحق أساسي من حقوق الإنسان وهو الحق في الخصوصية؛ فالخصوصية هي حق أساسي ومن الحقوق الملازمة للشخصية الطبيعية(١). الأمر الذي دفع كافة المجتمعات للبحث عن سبل حماية هذا الحق، فبدأت الدول في اصدار التشريعات الخاصة بحماية البيانات والمعلومات الشخصية، بعد أن صارت التشريعات التقليدية غير قادرة على حماية الخصوصية

(١) راجع في ذلك- **خالد حسن أحمد**: الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية- دار الكتب والدراسات العربية – الإسكندرية- ٢٠٢٠ – ص٧.

أشارت محكمة العدل الأوربية إلى أن الحق في الخصوصية يعني أن صاحب البيانات على يقين من أن معالجة بياناته الشخصية تتم بطريقة دقيقة وصحيحة وقانونية ويتم الكشف عنها للمستلمين المعتمدين.

CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer، 7 May 2009.

المعلوماتية والانتهاكات الخاصة بالبيانات الشخصية([1]). فالبيانات الشخصية محل الحماية هو تلك البيانات المتعلقة بالأشخاص الطبيعية وليست الاعتبارية([2]). وقد سار المشرع المصري على الدرب الهادف لفرض حماية قانونية فوضع قانون لمكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ ومن بعده قانون لحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠([3])، حيث تسير الدولة بخطًى ثابتة نحو فرض سيطرتها على المجال الرقمي وتداول البيانات، وهو الأمر الذي ينبغي أن يتم وفقًا للمعايير الدولية وحماية للحقوق الأساسية التي أكد عليها الدستور والتشريعات والاتفاقيات الدولية التي صدقت الدولة عليها، وحماية حق المواطن في الخصوصية، وضمانًا للحقوق والحريات الشخصية، وحتى لا يتم استخدام تلك البيانات بشكل غير قانوني من قِبل الغير([4]).

([1]) يحتفل العالم في ٢٨ يناير باليوم العالمي لحماية البيانات الشخصية والحفاظ على خصوصيتها، وهو اليوم الذي وقع فيه أعضاء مجلس أوروبا على وثيقة حماية البيانات الشخصية للتوعية بمخاطر اختراق البيانات وانتهاك الخصوصية.

([2]) **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية- مجلة كلية القانون الكويتية العالمية- س٣-ع٩-مارس ٢٠١٥- ص٤٠١.

([3]) يشير البعض إلى أن هذا القانون يرتبط ارتباطًا وثيقًا بالدفاع عن الحق في الخصوصية، ويعتبر وسيلة من وسائل العودة لحماية الخصوصية التي تعرضت لانتهاكات عديدة بفعل التقدم التكنولوجي والحرب ضد الإرهاب. لذلك فإن التأصيل الفلسفي لهذا القانون يرتبط، بصورة جوهرية، بمعرفة الحق في الخصوصية، باعتباره أحد أهم الحقوق التي نشأت في العصر الحديث- راجع في ذلك: **دراسة نقدية لقانون حماية البيانات الشخصية**- اعداد مركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية – القاهرة- ٢٠٢٠.

([4]) قضت المحكمة الدستورية الفيدرالية الألمانية في عام ١٩٨٣ بسلطة الفرد في اتخاذ قرار بنفسه على أساس فكرة تقرير المصير لتحديد زمان إيصال المعلومات المتعلقة بحياته الخاصة إلى

كانت التوجهات الأوربية قد سارت بخطوات سريعة نحو حماية البيانات الشخصية حيث نص التوجيه الأوربي رقم ٧٦/٤/٨ على حماية الأفراد من أنشطة التقييم الآلي للبيانات (The protection of the individual against the technical evolution of informatic)، كما نص التوجيه الأوربي رقم ٧٩/٥/٨ على حماية الأفراد في مواجهة التطور التقني لمعالجة البيانات (The protection of the rights of the individual in the face of technical developments in data processing)، كما نص التوجيه الأوربي رقم ٤٦/٩٥ على المبادئ الأساسية لحماية البيانات الشخصية، كما نصت اتفاقية مجلس أوروبا بشأن حماية الأفراد في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية لسنة ١٩٨١([1]) على حماية البيانات الشخصية ومن بين تلك البيانات بيانات الهاتف ورسائل البريد الالكتروني واستخدام الانترنت والبيانات المخزنة على

الآخرين وحدود ذلك. حيث يلعب مفهوم تقرير المصير فيما يتعلق بالمعلومات دوراً أساسياً في تطوير تشريعات حماية البيانات وهو مستمد من فكرة آلان ويستن على أن مطالبة الأفراد أو الجماعات أو المؤسسات بأن يقرروا بأنفسهم متي وكيف وإلى أى مدى يتم إيصال المعلومات المتعلقة بهم إلى الآخرين.

([1]) تعرف بالاتفاقية المعالجة التلقائية للبيانات الشخصية (ETS رقم ١٠٨) وهي معاهدة دولية أوربية ملزمة قانونًا لحماية البيانات. ودعا البروتوكول الإضافي للاتفاقية المتعلق بالسلطات الإشرافية وتدفقات البيانات عبر الحدود لعام ٢٠٠١، إلى إنشاء سلطات إشرافية لضمان حماية البيانات واحترام الخصوصية في مشاركة البيانات. ولها بروتوكول آخر (CETS رقم ٢٢٣) وتم تحديث الاتفاقية وتعديلها بالبروتوكول عام ٢٠١٨. ويهدف تحديث الاتفاقية إلى تحقيق هدفين رئيسيين: [١] التعامل مع التحديات الناتجة عن استخدام تقنيات المعلومات والاتصالات الجديدة، [٢] تعزيز التنفيذ الفعال للاتفاقية.

خوادم الكمبيوتر باعتبارها ضمن نطاق حماية المادة الثامنة من الاتفاقية الأوربية لحقوق الإنسان([1]).

وأخيراً وضع الاتحاد الأوربي في ٢٠١٦/٥/٢٤ اللائحة العامة لحماية البيانات ""e règlement général sur la protection des données – RGPD([2]) والتي صدرت عن البرلمان الأوربي والمجلس بقراره رقم ٢٠١٦/٦٧٩ بتاريخ ٢٠١٦/٤/٢٧ شأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، وألغي التوجيه السابق لسنة ١٩٩٥(relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données.)، وأشارت اللائحة إلى وضع مبادئ وقواعد تحكم حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية المتعلقة بهم،

([1]) راجع في ذلك : موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة- www.unodc.org

([2]) دخلت اللائحة حيز التنفيذ يوم ٢٥ مايو ٢٠١٨، وتنطبق على جميع المؤسسات داخل وخارج الاتحاد الأوروبي التي تتعامل مع بيانات سكان منطقة الاتحاد الأوروبي وتعالجها. ويكمن الغرض من اللائحة إلي تقوية حماية البيانات ومنح الأشخاص قدرًا أكبر من التحكم في الطريقة التي يتم بها استخدام وتخزين ومشاركة معلوماتهم الشخصية من قِبل المؤسسات التي لها حق الوصول إليها، بدءًا من أصحاب العمل ووصولاً إلى الشركات التي يشتري هؤلاء الأشخاص أو يستخدمون منتجاتها وخدماتها. كما تفرض على المؤسسات أن تضع حيز التنفيذ عناصر فنية وتنظيمية للتحكم في الأمان والمصممة لتفادي فقدان البيانات، أو تسريب المعلومات، أو الاستخدامات الأخرى غير المصرح به للبيانات- راجع في ذلك **الدراسة النقدية** سابق الاشارة إليها- ص١٩.

مهما كانت جنسية هؤلاء الأشخاص الطبيعيين أو إقامتهم، أن تحترم حرياتهم وحقوقهم الأساسية، ولا سيما حقهم في حماية البيانات الشخصية، وتهدف هذه اللائحة إلى المساهمة في خلق مساحة من الحرية والأمن والعدالة والاتحاد الاقتصادي، وتحقيق التقدم الاقتصادي والاجتماعي، وتوحيد وتقارب الاقتصادات داخل السوق الداخلية، فضلاً عن تحقيق الرفاهية من الأفراد([1]). ومن الصعوبات التي تعترض نظام الحماية القانونية للبيانات الشخصية أن اللائحة الأوربية لاتلزم الدول باتباع نظام معين ولكنها تستهدف نتيجة معينة وتترك للدول حرية تحقيقها بالشكل والوسائل اللازمة لتحقيق تلك النتيجة([2]).

أهداف الدراسة:

الهدف العام من وضع تشريع خاص بحماية البيانات الشخصية التي تم معالجتها إلكترونيا هو تحديد الأطر التنظيمية لاستخدام البيانات الشخصية الخاصة بالمواطنين وحماية تلك البيانات حتى لا تستخدم لغير الغرض الذي نشأت من أجله، فالبيانات الشخصية تتعلق بأمور شخصية وذاتية بمواطنين أمنوا الدولة عليها؛ فاستباحت تناولها لمصلحتهم أو للمصلحة العامة للدولة؛ لذا فإن هناك إشكالية من

([1]) راجع في ذلك:

Guillaume Desgens-Pasanau: RGPD: entre incertitudes et occasions manquées, Dalloz, IP/IT, août / septembre 2016, p.335 .

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

تداولها في غير الأغراض المرخصة لذلك، فالحق في الحصول على المعلومات والبيانات يجب أن يكون في الأطر التي تتعامل معها الدولة؛ لضمان سلامة منظومة الأمن الوطني والقومي بها؛ ولا يباح لأى شخص الحصول علي البيانات الشخصية للآخرين وتداولها، ويجب أن تخضع بيانات الأشخاص لقواعد الحماية حال جمعها أو معالجتها أو الافصاح عنها أو تداولها أو نقلها؛ وخاصة إذا كان ذلك عبر وسائل الاتصال الحديثة وشبكة الانترنت.

وتهدف الدراسة إلى:

[١] التعرف على ماهية البيانات الشخصية محل الحماية المدنية

[٢] إعمال حقوق صاحب البيانات الشخصية ومدى تطابقها من الحقوق والحريات العامة.

[٣] مقارنة المواد القانونية في القانون المصري والقوانين المقارنة مع مبادئ اللائحة الأوربية.

[٤] تحليل بعض المشكلات التي أشار إليها القانون المصري، أو التي لم يشر إليها.

مشكلة الدراسة:

تنبع مشكلة الدراسة أنها تتناول موضوع علمي وفني يتمثل في تحليل ومعالجة البيانات الشخصية إلكترونيا الأمر الذي كان مشكلة بالنسبة للدراسة حيث أن على الباحث البحث في مجالات علمية وفنية وتطبيقها على القانون، كما أن الموضوع محل الدراسة موضوع حديث نسبياً وهو يتعامل مع أضرار تقع على شخص طبيعي

ارتبط بأجهزة تقنية المعلومات والمواقع الالكترونية، وهذه الأضرار أشد من الأضرار البسيطة الخارجة عن التقنيات ووسائل التواصل الاجتماعي والتكنولوجيا الحديثة. وتبدو الاشكالية في مدى التفرقة بين البيانات الشخصية ذات الطابع الخاص والحساس وتلك البيانات الشخصية التي ليست لها طابع خاص ولا ضرر من التعامل معها الكترونياً.

منهج الدراسة:

لما كان المشرع المصري قد أخذ العديد من قواعد من اللائحة الأوربية الخاصة بحماية البيانات الشخصية، فقد تمت الدراسة من خلال عدة مناهج في البحث من خلال الاعتماد على المنهج الوصفي؛ وذلك من خلال عرض النصوص القانونية المرتبطة بالبيانات الشخصية، والمنهج التحليلي وذلك بتحليل تلك النصوص، والمنهج المقارن من خلال بحث القوانين المقارنة والتوجهات الأوربية المتعلقة بموضوع الدراسة ومقارنتها، واستخلاص القواعد والأحكام منها وتحليلها، حيث أن الدراسة ارتبطت بالعديد من القواعد القانونية الوطنية والدولية.

خطة الدراسة:

مبحث تمهيدى: ماهية البيانات الشخصية ونطاق تطبيقها

المبحث الأول: معالجة البيانات الشخصية.

المبحث الثاني: حق الشخص المعني بالبيانات في المعالجة الصحيحة لبياناته

مبحث تمهيدى

ماهية البيانات الشخصية ونطاق تطبيقها

مقدمة:

ماهية الشيء تعني استجلاء حقيقة أمره وطبيعته وخصائصه وسماته([1])، حيث أصبحت البيانات الشخصية متاحة للاطلاع من قبل الكثير من الجهات والأشخاص، مما يعرض تلك البيانات لكثير من الممارسات الخاطئة كالاستعمال غير المشروع لها أو معالجة تلك البيانات دون موافقة أصحابها، وانتهاك حقوق الشخص في الخصوصية؛ لذا جاءت التشريعات والاتفاقيات الدولية لتضع تعريفاً للبيانات الشخصية التي تتضمن أي معلومات تتعلق بشخص ما يمكن استخدامها لتحديده، سواء مباشرة أو غير مباشرة. ويختلف هذا التعريف من قانون لآخر.

ونتناول من خلال هذا المبحث فلسفة إصدار قانون معني بحماية البيانات الشخصية ونطاق تطبيقه المكاني والشخصي، كما نتعرف على المفاهيم المتعلقة بالبيانات الشخصية وأنواع تلك البيانات، وسوف نتناول ذلك من خلال المطلبين التاليين:

([1]) **ميادة مصطفي المحروقي**: الحماية الجنائية لبيانات الأفراد الشخصية المعالجة الكترونيا- المجلة القانونية- جامعة القاهرة – فرع الخرطوم- المجلد رقم ١٦- العدد٧- مايو ٢٠٢٣- ص١٤٨٥.

المطلب الأول: فلسفة إصدار تشريع لحماية البيانات الشخصية ونطاق تطبيقه

المطلب الثاني: تعريف البيانات الشخصية وأنواعها

المطلب الأول

فلسفة إصدار تشريع لحماية البيانات الشخصية ونطاق تطبيقه

أولاً: فلسفة إصدار تشريع لحماية البيانات الشخصية

تعني "فلسفة إصدار قانون لحماية البيانات الشخصية" : الغاية التي يسعي إليها المشرع من إصدار هذا القانون، فالغاية تكمن في حماية البيانات الشخصية للشخص الطبيعي، وقد وضع المشرع في القانون عدداً من المبادئ وترك بعضها لتوضع بمعرفة اللائحة التنفيذية باعتبارها قواعد إجرائية وتنظيمية، فأخذ كثيراً من اللائحة الأوربية المعنية بحماية البيانات، وتنبع فلسفة اصدار هذه اللائحة وغيرها من التوجيهات الأوربية من مجلس أوروبا([1]) إلى تغطية كافة الموضوعات التي يتعامل فيها دول الاتحاد الأوربي فهي عبارة عن قوانين نموذجية تصدر عن البرلمان الأوربي بهدف توحيد قوانين الدول أعضاء الاتحاد في الموضوع الذي يتناوله التوجيه وتكون الدول الأعضاء بالاتحاد ملزمة بإدخال القواعد القانونية التي نص عليها التوجيه في

([1]) **سامح عبد الواحد التهامي**: نطاق الحماية القانونية للبيانات الشخصية والمسئولية التقصيرية من معالجتها- مجلة البحوث القانونية والاقتصادية- العدد ٦٧- ديسمبر ٢٠١٨- ص٦٢٥ هامش٣.

قوانينها الوطنية سواء من خلال اصدار تشريعات جديدة أو تعديل التشريعات السارية لتتماشي مع التوجيه.

كما سبق وذكرنا فإن اللائحة العامة لحماية البيانات (e règlement général sur la protection des données – RGPD) الصادرة عن البرلمان الأوربي بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية قد أرست قواعد تحكم حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية المتعلقة بهم، مهما كانت جنسية هؤلاء الأشخاص الطبيعيين أو إقامتهم، فهي تحترم حرياتهم وحقوقهم الأساسية، لاسيما حقهم في حماية البيانات الشخصية. حيث تهدف هذه اللائحة إلى المساهمة في خلق مساحة من الحرية والأمن والعدالة والاتحاد الاقتصادي، وتحقيق التقدم الاقتصادي والاجتماعي، وتوحيد وتقارب الاقتصادات داخل السوق الداخلية، فضلاً عن تحقيق الرفاهية من الأفراد([1]). وتوافقاً مع اللائحة الأوربية أصدر المشرع الفرنسي القانون رقم ٤٩٣/ ٢٠١٨ المتعلق بحماية البيانات الشخصية حيث وضع القانون أحكام خاصة بتطبيق لائحة الاتحاد الأوربي من قبل الدولة الفرنسية، وكذلك نص على الأحكام المتعلقة بالهيئة الوطنية لتكنولوجيا

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

أشارت الديباجة الخاصة اللائحة أن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية هي حق أساسي. تنص عليه المادة ٨ (١) من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة ١٦ (١) من معاهدة أداء الاتحاد الأوروبي على أن أي شخص له الحق في حماية البيانات الشخصية المتعلقة به.

المعلومات والحريات(Dispositions relatives à la Commission nationale de l'informatique et des libertés)، وهي الهيئة القائمة على مراقبة أعمال المعالجة من قبل الشركات المتخصصة في فرنسا.

أما بالنسبة للمشرع المصري فقد أشار تقرير اللجنة التي أعدت القانون إلى فلسفة إصدار قانون حماية البيانات الشخصية الذي يتمثل في([1]):

[١] ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً.

[٢] وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين، ومكافحة انتهاك خصوصيتهم.

[٣] تطبيق إطار معياري يتواكب مع التشريعات الدولية لحماية البيانات الشخصية للأفراد، وحرياتهم، واحترام خصوصيتهم.

[٤] صياغة التزامات على كل من المتحكم في البيانات، ومعالج البيانات باعتبارهما من العناصر الفاعلة في مجالات التعامل في البيانات الشخصية، سواء عن طريق الجمع أو النقل أو التبادل أو التخزين أو التحليل أو المعالجة بأي صورة من الصور.

([1]) هي اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي – راجع تقرير اللجنة ص٩ وما بعدها.

[٥] إلزام المؤسسات والجهات والأفراد المتحكمين في البيانات الشخصية، والمعالجين لها بتعيين مسئول لحماية البيانات الشخصية داخل مؤسساتهم وجهاتهم، بما يسمح بضمان خصوصية بيانات الأفراد، واقتضاء حقوقهم المنصوص عليها في هذا القانون.

[٦] تقنين وتنظيم أنشطة استخدام البيانات الشخصية في عمليات الإعلان والتسويق على الإنترنت، وفى البيئة الرقمية بشكل عام.

[٧] وضع إطار إجرائي لتنظيم عمليات نقل البيانات عبر الحدود وضمان حماية بيانات المواطنين وعدم نقلها أو مشاركتها مع دول لا تتمتع فيها البيانات بالحماية.

[٨] تنظيم العمليات المعالجة إلكترونيا للبيانات الشخصية، وإصدار تراخيص لمن يقوم بها، وعلى الأخص فيما يتعلق بالبيانات الشخصية الحساسة ذات الطابع الخاص.

[٩] إنشاء مركز حماية البيانات الشخصية كهيئة عامة يكون مختصاً بتنظيم والإشراف على تنفيذ أحكام القانون.

وعليه فإن اللجنة المشار إليها قد وضعت الأطر التي من أجلها أصدر المشرع هذا القانون ليتواكب مع التطورات العالمية في نظم وتكنولوجيا المعلومات وليتوافق مع توجه الدولة نحو وضع إطار حمائي للبيانات الشخصية ووضع أطر تشريعية ولائحية يلتزم بها كافة المتعاملين مع البيانات الشخصية وتكون كافة التعاملات في إطار حماية حقوق الأشخاص، وأن تكون تلك التعاملات تحت بصر المنظمات الحكومية

وعلى رأسها مركز حماية البيانات الشخصية، كما أنها نظمت الالتزامات الواجب الالتزام بها أثناء التعامل مع البيانات الشخصية وفي أي تعامل سواء من خلال المعالجة أو النقل عبر الحدود أو من خلال التسويق أو غير ذلك من أطر التعامل.

ثانياً: نطاق تطبيق تشريع لحماية البيانات الشخصية

نظراً لأهمية وخطورة حماية البيانات الشخصية فقد اختصها المشرع في المادة الأولي من مواد الإصدار فجاء النص ليحدد أن ذلك القانون محدد بنطاق أشخاص محددين وبيانات محددة فهو يتعامل مع:

[١] البيانات الشخصية المعالجة الكترونياً جزئياً أو كلياً،

[٢] محدد بالأشخاص الطبيعيين فلا ينطبق على الأشخاص الاعتباريين([1])،

[٣] لا ينطبق على أي بيانات أخري (فلم ينص القانون على حماية البيانات الورقية أو المكتوبة بطريقة يدوية وهذا وإن كان يتفق مع اللائحة الأوربية إلا أنه يؤثر على حماية تلك البيانات لأنها لا تقل في أهميتها عن البيانات الالكترونية، ولأن البيانات الالكترونية قد تكون في الأصل بيانات ورقية وتم معالجتها الكترونيا طالما

([1]) يحمي القانون رقم ١٧٥ لسنة ٢٠١٨ البيانات المتعلقة بالأشخاص بالمعنوية العامة حيث تعرف البيانات الحكومية في المادة الأولي من القانون: بأنها بيانات متعلقة بالدولة أو احدى سلطاتها أو أجهزتها أو وحداتها أو الهيئات العامة أو الهيئات المستقلة أو الأجهزة الرقابية أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها والمتاحة على الشبكة المعلوماتية أو على أى نظام معلوماتي أو على حاسب أو ما في حكمها.

انصبت على بيانات ذات طابع شخصي نظراً لوحدة الوظائف والأهداف وإن اختلف أسلوبها من الجهة التقنية فيجب أن تمتد الحماية لهما)([1]).

أشارت اللائحة الأوربية في المادة ٢٣ على القيود([2]) ومنحت الدول الأعضاء في الاتحاد الحق في وضع قيود(Limitations) لحماية متطلبات الأمن القومي وغيرها؛ وهذا يعني إمكانية حماية بيانات الأشخاص الاعتباريين حيث أنها تهدف في الأساس لضمان تحقيق توازن عادل بين احترام الحقوق الأساسية للأشخاص الطبيعيين المتأثرين بمعالجة البيانات الشخصية والحاجة إلى حماية المصالح المشروعة الأخرى في مجتمع ديمقراطي([3]). ووفقاً للائحة الأوربية فلكل شخص طبيعي الحق في ممارسة العديد من الحقوق التي منحتها إياه القوانين والتشريعات على اختلافها وأدرجتها صراحة في ثنايا نصوصها حفاظاً منه على بياناته الشخصية والتي هي حق لصيق به، وقد وضعت التشريعات من القيود التي تمنع الاضرار

([1]) راجع في ذلك: **الدراسة النقدية**- سابق الاشارة إليها – ص٢٤.

([2]) تنص المادة ١/٢٣ من اللائحة الأوربية على أنه: يجوز لقانون الاتحاد أو قانون الدولة العضو التي تخضع لها وحدة التحكم أو المعالج، من خلال التدابير التشريعية، أن يحد من نطاق الالتزامات والحقوق المنصوص عليها في المواد من ١٢ إلى ٢٢ وفي المادة ٣٤، وكذلك في المادة ٥ إلى الحد الذي تتوافق فيه أحكام القانون المعني مع الحقوق والالتزامات المنصوص عليها في المواد من ١٢ إلى ٢٢، عندما تحترم هذه القيود جوهر الحقوق والحريات الأساسية وتشكل إجراءً ضروريًا ومتناسبًا في مجتمع ديمقراطي.

([3]) **ميادة مصطفي المحروقي**: المرجع السابق- ص١٤٩٢.

بحقوق الإنسان إلا ما كان منها مرتبطاً بالمساس بالأمن القومي أو الدفاع الوطنى أو السلامة العامة أو منع الجريمة([1]).

كما حدد المشرع النطاق المكاني لسريان هذا القانون حيث نصت المادة الثانية من مواد الإصدار على سريان أحكام هذا القانون والقانون المرافق له علي كل من ارتكب إحدى الجرائم المنصوص عليها في القانون المرافق متي كان الجاني من المصريين داخل الجمهورية أو خارجها، أو كان من غير المصريين المقيمين داخل الجمهورية أو كان من غير المصريين خارج الجمهورية إذا كان الفعل معاقبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية .

وبالتالي فإن القانون ينطبق متي كان مرتكب الفعل من المصريين داخل القطر أو خارجه وكذلك يطبق على غير المصريين المقيمين داخل القطر، وجاء هذا حتى يؤكد على حق الدول في الحفاظ على سيادتها على كل ما يقع من جرائم داخل الدولة وكذلك المصريين داخل الدولة وخارجها باعتبارهم مواطنين ملتزمين بقانون البلد التي يحملوا جنسيتها متي ارتكبوا الفعل المجرم سواء داخل الدولة أو خارجها، وكذلك فقد

([1]) أشارت محكمة العدل الأوربية إلى أن نظام معالجة البيانات الشخصية التي تنص على الدول في تشريعاها يجب أن يتوافق مع قانون الاتحاد الأوربي ويجب على المحاكم الوطنية التأكد من استيفاء هذه الشروط، ولا يجب أن يختلف المعني بين دولة وأخري، وتفسير القانون يجب أن يعكس هدف التوجيه الأوربي

CJEU, C-524/06, Heinz Huber v. Bundesrepublik Deutschland [GC], 16 December 2008, paras. 54, 58-59and 66-68 .

فرض سلطته على غير المصريين الذين يرتكبوا الفعل المحظور خارج نطاق سيادة الدولة متي كان الفعل معاقب عليه في الدولة التي ارتكبوا فيها الفعل وكان السلوك الضار وقع على مصريين أو أجانب مقيمين في الدولة.

كما حدد المشرع سريان القانون فأخذ بمبدأ شخصية وإقليمية القانون إذ يستند **مبدأ شخصية القانون** على مبدأ حق الدولة في السيادة على كل رعاياها، إذ أن الشعب هو الآخر ركن من أركان الدولة فيطبق قانون الدولة على كافة رعاياها أي الأشخاص الذين يحملون جنسيتها (المواطنين) أينما وُجدوا، داخل إقليم الدولة أو خارجها. أما **مبدأ اقليمية القانون** فيستند على مبدأ أساسي في القانون وهو سيادة الدولة على إقليمها، إذ أن الاقليم يعتبر ركناً من أركان الدولة، وبالتالي فإن لهذه الأخيرة حق السيادة الكاملة على كل ما يقع في إقليمها. فيسري القانون بعد نشره ودخوله حيز النفاذ في كل إقليم الدولة بكل أجزائه (البري، الجوي والبحري) ويطبق القانون على كل الأشخاص الطبيعية المقيمين بالإقليم مواطنين أو أجانب.

أشارت المادة الثانية من اللائحة الأوربية إلى النطاق المادى (Champ d'application matériel) التي تطبق عليه اللائحة بحيث أوضح متي تطبق المعالجة ومتي لا تطبق؟، حيث تنص على أنه([1]): تنطبق هذه اللائحة على معالجة البيانات الشخصية كليًا أو جزئيًا بالوسائل الآلية وعلى المعالجة بخلاف الوسائل الآلية للبيانات الشخصية التي تشكل جزءًا من نظام حفظ الملفات، وأضافت الفقرة

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

الثانية من تلك المادة الحالات التي لاتنطبق عليها حيث نصت على أنه: لا تنطبق هذه اللائحة على معالجة البيانات الشخصية: [١] في سياق نشاط يقع خارج نطاق القانون الاتحادي؛ [٢] من قبل الدول الأعضاء عند القيام بالأنشطة التي تقع ضمن نطاق الفصل ٢ من الباب الخامس منTEU ؛ [٣] من قبل شخص طبيعي في سياق نشاط شخصي أو منزلي بحت؛ [٤] من قبل السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو ملاحقتها قضائيا أو تنفيذ العقوبات الجنائية، بما في ذلك الحماية من التهديدات للأمن العام ومنعها.

كما تنص المادة الثالثة من اللائحة الأوربية على أن أحكامه تطبق على الجرائم التي تقع داخل الاتحاد وخارجه(Champ d'application territorial) ، متي تعلقت بأمور خاصة بسلع أو خدمات لأصحاب هذه البيانات داخل الاتحاد أو مكان ينطبق عليه ذلك، ويشير البعض إلى أن اللائحة الأوربية أخذت بمعيار موطن المعالج أو المتحكم في البيانات بصرف النظر عما إذا كانت المعالجة تتم في الاتحاد الأوربي أم لا، كما تنطبق اللائحة على البيانات المتداولة داخل الاتحاد رغم وجود المعالج أو المتحكم خارج الاتحاد متي تعلقت أنشطة المعالجة بعرض سلع أو خدمات لأصحاب هذه البيانات داخل الاتحاد أو يوجد في مكان ينطبق فيه قانون الدول الأعضاء بموجب القانون الدولي العام([1]). وعليه فإن التشريعات تجرم الاعتداء على البيانات الشخصية فتعاقب المقيمين خارجها إذا ارتكبوا جرائم تضر بالمقيمين داخلها

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

سواء كانوا مواطنين بالدولة أو من المقيمين بها. وعليه فإن المشرع معني بالشخص المعني بالبيانات سواء كان من مواطني الدولة أو المقيمين بها إذا وقعت الجريمة عليه([1]).

نص القانون في المادة الخامسة من مواد الإصدار على الاختصاص القضائي بنظر الجرائم المتعلقة بحماية البيانات الشخصية، وأشار القانون لاختصاص المحاكم الاقتصادية دون غيرها بنظر الجرائم المرتكبة بالمخالفة لهذا القانون، فالمحاكم الاقتصادية والتي أنشأت بموجب القانون ١٢٠ لسنة ٢٠٠٨ تختص بنظر بعض الجرائم المرتكبة بالمخالفة لبعض القوانين مثل قانون حماية المستهلك وحماية الملكية الفكرية والتوقيع الالكتروني وغيرها، ونري أنه يجب إنشاء دوائر خاصة داخل تلك المحكمة تختص بحماية البيانات الشخصية.

([1]) راجع في ذلك: **الدراسة النقدية** السابق الاشارة إليها – ص٢٦.

المطلب الثاني

تعريف البيانات الشخصية وأنواعها

أولاً: تعريف البيانات الشخصية

أشارت التشريعات واللائحة الأوربية إلى حماية البيانات الشخصية وأخرجت من جعبتها حماية البيانات غير الشخصية([1])، وتعرف البيانات الشخصية محل الحماية بأنها كافة المعلومات التي لا تدعو مجالاً للشك بأنها الخاصة بشخص محدد، ولم تعد البيانات هي تلك البيانات الخاصة باسم الشخص ولقبه وصفته وبياناته العادية بل كل البيانات الخاصة به من عاداته وسلوكياته ومتطلباته الشخصية وكذا البيانات المتعلقة بجسده (البيانات البيومترية).

عرفت المادة الأولي من القانون المصري رقم ١٥١ لسنة ٢٠٢٠ **البيانات الشخصية** بأنها([2]): 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

([1]) **تعرف البيانات غير الشخصية بأنها** تلك البيانات التي لا تتعلق بشخص معروف ومحدد فهي أى بيانات أخري سواء تلك البيانات التي تتعلق بشخص معنوى باعتبار أنه يخرج عن حدود الحماية القانونية أو بيانات لا تفصح عن شخص طبيعي سواء كانت بيانات متعلقة بالمأكولات أو الطرق أو السيارات أو كانت متعلقة بشخص، ولكن لا يمكن من خلالها تحديد هوية الشخص مثل الذكورة والأنوثة فهي بيانات غير ناطقة بالدلالة على شخص معين.

([2]) يشار إلى أن المادة الأولي من القانون ١٧٥ لسنة ٢٠١٨ قد عرفت البيانات الشخصية بأنها: : أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري.

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. ونري أنه كان على المشرع أن يضيف عبارة وغير ذلك من البيانات ذات الطابع الشخصي دون تحديد فقد يظهر في المستقبل أنواع أخري من البيانات.

عرفت المادة الثالثة من القانون الجزائري رقم (٠٧-١٨) المعطيات ذات الطابع الشخصي بأنها: كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه (الشخص المعني) بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية. كما عرفت المادة ١/١ من القانون المغربي رقم (٠٩-٠٨) المعطيات ذات الطابع الشخصي بأنها: كل معلومة كيفما كان نوعها بغض النظر عن دعامتها بما في ذلك الصوت والصورة والمتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه والمسمي بعده (بالشخص المعني).

عرفت المادة الأولي من نظام حماية البيانات الشخصية السعودى الصادر بالمرسوم الملكي رقم (م/١٩) في ١٤٤٣/٢/٩ هـ الموافق ٢٠٢١/٩/١٦ م البيانات الشخصية بأنها: كل بيان -مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات

الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

عرفت المادة الأولي من القانون الاماراتي رقم ٤٥ لسنة ٢٠٢١ البيانات الشخصية بأنها: أي بيانات تتعلق بشخص طبيعي محدد، أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال الربط بين البيانات، من خلال استخدام عناصر التعريف كاسمه، أو صوته، أو رقمه التعريفي، أو المعرف الالكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية، أو الاقتصادية، أو الثقافية، أو الاجتماعية، وتشمل البيانات الشخصية الحساسة والبيانات الحيوية البيومترية. كما عرف القانون القطري ١٣ لسنة ٢٠١٦ البيانات الشخصية بأنها: بيانات عن الفرد الذي تكون هويته محددة أو يمكن تحديدها بصورة معقولة سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى.

وقد نصت المادة الثامنة من ميثاق الحقوق الأساسية للاتحاد الأوربي على حماية البيانات الشخصية كحق مستقل([1])، وقد عرفت اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوربي بالقرار رقم (2016/679) البيانات

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

الشخصية بأنها([1]): تعني أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته ("موضوع البيانات")؛ الشخص الطبيعي الذي يمكن تحديد هويته هو الشخص الذي يمكن التعرف عليه، بشكل مباشر أو غير مباشر، ولا سيما بالرجوع إلى معرف مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف عبر الإنترنت أو إلى واحد أو أكثر من العوامل المحددة للعوامل الجسدية أو الفسيولوجية أو الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص الطبيعي([2]).

نصت المادة الأولي من القانون الفرنسي إلى أنه يهدف إلى حماية الشخصية والحقوق الأساسية للأشخاص الطبيعيين الذين تخضع بياناتهم الشخصية للمعالجة.

([1]) حلت محل التوجيه الصادر في ١٩٩٥/١٠/٢٤ الذي كان يعرف المعطيات ذات الطابع الشخصي بأنها كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه(الشخص المعني) يعد قابلا للتعرف عليه الشخص الذي يمكن معرفته بصفة مباشرة أو غير مباشرة لا سيما بالرجوع إلى رقم تعريف أو إلى عدة عناصر خاصة مميزة لهويته الطبيعية الفيزيولوجية النفسية الاقتصادية الثقافية أو الاجتماعية.

([2]) راجع في ذلك تلك التعريفات بالقرار الأوربي:

‘ personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person؛

عرف المشرع الفرنسي في القانون ٨٠١ لسنة ٢٠٠٤ البيانات الشخصية بأنه([1]): يعتبر بياناً شخصياً أي معلومات تتعلق بشخص طبيعي تم تحديد هويته أو يمكن التعرف عليه، بشكل مباشر أو غير مباشر، بالرجوع إلى رقم تعريفي أو إلى عنصر أو أكثر خاص به. ولتحديد ما إذا كان من الممكن تحديد هوية الشخص، فمن المناسب النظر في كل وسيلة لتمكين تحديد الهوية المتاح أو الذي يمكن لمراقب البيانات أو أي شخص آخر الوصول إليه.

عرفت المادة الثانية من الفصل الأول (أحكام عامة) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات البيانات بأنها كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما إليها...، ويعرف البعض([2]) البيانات الشخصية بأنها كل بيان يتعلق بالشخص يساعد فى التعرف على هويته كاسمه ولقبه وجنسيته وجنسه ورقم هاتفه وعنوان منزله وكل ما يتعلق بأفراد أسرته وسواء أكان مجال التعرف يشتمل على حروف أو أرقام أو صور أو مقاطع صوتية كما يشتمل بياناته المرتبطة بوسائل الاتصال الالكترونية كعنوان بريده الالكتروني وحساباته الالكترونية وكذلك البيانات المخزنة عبر هذه الوسائل وغير ذلك

([1]) صدر هذا القانون لتفعيل التوجيه الأوربي الصادر في ٢٤ أكتوبر ١٩٩٥ والمتعلق بحماية بيانات الأشخاص وحرية حركة هذه البيانات، وقد عدل القانون بموجب القانون رقم ١١٢٥-٢٠١٨ المؤرخ في ١٢ ديسمبر ٢٠١٨، وذلك بموجب قرار البرلمان الأوربي رقم (EU 2016/680).

([2]) **ميادة مصطفي المحروقي**: المرجع السابق- ص١٤٨٩.

من بياناته الحساسة كالأصل العرقي والدين والفكر والسياسة والصحة وبياناته الانتمائية والبيومترية....إلخ.

وعليه فإن البيانات الشخصية هي كافة البيانات الخاصة بالحياة الخاصة لشخص طبيعي يمكن من خلالها التعرف على شخصيته وهويته وخصائص ذاتية له(١). أشار البعض إلى أن أهم العناصر في تعريف البيانات الشخصية هي(٢): [١] البيانات التي تؤدى إلى تحديد شخص الفرد، [٢] البيانات التى تؤدى بشكل مباشر أو غير مباشر على إمكانية التعرف على الفرد، [٣] أى بيانات أخري مستجدة تأخذ طابع البيانات الشخصية.

تتميز البيانات الشخصية بأنها حقوق لصيقة بالإنسان ومن ثم تتميز بكافة الخصاص المتعلقة بحقوق الإنسان من حيث عالميتها، وعدم جواز المساس بها. ولا تتقادم الجرائم الخاصة بها. ولا يقبل التصرف فيها أو التنازل عنها أو التصرف فيها أو نزع ملكيتها. وتمنح صاحبها الحق في الحماية الذاتية ومنع الغير من التعرض لها وطلب الحماية القانونية وفقاً لقواعد القانون، وتمكن من التعرف على الشخص وعلى هويته الاسم واللقب والجنس والسن ورقم الهاتف وعنوانه وبريده الالكتروني وكافة

(1) **Nathalie MALLET-POUJOL**: protection de la vie privée et des données à caractére personnel, étude disponible sur, la date de mise en ligne est: mai 2007, p 32.

(٢) **فهد بن عايد الشمري**: الاطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية- مجلة البحوث الفقهية والقانونية- العدد ٤٣ – أكتوبر ٢٠٢٣- ص٣٣.

البيانات الحساسة الخاصة به. كما أنها يمكن أن تتعرض أثناء المعالجة للاختراق أو المحو والابتزاز والسرقة والاضرار بالشخص المعنى.

ثانياً: أنواع البيانات الشخصية

تطورت البيانات الشخصية مع التطور التكنولوجي فلم تعد البيانات هي الاسم واللقب ورقم الهاتف والعنوان البريدى بل ازدادت وتنوعت لتشمل كل ما يمس الإنسان من بيانات وراثية وائتمانية وصورة وصوت وبيانات أسرية وحالة صحية وسلوكيات وعادات وميول وأذواق وغيرها([1])، ويمكن تقسيم البيانات الشخصية إلى عدة أقسام:

[١] بيانات شخصية غير محمية وهي التي نصت عليها المادة الثالثة من القانون ١٥١ لسنة ٢٠٢٠ حيث استثني المشرع المصري في المادة الثالثة من مواد الإصدار بعض البيانات الشخصية للشخص الطبيعي لطبيعتها، حيث نصت تلك المادة على أنه لا تسري أحكام القانون علي ما يأتي:

[١] البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي.

([1]) يشير البعض إلى أن من صور البيانات الشخصية: الاسم واللقب، الصوت والصورة، الأرقام الشخصية، العنوان، الحالة الاجتماعية، الخصائص الجسمانية، الحالة الصحية، الأصول العرقية، الجنسية، الآراء السياسية والمعتقدات الدينية، نتائج الاختبارات النفسية، البصمة، رقم الهاتف، رقم السيارة رقم الحساب البنكي، عنوان البريد الالكتروني، عنوان الكمبيوتر، وميلاد الشخص ومهنته وعنوان البريد العادى ورقم الفاكس وعلاقاته الأسرية وهواياته، ويضيف لما سبق أن كل معلومة تتعلق بصفة مباشرة أو غير مباشرة بشخص طبيعي محدد هويته أو من الممكن تحديدها هي بيان شخصي يخضع للحماية القانونية للبيانات الشخصية- **سامح عبد الواحد التهامي**: نطاق الحماية القانونية للبيانات الشخصية- مرجع سابق- ص٦٢٣ وما بعدها.

[٢] البيانات الشخصية التي تتم معالجتها بغرض الحصول علي البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني([1]).

[٣] البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخدم في أي أغراض أخري، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام([1]).

([1]) نص المشرع **بالقانون ٣٥ لسنة ١٩٦٠ بشأن الاحصاء والتعداد** والمعدل بالقانون ٢٨ لسنة ١٩٨٢ على القواعد الخاصة بالإحصاءات والتعدادات التي تحتاجها الدولة وقد أشارت **المادة الثانية** من القانون على التزام الوزارات والمصالح والهيئات العامة بالتعاون مع المكلفين بإجراء الإحصاء أو التعداد بما يكفل تأدية مهمتهم على أكمل وجه، كما أشارت الفقرة الثانية من ذات على أنه: وعلى الأفراد والهيئات أن يقدموا إلى الجهة المكلفة بالإحصاء أو التعداد جميع البيانات التى تطلب منهم بما يطابق الحقيقة وبالكيفية وفى المواعيد التى تحددها الهيئة الفنية، وعليه فهناك التزام سواء على الأشخاص الطبيعيين أو المعنويين أن يساعدوا في قيام الجهات الفنية المختصة بالإحصاءات والتعدادات بالقيام بعملها، وتنص **المادة الثالثة** على سرية البيانات الفردية التى تتعلق بأى إحصاء أو تعداد ولا يجوز إطلاع أى فرد أو هيئة عامة أو خاصة عليها أو إبلاغه شيئًا منها كما لا يجوز استخدامها لغير الأغراض الإحصائية أو نشر ما يتعلق منها بالأفراد إلا بمقتضى إذن مكتوب من ذوى الشأن. ولا يجوز استغلال أى بيان إحصائي كأساس لربط ضريبة أو لترتيب أى عبء مالى آخر ولا اتخاذه دليلًا فى جريمة أو أساسًا لأى عمل قانونى. وتنص **المادة الرابعة** على عقاب من يقوم بالأفعال الآتية: [١] كل من أخل بسرية البيانات الإحصائية أو أفشى بيانًا من البيانات الفردية أو سرًا من أسرار الصناعة أو التجارة أو غير ذلك من أساليب العمل التى يكون قد أطلع عليها بمناسبة عمله فى الإحصاء أو التعداد. [٢] كل من حصل بطريق الغش أو التهديد أو الإيهام بأية وسيلة أخرى على بيانات أو معلومات سرية بشأن الإحصاءات أو التعدادات أو شرع فى ذلك. [٣] كل من عطل عمدًا عملًا من أعمال الإحصاء أو التعداد التى تقررها الهيئة الفنية أو تسبب فى ذلك. [٤] كل من نشر إحصاءات أو تعدادات أو نتائج استقصاء غير صحيحة مع علمه بذلك. [٥] كل من امتنع عن الإدلاء بالبيانات المطلوبة أو أدلى ببيانات غير صحيحة مع علمه بذلك. ويعتبر ممتنعًا من لم يقدم البيان خلال أسبوع، من الميعاد المحدد ما لم يثبت أن التأخير فى تقديم البيانات كان بعذر مقبول.

[٤] البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوي القضائية([٢]).

[٥] البيانات الشخصية لدي جهات الأمن القومي([٣])، وما تقدره لاعتبارات أخري. ويجب علي المركز، بناءً علي طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال

([١]) نص المشرع في **المادة ٢٧ من قانون الهيئة الوطنية للصحافة رقم ١٧٩ لسنة ٢٠١٨** على أنه: يلتزم العاملون بالهيئة بالحفاظ على سرية وخصوصية المعلومات والوثائق التي يتم الحصول أو الاطلاع عليها بمناسبة القيام بمهامهم، وعدم إفشائها، أو استخدامها في غير الأغراض المخصصة لها، وتنص **المادة ٥٥ من ذات القانون** على عقاب من يخالف ذلك النص بغرامة لا تقل عن مائة ألف جنيه ولا تزيد على خمسمائة ألف جنيه، كما تنص **المادة ٨٩ من القانون ١٨٠ لسنة ٢٠١٨ بشأن تنظيم الصحافة والاعلام والمجلس الأعلى لتنظيم الاعلام على** التزام العاملون بالحفاظ على سرية المعلومات والوثائق التى يتم الحصول أو الاطلاع عليها بمناسبة القيام بمهامهم، وذلك بعدم إفشائها أو استخدامها فى غير الأغراض المخصصة لها. كما تنص المادة ٩٩ من ذات القانون على عقاب من يخالف ذلك النص بالغرامة.

([٢]) تنص **المادة ٧٥ من قانون الاجراءات الجنائية** على أنه: تعتبر إجراءات التحقيق ذاتها والنتائج التي تسفر عنها من الأسرار. ويجب على قضاة التحقيق وأعضاء النيابة العامة ومساعديهم من كتاب وخبراء وغيرهم ممن يتصلون بالتحقيق أو يحضرونه بسبب وظيفتهم أو مهنتهم عدم إفشائها، ومن يخالف ذلك منهم يعاقب طبقاً للمادة ٣١٠ من قانون العقوبات. وتنص **المادة ٣١٠ من قانون العقوبات** على أنه: كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعاً إليه بمقتضى صناعته أو وظيفته سر خصوصي ائتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مدة لا تزيد على ستة شهور أو بغرامة لا تتجاوز خمسمائة جنيه.

([٣]) عرفت **المادة الأولي من القانون ١٥١ لسنة ٢٠٢٠ جهات الأمن القومي** بأنها: رئاسة الجمهورية ووزارة الدفاع ووزارة الداخلية وجهاز المخابرات العامة وهيئة الرقابة الإدارية .

مدة زمنية محددة، وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به([1]) .

[٦] البيانات الشخصية لدي البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة، علي أن يراعي في شأنهما القواعد المقررة من البنك المركزي المصري بشأن التعامل مع البيانات الشخصية([2]).

([1]) تنص **المادة ١٢٥ من قانون هيئة الشرطة ١٠٩ لسنة ١٩٧١** المضافة بالقانون ١٧٥ لسنة ٢٠٢٠ على أن قطاع الأمن الوطني له اتخاذ عدد من الإجراءات من بينها حق طلب الاطلاع أو التحفظ على أية ملفات أو بيانات أو أوراق أو الحصول على صورة منها وذلك من الجهة الموجودة فيها هذه الملفات أو البيانات أو الأوراق بأمر قضائي مسبب. التعاون وتبادل الخبرات والمعلومات والبيانات مع جهات الأمن القومي في الدولة.

([2]) تنص **المادة ١٦ من القانون رقم ١٩٤ لسنة ٢٠٢٠ بإصدار قانون البنك المركزي والجهاز المصرفي** على أنه: ينشأ بالبنك المركزي نظام لتسجيل بيانات العملاء لإعداد الدراسات اللازمة لتعزيز الشمول المالي وتطوير الخدمات المصرفية ، وذلك طبقاً للضوابط والإجراءات التي يحددها مجلس الإدارة مع مراعاة المحافظة على سريتها، كما تنص **المادة ١٤٠ من ذات القانون** على أن جميع بيانات العملاء وحساباتهم وودائعهم وأماناتهم وخزائنهم في البنوك وكذلك المعاملات المتعلقة بها سرية ولا يجوز الاطلاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر إلا باذن كتابي من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصى لهم بكل هذه الأموال أو بعضها ، أو من نائبه القانوني أو وكيله أو بناء على حكم قضائي أو حكم تحكيم ..... ويسرى الحظر على جميع الأشخاص والجهات بما في ذلك الجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون .....، كما تنص **المادة ١٤٢ من ذات القانون** على أنه: يحظر على كل من يتلقى أاو يطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر أو غير مباشر على معلومات أو بيانات عن العملاء أو حساباتهم أو ودائعهم أو الأمانات أو الخزائن الخاصة بهم أو معاملاتهم إنشاؤها أو تمكين الغير من الاطلاع عليها وذلك في غير الحالات المرخص بها بمقتضى أحكام هذا القانون ،

ولاشك أن هناك بيانات لها حماية بطبيعتها – ولو أنها قد لا تخضع للمعالجة الالكترونية – وتستمد تلك الحماية بوصفها وصلت للشخص المسئول – بحكم وظيفته – ويعاقب إذا قام بإفشائها، حيث تنص المادة ٣١٠ عقوبات على عقاب كل من أودع لديه سر خصوصي بمقتضي صناعته أو وظيفته فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك.

ويشار إلى أن المشرع المصري قد توسع كثيراً في طائفة البيانات المستبعدة بخلاف اللائحة الأوربية([1])، ونري أن ذلك استحسان من المشرع لأن التشريع الوطني يحرص على خدمة المصلحة العامة والأمن القومي أولاً باعتبارها المصلحة الأولي بالرعاية، فيجب ألا يضيق على جهات الأمن القومي خاصة وأنها تستهدف عدم الاضرار بالشخص الطبيعي.

[٢] البيانات الشخصية المتداولة والبيانات المستعارة: تعرف البيانات الشخصية المتداولة بأنها: تلك البيانات الشخصية التي يسمح صاحبها للغير بتداولها ونشرها على وسائل التواصل الاجتماعي، وليس لها أي خصوصية بالنسبة له وليس

ويستمر هذا الحظر بعد تركهم للعمل . كما تنص **المادة ٢٣١ من ذات القانون** على عقاب من يخالف المواد السابقة بالحبس والغرامة، وتتعدد الغرامات بتعدد المجنى عليهم .

([1]) اعتبرت المحكمة الأوربية قرار السلطات الضريبية في النرويج بمطالبة الشركات بتزويد مراجعي الضرائب ببيانات محفوظة لديها اخلال بالمادة الثامنة من الاتفاقية الأوربية.

ECtHR, Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013. See also, however, ECtHR, Liberty and Others v. the United Kingdom, No. 58243/00, 1 July 2008.

من شأن استغلالها إحداث أي ضرر به. أما البيانات الشخصية المستعارة فهي تلك البيانات الشخصية مجهولة المصدر حيث يقوم صاحبها بوضع بيانات عامة مثل (السيدة العجوز) أو (صاحب البشرة السمراء) أو (بنت الشاطئ) فلا يستدل عليه، وقد وضعت اللائحة الأوربية تعريف خاص بالتسمية المستعارة وهي([1]): تلك البيانات التي لا تدخل تحت مسمي شخص محدد وعرفتها بأنها معالجة البيانات الشخصية بطريقة لا يمكن بعدها ربط البيانات الشخصية بشخص محدد هو موضوع تلك البيانات من دون استخدام معلومات إضافية شريطة الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل وأن تخضع تلك البيانات الإضافية لتدابير تقنية وتنظيمية لضمان عدم انتسابها لشخص طبيعي معرف أو قابل للتعريف.

[٣] البيانات الشخصية المحمية(الحساسة) : هي بيانات ذات طابع شخصي مثل البيانات الخاصة بصحة الشخص وحالته الجسدية والنفسية وعلاقاته الأسرية، وتتميز البيانات الشخصية الحساسة عن المتداولة أن الأولي من شأن سوء استخدامها الاضرار الجسيم بالشخص ولا يجوز معالجتها إلا بعد الرجوع لصاحبها أو المسئول عنه. وقد عرفت المادة الأولي من القانون ١٥١ لسنة ٢٠٢٠ **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

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة.

عرفت المادة الأولي من القانون الاماراتي رقم ٤٥ لسنة ٢٠٢١ البيانات الشخصية الحساسة بأنها: أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة الشخص الطبيعي أو أصله العرقي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية له التي تكشف عن وضعه الصحي.

عرفت المادة الثالثة من القانون الجزائري رقم (٠٧-١٨) البيانات الحساسة بأنها: معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية.

عرفت المادة ١١/١ من نظام حماية البيانات الشخصية السعودى البيانات الحساسة بأنها: كل بيان شخصي يتعلق بأصل الفرد العرقي أو أصله الإثني، أو معتقده الديني أو الفكري أو السياسي. وكذلك البيانات الأمنية والجنائية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الصحية، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما".

تعرف البيانات الحيوية البيومترية بأنها([1]): البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات، والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات، مثل صورة الوجه أو بيانات البصمة، أي هي تلك البيانات التي تتعلق بجسد الإنسان([2]). بينما تركت اللائحة الأوربية لدول الاتحاد وضع الحماية المناسبة لاستخدام البيانات الحساسة(وفقاً لظروف كل دولة)، ولكن عرفت في المادة ١٣/٤ من اللائحة البيانات الجينية بأنها([3]): البيانات الشخصية المتعلقة بالخصائص الجينية الوراثية أو المكتسبة لشخص طبيعي والتي توفر معلومات فريدة عن الحالة الفسيولوجية أو الحالة الصحية لذلك الشخص الطبيعي والتي تنتج، على وجه الخصوص، من تحليل عينة بيولوجية من الطبيعي الشخص المعني، وكانت ديباجة

([1]) لم يضع المشرع المصري تعريفاً لما يسمي بالبيانات البيومترية أو البيانات الجينية أو البيانات المتعلقة بالصحة، ونري أنه قد تركها للائحة التنفيذية للقانون أو أنه تغاضي عنها باعتبار أنها تدخل في البيانات الحساسة أو أنه قد تركها للفقه والقضاء حتى لا يكون تحديده لها من شأنه اغفال نوع من تلك البيانات.

([2]) **جمالي أبو هشيمة كامل:** حماية البيانات الشخصية في البيئة الرقمية- بحث مقدم إلى مؤتمر العصر الرقمي واشكالياته القانونية- كلية الحقوق جامعة أسيوط- الفترة من ١٢-٢٠١٦/٤/١٣ ص٤.

([3]) «données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

اللائحة قد نصت على أنه من بين تلك البيانات تحليل الكروموسومات (DNA) و حمض (RNA)، أو تحليل أي عنصر آخر، كما عرفت البيانات البيومترية بأنها([1]): البيانات الشخصية الناتجة عن معالجة تقنية محددة، تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية للشخص الطبيعي، والتي تمكن أو تؤكد تحديد هويته الفريدة، مثل صور الوجه أو بيانات بصمات الأصابع. كما عرفت البيانات الصحية بأنها([2]): البيانات الشخصية المتعلقة بالصحة الجسدية أو العقلية للشخص الطبيعي، بما في ذلك توفير خدمات الرعاية الصحية، والتي تكشف معلومات حول الحالة الصحية لذلك الشخص الطبيعي([3]). وقد حظر المشرع الفرنسي معالجة البيانات الشخصية المتعلقة بالأصل العنصري أو الإثني المزعوم أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية. كما حظر معالجة البيانات الجينية أو البيانات

([1]) «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

([2]) «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

([3]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

البيومترية لأغراض تحديد هوية الشخص الطبيعي بشكل فريد أو البيانات المتعلقة بالصحة أو البيانات المتعلقة بالحياة الجنسية أو التوجه الجنسي للشخص. بالنسبة للقاصرين الذين تقل أعمارهم عن خمسة عشر عامًا، واشترط موافقة أصحاب السلطة الأبوية لمعالجة البيانات الشخصية على الشبكات الاجتماعية.

المبحث الأول

معالجة البيانات الشخصية

مقدمة:

أشار المشرع المصري والتشريعات المقارنة واللائحة الأوربية لحماية البيانات إلى معالجة البيانات، وأشارت الديباجة الخاصة باللائحة الأوربية إلى أنه يجب أن تكون معالجة البيانات الشخصية مصممة لخدمة الإنسانية. فالحق في حماية البيانات الشخصية ليس حقًا مطلقًا؛ ويجب النظر إليها فيما يتعلق بوظيفتها في المجتمع ومقارنتها بالحقوق الأساسية الأخرى، ووفقا لمبدأ التناسب، حيث تشير اللائحة إلى احترام كافة الحقوق الأساسية والحريات والمبادئ التي يعترف بها الميثاق الأوربي والمنصوص عليها في المعاهدات، ولاسيما احترام الحياة الخاصة والعائلية، والمنزل والاتصالات، وحماية البيانات الشخصية، وحرية الفكر والضمير والدين، وحرية التعبير عن الرأي، وحرية الأعمال، والحق في الانتصاف الفعال.

تعرف المعالجة بأنها مجموعة من العمليات سواء تم تنفيذها بطريقة آلية أو غير آلية ويتم تطبيقها على المعلومات الشخصية لشخص محدد أو مجموعة من البيانات مثل التجميع والنقل والتسجيل والحفظ والتعديل والاستخدام والنشر والاتاحة، وتهدف عمليات المعالجة إلى القيام بأعمال محددة صريحة ومشروعة لحماية المصالح الحيوية لصاحب البيانات أو للمصلحة العامة أو لأغراض البحث العلمي لفترة محددة من الزمن على أن تتم المعالجة بطريقة آمنة ومحمية وبموافقة الشخص

المعني من الحماية، وتشمل المعالجة أية إجراءات متعلقة بالبيانات بغض النظر عن الطريقة التي استخدمت في هذا الاجراء، فأى إجراء يتم اتخاذه ويتعلق بالبيانات الشخصية يعتبر معالجة لهذه البيانات([1]). وتتم المعالجة وفقاً لضوابط محددة حتى لا تخرج عن الغرض المستهدف منها، وسوف نتناول في هذا المبحث ماهية معالجة البيانات الشخصية وضوابط معالجة تلك البيانات وذلك على النحو التالي:

المطلب الأول: ماهية معالجة البيانات الشخصية

المطلب الثاني: ضوابط معالجة البيانات الشخصية

([1]) **الدراسة النقدية** السابق الإشارة إليها- ص٣٩.

المطلب الأول

ماهية معالجة البيانات الشخصية

تعرف معالجة البيانات بأنها: نشاط تقني أفرزه التطور التكنولوجي فهو عملية فنية معقدة تمر بسلسلة من المراحل([1])، حيث تتعرض البيانات الشخصية لعدد من المراحل أو العمليات تتناسب مع طبيعتها فيما يسمي بالمعالجة، وتعرف تلك المعالجة بأنها إجراء أو أكثر يتعلق بالبيانات الشخصية أيا كانت الطريقة المستخدمة في هذا الاجراء سواء كان التجميع أو التسجيل أو التنظيم أو الحفظ أو التعديل أو الاستخلاص أو الاطلاع أو الاستخدام أو الإبلاغ بطريق النقل أو النشر أو الربط أو المنع أو المحو أو التدمير. عرفت المادة الأولي من القانون ١٥١ لسنة ٢٠٢٠ **المعالجة** بأنها: أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية أو تجميعها أو تسجيلها أو حفظها أو تخزينها أو دمجها أو عرضها أو إرسالها أو استقبالها أو تداولها أو نشرها أو محوها أو تغييرها أو تعديلها أو استرجاعها أو تحليلها؛ وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئياً أو كلياً.

([1]) **عمرو طه بدوى**: التنظيم القانوني لمعالجة البيانات الشخصية: دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية- دار النهضة العربية- القاهرة- ٢٠٢٠- ص٣٥ حيث يشير إلى أن معالجة البيانات تمر بثلاث مراحل هي إدخال البيانات ثم مرحلة المعالجة ثم مرحلة إخراج النتائج.

وباستعراض ذلك التعريف يتضح لنا الآتي:

[١] المشرع حدد عمليات معالجة محددة تجري على البيانات الشخصية وهي الكتابة والتجميع والتسجيل والحفظ والتخزين والدمج والعرض والارسال والاستقبال والتداول والنشر والمحو والتغيير والتعديل والاسترجاع والتحليل وهو ذكر على سبيل الحصر وليس على سبيل المثال وكان من المفروض على المشرع أن يضيف وأى عمليات أخرى لأنه قد تسفر التقنيات الحديثة عن ظهور عمليات معالجة أخرى، أو أن يقول في بداية التعريف أي عملية ومنها ويسرد تلك العمليات.

[٢] لم يتطرق المشرع لتعريف كل نوع من العمليات التي أشار إليها ونري أن المشرع قد ترك ذلك للائحة التنفيذية، أو أنه ترك ذلك للجان الفنية التي يشكلها القاضي حتى توضح نوع العملية التقنية التي استخدمها المخالف.

[٣] أحسن المشرع عندما ذكر باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية بحيث لا يتطلب ذلك وسيط معين. كما أنه ذكر جزئيا أو كليا بحيث ينطبق القانون على معالجة جزء من البيانات الشخصية أو كلها.

عرفت اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوربي بالقرار رقم (2016/679)"المعالجة" بأنها([1]): تعني أي عملية أو مجموعة من العمليات يتم إجراؤها على البيانات الشخصية أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أم لا، مثل التجميع أو التسجيل أو التنظيم أو الهيكلة أو

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

التخزين أو التكيف أو التغيير أو الاسترجاع أو الاستشارة أو الاستخدام أو الكشف عن طريق النقل أو النشر أو الإتاحة بطريقة أخرى أو المواءمة أو الجمع أو التقييد أو المحو أو التدمير([1])، كما عرفت المادة الثالثة من القانون الجزائري رقم (٠٧-١٨) المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي **معالجة المعطيات ذات الطابع الشخصي** بأنها: كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الايصال عن طريق الارسال أو النشر أو أى شكل آخر من أشكال الاتاحة أو التقريب أو الربط البيني وكذا الاغلاق أو التشفير أو المسح أو الاتلاف.

عرفت المادة ٥/١ من نظام حماية البيانات الشخصية السعودى المُعالجة: أي عملية تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر،

([1]) راجع في ذلك تلك التعريفات باللائحة الأوربية:

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف. كما عرفها المشرع القطري في المادة الأولي بأنها إجراء عملية أو مجموعة عمليات على البيانات الشخصية كالجمع والاستلام والتسجيل والتنظيم والتخزين والتهيئة والتعديل والاسترجاع والاستخدام والافشاء والنشر والنقل والحجب والتخلص والمحو والالغاء.

وقد أحسن المشرع السعودى عن المشرع المصري عندما أقر بحماية المعالجة اليدوية، وكان يجب أن يضعها المشرع المصري في تعريفه، فالمعالجة اليدوية يقصد بها وضع البيانات الشخصية في ملفات ورقية عادية دون أن تتم معالجتها بوسائل تقنية ودون الاستعانة ببرامج آلية والكترونية(١). ونري أن معالجة البيانات الشخصية هي عملية أو أكثر تنجز بطريقة آلية أو يدوية وتتخذ عدد من الأشكال كالتجميع والتنظيم والتسجيل والحفظ والتخزين والعرض والارسال والاستقبال والتداول والنشر والتعديل والاسترجاع والتحليل وغير ذلك بما يسهل للغير بالنفاذ إليها.

(١) راجع في ذلك: **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية – المرجع السابق– ص٤١٢.

Baffard WILLIAM: Le système de traitement des infractions constatées personnelles ،mémoire de DEA informatique et droit ، faculté de droit université de Montpellier I , 2003, p 16.

المطلب الثاني

ضوابط معالجة البيانات الشخصية

تحدد التشريعات الضوابط الخاصة باستخدام البيانات الشخصية، ومن شأن هذه الضوابط أن تضع ضمان للشخص المعني بالبيانات من عدم الإساءة لبياناته الشخصية. وكان القانون ١٥١ لسنة ٢٠٢٠ قد نص في أكثر من موضع على إحالة بعض نصوصه لتنظيمها من خلال اللائحة التنفيذية إلا أن اللائحة لم تصدر حتى الآن. حيث يتم تحديد أغراض المعالجة في هذا الأساس القانوني أو تكون ضرورية لأداء مهمة يتم تنفيذها للمصلحة العامة أو تتعلق بممارسة السلطة العامة المسؤول عن المعالجة. لذا يجب تحديد الشروط العامة التي تحكم مشروعية المعالجة من قبل الشخص القائم بالمعالجة وتحديد البيانات التي تخضع للمعالجة والأشخاص المعنيين والكيانات التي قد يتم إرسال البيانات الشخصية إليها والأغراض التي يمكن إرسالها من أجلها وتقييد الأغراض وفترات الاحتفاظ وعمليات وإجراءات المعالجة، بما في ذلك التدابير اللازمة لضمان المعالجة القانونية والعادلة، وذلك بهدف حماية الشخص المعني وتحقيق المصلحة العامة وبما يتناسب مع الهدف المشروع المنشود. مع وضع ضمانات محددة حتى لا يخرج القائم بالمعالجة عن الحدود والقواعد الخاصة بذلك.

حدد القانون ١٥١ لسنة ٢٠٢٠ في المادة الثالثة تلك الضوابط أو الشروط، حيث نصت المادة الثالثة على أنه: يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية:

[١] أن تجمع 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 لدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها

.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات.

كما نصت اللائحة الأوربية في المادة الخامسة على المبادئ المتعلقة بمعالجة البيانات الشخصية (Principes relatifs au traitement des données à caractère personnel) وتضمنت الآتي: يجب أن تكون معالجة البيانات الشخصية([1]) على النحو التالي: [أ] معالجتها بطريقة قانونية وعادلة وشفافة فيما يتعلق بموضوع البيانات (الشرعية والولاء والشفافية- licéité, loyauté, transparence)؛ [ب] يتم جمعها لأغراض محددة وصريحة ومشروعة، ولم تتم معالجتها لاحقًا بطريقة لا تتوافق مع تلك الأغراض؛ لا تعتبر المعالجة الإضافية لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية، وفقًا للمادة ٨٩(١)، غير متوافقة مع الأغراض الأصلية

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

(أغراض التقييد– limitation des finalités)؛ [ج] كافية وذات صلة ومحدودة بما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجلها (تقليل البيانات– minimisation des données)؛ [د] دقيقة وحديثة عند الضرورة؛ يجب اتخاذ جميع التدابير المعقولة لضمان مسح أو تصحيح البيانات الشخصية غير الدقيقة، مع مراعاة الأغراض التي تتم معالجتها من أجلها، دون تأخير (الدقة– exactitude)؛ [هـ] يتم الاحتفاظ بها في نموذج يسمح بتحديد أصحاب البيانات لفترة لا تتجاوز الفترة اللازمة للأغراض التي تتم معالجتها من أجلها؛ يجوز الاحتفاظ بالبيانات الشخصية لفترات أطول إلى الحد الذي ستتم معالجته حصريًا لأغراض الأرشفة للمصلحة العامة، أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية وفقًا للمادة ٨٩، الفقرة ١، بشرط توفر الإجراءات الفنية والتقنية المناسبة يتم تنفيذ التدابير التنظيمية التي تتطلبها هذه اللائحة من أجل ضمان حقوق وحريات صاحب البيانات (تقييد الاحتفاظ– limitation de la conservation)؛ [و] معالجتها بطريقة تضمن الأمان المناسب للبيانات الشخصية، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقدان العرضي أو التدمير أو الضرر، باستخدام التدابير الفنية أو التنظيمية المناسبة (النزاهة والسرية– intégrité et confidentialité)؛ تحدد التشريعات المعنية بحماية البيانات الشخصية الضمانات القانونية التي ينبغي أن تتم في إطارها معالجة البيانات الشخصية، حيث وضعت التشريعات سابقة على معالجة البيانات، وضمانات لاحقة على إجراء المعالجة.

ويمكن أن نستخلص من ذلك الضوابط الآتية([1]):

[١] الضوابط السابقة على المعالجة:

[أ] الترخيص بمزاولة نشاط معالجة البيانات الشخصية

حتى يمكن لأي جهة القيام بمعالجة البيانات الشخصية فعليها أن تتخذ الخطوات والإجراءات التي نصت عليها المادة العاشرة من القانون ١٥١ لسنة ٢٠٢٠

([1]) أشار دليل الاتحاد الأوربي بشأن حماية البيانات الشخصية إلى ضوابط المعالجة وهي:

The principles of lawfulness, fairness and transparency apply to all personal data processing.

•Under the GDPR, lawfulness requires either: 1- consent of the data subject؛ 2- necessity to enter a contract؛ 3- a legal obligation؛ 4- necessity to protect the vital interests of the data subject or of another person؛ 5- necessity for performing a task in the public interest؛ 6- necessity for the legitimate interests of the controller or a third party, if they are not overridden by the interests and rights of the data subject. 7- Personal data processing should be done in a fair manner. 8- The data subject must be informed of the risk to ensure that processing does not have unforeseeable negative effects. 9- Personal data processing should be done in a transparent manner. 10- Controllers must inform data subjects before processing their data, among other details, about the purpose of processing and about the identity and address of the controller. 11- Information on processing operations must be provided in clear and plain language to allow data subjects to easily understand the rules, risks, safeguards and rights involved. 12- Data subjects have the right to access their data wherever they are processed.

راجع في ذلك - Handbook on European, data protection law, 2018 edition

والتي نصت علي أنه: يلتزم كل من المتحكم والمعالج والحائز عند طلب إتاحة البيانات الشخصية بالإجراءات الآتية: [١] أن يكون بناءً علي طلب كتابي يقدم إليه من ذي صفة أو وفقًا لسند قانوني، [٢] التحقق من توافر المستندات اللازمة لتنفيذ الإتاحة والاحتفاظ بها،[٣] البت في الطلب ومستنداته خلال ستة أيام عمل من تاريخ تقديمه إليه. وعند صدور قرار بالرفض يجب أن يكون الرفض مسببًا، ويعتبر مضي المدة المشار إليها دون رد في حكم الرفض. وعليه فإن المشرع قد نص على طريقة التقدم للحصول على الترخيص الخاص بمزاولة مهنة المتحكم أو المعالج.

عرفت المادة الأولي من القانون ١٥١ لسنة ٢٠٢٠ **الترخيص** بأنه وثيقة رسمية تصدر عن المركز للشخص الطبيعي تمنحه من خلالها الحق في مزاولة نشاط جمع البيانات الشخصية الالكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الالكتروني أو كل ما سبق والتعامل عليها بأى صورة وتحدد التزامات المرخص له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية لهذا القانون وذلك لمدة ثلاث سنوات قابلة للتجديد.

كما عرفت **التصريح** بأنه: وثيقة رسمية تصدر عن المركز للشخص الطبيعي أو الاعتباري تمنحه من خلالها الحق في ممارسة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الإلكتروني أو كل ما سبق والتعامل عليها بأي صورة، أو لأداء مهمة أو مهام معينة، وتحدد هذه الوثيقة التزامات المصرح له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية، لمدة مؤقتة لا تجاوز سنة، ويجوز تجديدها لأكثر من مدة.

كما عرفت **الاعتماد** بأنه: شهادة تصدر عن المركز تفيد أن الشخص الطبيعي أو الاعتباري قد استوفي جميع المتطلبات الفنية والقانونية والتنظيمية المحددة باللائحة التنفيذية لهذا القانون ويكون بموجبها مؤهلاً لتقديم الاستشارات في مجال حماية البيانات الشخصية . ويشير إليها البعض بشهادة الامتثال([1]) وهي شهادة الامتثال للمنظمات الشاملة في مجال إدارة البيانات وحوكمتها وحماية البيانات الشخصية هي شهادة تؤكد على فهم وتطبيق المعايير والإرشادات المنظمة في هذه المجالات. والحصول على هذه الشهادة يوفر إثباتًا للمنظمات أن نظم إدارة البيانات وحوكمة البيانات وحماية البيانات تتماشى مع المعايير والمتطلبات التنظيمية المعترف بها. وهذا يعزز الثقة في المنظمة ويساعدها على تجنب المخاطر التنظيمية والقانونية، وتغطي هذه الشهادة الامتثال لحوكمة البيانات، الامتثال للوائح إدارة البيانات، الامتثال لحماية البيانات الشخصية.

والحقيقة أن المشرع لم يوضح الفرق بين الترخيص والتصريح لذا نري أنه يجب أن يوضح ذلك في اللائحة التنفيذية، ومن المعروف أن الترخيص يكون لشخص اعتباري استوفي كافة التجهيزات والاشتراطات الفنية التي يتطلبها الترخيص بممارسة نشاط معالجة البيانات الشخصية والتي يتطلبها كمركز حماية البيانات الشخصية، أما التصريح فيكون لشخص طبيعي أو معنوى ويكون ممارسة النشاط بطريقة مبسطة مع

([1]) راجع في ذلك (Data Management Association and Decision Support Systems Research، جمعية إدارة البيانات وأبحاث أنظمة دعم القرار في المملكة العربية السعودية) موقع هذه الجمعية على شبكة الانترنت www.dmasaudi.org

الالتزامات والتجهيزات الفنية والاشتراطات المحددة من قبل المركز والتي تكون أقل بكثير مما يطلب من أصحاب الترخيص.

أما الفرق بين المتحكم والمعالج فقد نص القانون ١٥١ لسنة ٢٠٢٠ على وضع تعريف لكل منهما حيث عرف **المتحكم** بأنه: أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله الحق في الحصول علي البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها أو معالجتها والتحكم فيها طبقًا للغرض المحدد أو نشاطه. كما عرف **المعالج** بأنه: أي شخص طبيعي أو اعتباري مختص بطبيعة عمله بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته، حيث أشار البعض إلى أمثلة لذلك منها أن مزود الخدمة بمقتضي عقد بينه وبين الشخص المعني بالبيانات هو شركة الكهرباء والتي تعتبر في هذه الحالة متحكم بالبيانات بينما معالجة البيانات لاستخراج الفواتير لا يكون من قبل نفس الشركة في مصر وإنما من قبل شركة أخرى وتعد هذه الأخيرة في تلك الحالة معالجا للبيانات فقط دون أن تكون متحكمة بها([1]).

وقد حدد القانون رقم ١٥١ لسنة ٢٠٢٠، بإصدار قانون حماية البيانات الشخصية، أنواع التراخيص والتصاريح والاعتمادات التي يصدرها مركز حماية

([1]) **الدراسة النقدية** السابق الإشارة إليها– ص٣٩.

البيانات الشخصية([1])، وفى هذا الصدد، تنص المادة رقم (٢٦) على أن يقوم المركز بتصنيف التراخيص والتصاريح والاعتمادات وتحديد أنواعها، ووضع الشروط الخاصة بمنح كل نوع منها، وذلك وفقًا لما تحدده اللائحة التنفيذية لهذا القانون، ويصدر المركز التراخيص أو التصاريح أو الاعتمادات على النحو الآتى: [١] إصدار الترخيص أو التصريح للمتحكم أو المعالج لإجراء عمليات حفظ البيانات، والتعامل عليها ومعالجتها وفقًا لأحكام هذا القانون، [٢] إصدار التراخيص أو التصاريح الخاصة بالتسويق الإلكترونى المباشر، [٣] إصدار التراخيص أو التصاريح الخاصة بالمعالجات التى تقوم بها الجمعيات أو النقابات أو النوادى للبيانات الشخصية لأعضاء تلك الجهات وفى إطار أنشطتها، [٤] إصدار التراخيص أو التصاريح الخاصة بوسائل المراقبة البصرية فى الأماكن العامة، [٥] إصدار التراخيص أو التصاريح الخاصة بالتحكم ومعالجة البيانات الشخصية الحساسة، [٦] إصدار التصاريح والاعتمادات الخاصة بالجهات والأفراد التى تتيح لهم تقديم الاستشارات فى إجراءات حماية البيانات الشخصية ، وإجراءات الامتثال لها، [٧] إصدار التراخيص والتصاريح الخاصة بنقل البيانات الشخصية عبر الحدود.

وتحدد اللائحة التنفيذية لهذا القانون أنواع هذه التراخيص والتصاريح والاعتمادات وفئاتها ومستوياتها، وإجراءات وشروط إصدارها وتجديدها ونماذجها

([1]) أشار الدليل الأوربي بشأن حماية البيانات إلى ضرورة وجود هيئات اشرافية مستقلة من جانب الدول ينص عليها القانون الوطني والمنصوص عليها في المادة الثامنة من اللائحة على أن تعمل باستقلالية تامة.

المستخدمة، وذلك بمقابل رسوم لا تتجاوز مليونى جنيه بالنسبة للترخيص، ومبلغ لا يتجاوز خمسمائة ألف جنيه للتصريح أو الاعتماد.

[ب] الالتزام بالمبادئ الأساسية المتعلقة بمعالجة البيانات الشخصية:

حددت لائحة البيانات الأوربية وتوافق معها القانون ١٥١ لسنة ٢٠٢٠ في بعض منها على مبادئ تتعلق بمعالجة البيانات الشخصية يجب أن يلتزم بها المعالج قبل جمع البيانات، وهذه المبادئ هي المفتاح الحقيقي والفعال لإقامة نظام صحيح لمعالجة البيانات الشخصية وهذه المبادئ هي([1]):

[١] **مبدأ الأمانة**: يجب أن تعالج البيانات بطريقة سليمة ومشروعة ومتوافقة مع الغرض التي تتم من أجله، وأن تكون البيانات المعالجة ذات صلة بموضوع المعالجة.

[٢] **مبدأ الدقة**: يجب أن تتم المعالجة بطريقة دقيقة وأن يتخذ المعالج كافة الخطوات الصحيحة أثناء المعالجة.

([1]) قضت محكمة العدل الأوربية بضرورة التزام الدول في تشريعاتها بالمبادئ الستة الخاصة بمعالجة البيانات الشخصية وأضافت أنه: "لا يمكن للدول الأعضاء إضافة مبادئ جديدة تتعلق بمشروعية معالجة البيانات الشخصية إلى المادة ٧ من التوجيه (٤٦٤١١/٩٥) أو فرض متطلبات إضافية من شأنها تعديل نطاق أحد المبادئ الستة المنصوص عليها"

CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, paras. 40, 44 and 48-49

[٣] **مبدأ رضاء الشخص المعني**: يجب التأكد من الرضاء الصريح والمكتوب من الشخص المعني قبل المعالجة([١])، وأن يستمر ذلك الرضاء حتى انتهاء المعالجة، ورد البيانات للشخص المعني ومحوها.

[٤] **مبدأ الأمان والسرية**: يجب أن يتم الاحتفاظ بالبيانات بطريقة سليمة وآمنة ومنع تعرض الغير لها ومحاولة انتهاكها أو تدميرها، مع اتخاذ كافة التدابير التقنية والتنظيمية المناسبة، فيجب أن توفر طرق المعالجة من الوسائل التقنية ما يكفل أمن البيانات([٢]). وكان التوجيه الأوربي بشأن الخصوصية الإلكترونية EC/58/2002 المعدل في ٢٠٠٩ قد نص على ضمان تنفيذ سياسة أمنية فيما يتعلق بمعالجة البيانات الشخصية وبالتالي فيما يتعلق بإحكام الأمن والالتزام بإدخال شرط صريح بشأن امتلاك سياسة أمنية وتنفيذها([٣]).

([١]) **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية – المرجع السابق– ص٤١٢.

([٢]) عرفت المادة الأولي من القانون ١٥١ لسنة ٢٠٢٠ أمن البيانات بأنه: إجراءات وعمليات تقنية وتنظيمية من شأنها الحفاظ علي خصوصية البيانات الشخصية وسريتها وسلامتها ووحدتها وتكاملها فيما بينها .

أشار الدليل الأوربي لحماية البيانات إلى أن أمن البيانات الشخصية وسريتها أمران أساسيان لمنع التأثيرات السلبية على صاحب البيانات: [١] يمكن أن تكون التدابير الأمنية ذات طبيعة فنية و/أو تنظيمية. [٢] إخفاء الهوية هو عملية يمكنها حماية البيانات الشخصية. [٣] يجب تحديد مدى ملاءمة التدابير الأمنية على أساس كل حالة على حدة ومراجعتها بانتظام.

Handbook on European, data protection law, 2018 edition

وقد أشار الدليل الأوربي إلى أنه لا يجوز قيام موظف في شركة تأمين بالإدلاء بمعلومات من خلال مكالمة هاتفية من شخص يدعي أنه عميل ويطلب الحصول على معلومات متعلقة بعقد التأمين الخاص به لأن هذا يخالف الحد الأدني من تدابير الأمن.

([٣]) مشار إليه بالجريدة الرسمية الأوربية (L337–2009) – ص١١

[٥] **مبدأ توقيت الحفظ:** يجب تأقيت مدة الحفظ بحيث لا تزيد عن المدة المحددة للمعالجة وينتهي بعدها الحفظ، وتحذف أو تمحي بناء على طلب الشخص المعني.

[٦] **مبدأ الالتزام بالإخطار:** يتعلق هذا المبدأ بضرورة إبلاغ الشخص المعني في حالة حدوث انتهاك للبيانات واختراقها من جانب الغير، فذلك من شأنه تهديد المصالح الخاصة له، وهذا ما نص عليه المشرع في المادة السابعة من القانون ١٥١ لسنة ٢٠٢٠([1])، ما أكدته المادة ٣٤ من اللائحة الأوربية([2]). وقد وضع المشرع

([1]) تنص المادة السابعة على أنه: يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ المركز خلال اثنتين وسبعين ساعة ، وفي حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فوريا ، وعلي المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فورًا ، كما يلتزم بموافاة المركز خلال اثنتين وسبعين ساعة من تاريخ علمه بما يأتي: [١] وصف طبيعة الخرق أو الانتهاك ، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها، [٢] بيانات مسئول حماية البيانات الشخصية لديه، [٣] الآثار المحتملة لحادث الخرق أو الانتهاك، [٤] وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية، [٥] توثيق أي خرق أو انتهاك للبيانات الشخصية والإجراءات التصحيحية المتخذة لمواجهته، [٦] أي وثائق أو معلومات أو بيانات يطلبها المركز. وفي جميع الأحوال يجب علي المتحكم والمعالج، بحسب الأحوال، إخطار الشخص المعني بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات. وتحدد اللائحة التنفيذية لهذا القانون الإجراءات الخاصة بالإبلاغ والإخطار.

([2]) تنص المادة ٣٤ من اللائحة الأوربية على أنه:[١] عندما يكون من المحتمل أن يؤدي خرق البيانات الشخصية إلى خطر كبير على حقوق وحريات الشخص الطبيعي، يجب على المراقب إبلاغ خرق البيانات الشخصية إلى صاحب البيانات دون تأخير لا مبرر له. [٢] يصف التواصل مع صاحب البيانات المشار إليه في الفقرة ١ من هذه المادة، بعبارات واضحة وبسيطة، طبيعة خرق البيانات الشخصية ويحتوي على الأقل على المعلومات والتدابير المشار إليها في المادة ٣٣ (٣)،

المصري التزام على المتحكم في المادة الرابعة باتخاذ كافة الإجراءات التقنية والتنظيمية اختراق البيانات الشخصية أو اتلافها أو تغييرها أو العبث فيها.

[٧] **مبدأ المساءلة**: يجب أن يعلم المعالج أنه سوف يتعرض للمساءلة القانونية سواء الجنائية أو المدنية، ومنعه من ممارسة هذا النشاط لاحقا إذا تسبب في الاضرار بحقوق الشخص المعنى(١).

النقاط (ب)، (ج) و (د). [٣] لا يعد التواصل مع صاحب البيانات المشار إليه في الفقرة ١ ضروريًا في حالة استيفاء أي من الشروط التالية: [أ] نفذت وحدة التحكم تدابير الحماية الفنية والتنظيمية المناسبة وتم تطبيق هذه التدابير على البيانات الشخصية المتأثرة بالانتهاك المذكور، ولا سيما التدابير التي تجعل البيانات الشخصية غير مفهومة لأي شخص غير مصرح له بالوصول إليها، مثل التشفير؛ [ب] اتخذ المراقب تدابير لاحقة تضمن أنه من غير المحتمل أن تتحقق المخاطر العالية على حقوق وحريات أصحاب البيانات المشار إليها في الفقرة ١؛ [ج] سيتطلب جهداً غير متناسب. وفي هذه الحالة، يتم بدلاً من ذلك إجراء اتصالات عامة أو إجراء مماثل لتمكين المتضررين من إبلاغهم بطريقة فعالة بنفس القدر. [٤] إذا لم تكن وحدة التحكم قد أبلغت بالفعل صاحب البيانات بخرق البيانات الشخصية المتعلقة به أو بها، يجوز للسلطة الإشرافية، بعد فحص ما إذا كان خرق البيانات الشخصية هذا من المحتمل أن يؤدي إلى مخاطر عالية، أن تطلب من وحدة التحكم إجراء هذا الاتصال أو تقرر استيفاء واحد أو أكثر من الشروط المشار إليها في الفقرة ٣.

(١) راجع في ذلك- **تامر محمد الدمياطي**: الرضاء الرقمي بمعالجة البيانات الشخصية- مجلة القانون والتكنولوجيا كلية القانون الجامعة البريطانية بالقاهرة- مج٢- ع١- ابريل ٢٠٢٢- ص٧٤، **الصالحين محمد العيش**: حماية البيانات الشخصية في القانون الأوربي: مجلة كلية القانون الكويتية العالمية- س١١-ع٣-يونيو ٢٠٢٣- ص٣٠٦ وما بعدها.

قضت محكمة العدل الأوربية عن مسائلة شركة قامت بأخذ البيانات الشخصية لشخص وتقديمها لشركة أخري تعمل في العقارات.

CJEU, C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 11 December 2014, para. 25.

[٨] **مبدأ الشفافية وإعلام الجمهور:** يجب إعلام أصحاب الشأن بكيفية استخدام بياناتهم بشفافية وهذا مبدأ عام أشارت إليه اللائحة الأوربية لحماية البيانات(١)، فلا يكفي رضاء الشخص بمعالجة بياناته بل يجب قبوله لكيفية المعالجة، ويقصد بذلك إحاطته علما بسبب جمع بياناته وكيفية معالجتها(٢)، ويجب أن يكون العلم بشفافية ومحدد وينصب على عمليات المعالجة، فيجب أن يتم إعلام الشخص المعني بالبيانات بما سوف يتم وأن تكون هناك موافقة مسبقة من الشخص المعنى على جمع بياناته ومعالجتها. كما أكدت منظمة التعاون الاقتصادي والتنمية بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود لعام ٢٠١٣ على بعض مبادي الخصوصية وحماية البيانات(٣).

---

(١) راجع في ذلك:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

حيث تشير الديباجة الخاصة باللائحة الأوربية إلى أن مبدأ الشفافية يتطلب أن تكون أي معلومات موجهة إلى الجمهور أو الشخص المعني موجزة، ويسهل الوصول إليها، وسهلة الفهم، ومصاغة بعبارات واضحة وبسيطة، بالإضافة إلى توضيحها بمساعدة العناصر المرئية.

(٢) **فهد بن عايد الشمري:** المرجع السابق ص١٦٥٨.

(٣) وهذه المبادئ هي: [١] **مبدأ تقييد التحصيل** ويعني أنه يجب أن تكون هناك قيود على جمع البيانات الشخصية ويجب الحصول على أي من هذه البيانات بوسائل قانونية وعادلة، وعند الاقتضاء، بمعرفة أو موافقة صاحب البيانات. [٢] **مبدأ جودة البيانات** ويعني أنه يجب أن تكون البيانات الشخصية ذات صلة بالأغراض التي سيتم استخدامها من أجلها، ويجب أن تكون دقيقة وكاملة ومحدثة بالقدر اللازم لتلك الأغراض. [٣] **مبدأ مواصفات الغرض** ويعني يجب تحديد الأغراض التي يتم جمع البيانات الشخصية من أجلها في موعد لا يتجاوز وقت جمع البيانات والاستخدام اللاحق يقتصر على تحقيق تلك الأغراض أو غيرها من الأغراض التي لا تتعارض مع

[ج] موافقة الشخص المعني بالبيانات على أعمال المعالجة

نص المشرع على الموافقة الصريحة المسبقة للشخص المعني بالبيانات، وقد عرفت اللائحة الأوربية الموافقة بأنها أي إشارة يتم تقديمها بحرية ومحددة ومستنيرة ولا لبس فيها لرغبات صاحب البيانات والتي يشير من خلالها، من خلال بيان أو عمل إيجابي واضح، إلى الموافقة على معالجة البيانات الشخصية المتعلقة به او بها([1])،

تلك الأغراض وكما هو محدد في كل مناسبة للتغيير الغرض. [٤] **استخدام مبدأ التقييد** ويعني لا ينبغي الكشف عن البيانات الشخصية أو إتاحتها أو استخدامها بطريقة أخرى لأغراض أخرى غير تلك المحددة وفقًا للفقرة ٩ باستثناء: موافقة صاحب البيانات؛ أو سلطة القانون. [٥] **مبدأ الضمانات الأمنية** يعني أنه يجب حماية البيانات الشخصية بضمانات أمنية معقولة ضد مخاطر مثل فقدان البيانات أو الوصول غير المصرح به أو إتلافها أو استخدامها أو تعديلها أو الكشف عنها. [٦] **مبدأ الانفتاح** يعني أنه يجب أن تكون هناك سياسة عامة للانفتاح حول التطورات والممارسات والسياسات المتعلقة بالبيانات الشخصية. ويجب أن تكون الوسائل متاحة بسهولة لإثبات وجود وطبيعة البيانات الشخصية، والأغراض الرئيسية لاستخدامها، بالإضافة إلى الهوية والإقامة المعتادة لمراقب البيانات. [٧] **مبدأ المشاركة الفردية** وتعني أنه يجب أن يكون للفرد الحق في الحصول من مراقب البيانات، أو خلاف ذلك، على تأكيد ما إذا كان مراقب البيانات لديه بيانات متعلقة به أم لا، أن يبلغه بالبيانات المتعلقة به في غضون فترة زمنية معقولة؛ بتهمة غير مفرطة، إن وجدت؛ بطريقة معقولة وبصيغة يسهل فهمها له؛ إبداء الأسباب في حالة رفض الطلب المقدم بموجب الفقرتين الفرعيتين (أ) و(ب)، والقدرة على الطعن في هذا الرفض؛ الاعتراض على البيانات المتعلقة به، وإذا نجح التحدي في محو البيانات أو تصحيحها أو إكمالها أو تعديلها. [٨] **مبدأ المساءلة** يعني أنه يجب أن يكون مراقب البيانات مسؤولاً عن الامتثال للتدابير التي تؤدي إلى تنفيذ المبادئ المذكورة أعلاه.

([1]) حيث تنص على أنه:

(consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative

وقد أضافت المادة السابعة من اللائحة شروطاً خاصة بالموافقة وحق الشخص المعنى بالبيانات في سحب موافقته المسبقة على معالجة البيانات الكترونيا وذلك في أي وقت([1]). حيث تنص على أنه([2]): [١] في الحالات التي تعتمد فيها المعالجة على الموافقة، يكون المراقب قادرًا على إثبات أن صاحب البيانات قد أعطى الموافقة على معالجة البيانات الشخصية المتعلقة به. [٢] إذا تم إعطاء موافقة صاحب البيانات في إطار إعلان مكتوب يتعلق أيضًا بأمور أخرى، فيجب تقديم طلب الموافقة في شكل يميزه بوضوح عن هذه الأمور الأخرى ةفي شكل مفهوم ويمكن الوصول إليه بسهولة، وتصاغ بعبارات واضحة وبسيطة، ولا يوجد أي جزء من هذا البيان يشكل انتهاكًا لهذه اللوائح. [٣] يحق لصاحب البيانات سحب الموافقة في أي وقت ولا يؤدي سحب الموافقة إلى المساس بمشروعية المعالجة بناءً على الموافقة المقدمة قبل هذا السحب. ويتم إبلاغ الشخص المعني بذلك قبل إعطاء الموافقة ومن السهل الانسحاب مثل إعطاء الموافقة.[٤] عند تحديد ما إذا كانت الموافقة تُمنح بحرية أم لا، ينبغي إيلاء

---

action, signifies agreement to the processing of personal data relating to him or her;)

([1]) كان التوجيه الأوربي الصادر في ٧ ابريل ١٩٧٨ بشأن قانون المعلومات والسجلات والحريات لا يجيز إجراء معالجة البيانات بغير رضاء صاحب هذه البيانات وأن يصدر الرضا عن إرادة حرة غير مشوبة بأى عيوب وأن يكون محددا وأن يكون على بصيرة وعلم من غرض طلبها وتجميعها.

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

الاعتبار الواجب لأمور من بينها ما إذا كان تنفيذ العقد، بما في ذلك تقديم الخدمة، يخضع للموافقة على معالجة البيانات الشخصية التي ليست ضرورية لتنفيذ قال العقد.

تنص المادة الثانية من القانون ١٥١ لسنة ٢٠٢٠ على أنه([١]): لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانونًا، وعليه فإن المشرع قد خص بالحماية الشخص الطبيعي دون الشخص الاعتباري، وهذا ما أشارت إليه كافة القوانين وكذا اللائحة الأوربية باعتبار أن الشخص الاعتباري هو مؤسسة وهي تعمل وفقاً لنظم وقواعد يحميها المشرع، وأن الحماية في هذا القانون تستهدف البيانات الشخصية للشخص الطبيعي فقط. ونستخلص من ذلك أن المشرع قد قصر الحماية على البيانات المعالجة الكترونيا وهذا يتفق مع نص المادة الثانية من اللائحة الأوربية، كما أنه خاص بالأشخاص الطبيعيين دون سواهم([٢]).

([١]) نصت المادة السابعة من القانون الجزائري على شرط الموافقة الصريحة والكتابية على عملية المعالجة.

([٢]) نصت المادة ٣٦ من القانون ١٥١ لسنة ٢٠٢٠ على أنه: يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات .وتكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول علي منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.

أشارت اللائحة الأوربية في المادة ١١/٤ إلى ضرورة موافقة الشخص المعني، حيث عرفت الموافقة الصادرة من الشخص المعني بأنها ([1]): كل مظهر من مظاهر الإرادة الحرة والمحددة والواضحة والفريدة من نوعها من قبل الشخص المعني الذي يقبله من خلال إعلان أو من خلال عمل إيجابي واضح، حيث أن البيانات الخاصة بشخصية الشخص المعني تتعلق بالموضوع([2]).

وقد نصت اللائحة الأوربية على قواعد خاصة بالأطفال حيث نصت المادة الثامنة إلى عند موافقة الأطفال فيما يتعلق بمعالجة البيانات يجب أن يبلغ الطفل ١٦ سنة على الأقل، وإلا تم الرجوع إلى المسئول عنه سواء كان الأب أو الولي عليه، وأقر حق الدول الأوربية في تخفيض السن عن ذلك بشرط ألا يقل عن ١٣ سنة. وقد أشارت الديباجة الخاصة باللائحة إلى أنه يستحق الأطفال حماية خاصة فيما يتعلق ببياناتهم الشخصية لأنهم قد يكونون أقل وعيًا بالمخاطر والعواقب والضمانات المعنية

([1]) «consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

([2]) أقرت محكمة العدل الأوربية قرار المفوضية الأوربية بشأن رفض منح احدى الشركات المحاضر الخاص باجتماع عقدته المفوضية من أجل حماية البيانات الشخصية للأشخاص في الاجتماع لأن المشاركين لم يوافقوا على الكشف عن بياناتهم وأن الشركة لم تثبت أمام المحكمة ضرورة للوصول إلى تلك المعلومات.

CJEU, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd [GC], 2010 .

وحقوقهم المتعلقة بمعالجة البيانات الشخصية. وينبغي أن تنطبق هذه الحماية المحددة، على وجه الخصوص، على استخدام البيانات الشخصية المتعلقة بالأطفال لأغراض التسويق أو إنشاء ملفات تعريف الشخصية أو المستخدمين وجمع البيانات الشخصية المتعلقة بالأطفال عند استخدام الخدمات المقدمة مباشرة إلى الطفل. لا ينبغي أن تكون موافقة صاحب المسؤولية الأبوية ضرورية في سياق خدمات الوقاية أو الاستشارة المقدمة مباشرة للطفل.

[٢] الضوابط اللاحقة على المعالجة

[أ] المشروعية والنزاهة

وهذا يعني أن تتم المعالجة بطريقة مشروعة ونزيهة وبشكل قانوني وأن تستند إلى مبررات حقيقية ومشروعة([1])، والتأكد من موافقة صاحب الشأن وأن تكون لازمة لحماية مصالحه ومصالح المجتمع، فالمشروعية تعني توافق ذلك مع القانون فلا يجوز جمع البيانات إلا لغاية أكد عليها. ويجب أن يكون المعالج حريص على عدم تعرف الغير على تلك البيانات أو الوصول إليها وكذلك عدم حدوث أي تعديل أو تغيير للبيانات لإظهار الشخص المعنى على نحو سيء. اعتبرت محكمة النقض

([1]) **إكرام سليمان قجم**: الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن- رسالة ماجستير مقدمة لكلية القانون جامعة قطر- ٢٠٢١- ص٢٢، يشير البعض إلى أنه يجب ألا تتم معالجة البيانات الشخصية إلا بناء على اتباع أسس وأساليب تتسم بالشفافية دون استخدام طرق احتيالية أو أسباب غير واضحة وغير صريحة للحصول على موافقة صاحب البيانات دون علمه الواضح بما سيجري على بياناته- **ميادة مصطفي المحروقي**: المرجع السابق- ص١٥١٢.

الفرنسية تجميع البريد الالكتروني للأشخاص دون علمهم تجميعاً غير مشروع للبيانات الشخصية يستحق فاعله العقاب([1]).

وضع المشرع في القانون ١٥١ لسنة ٢٠٢٠ حالات مستثناة من الحصول على موافقة الشخص المعني بالبيانات متي كانت المعالجة تحقق مصلحته وتعذر الاتصال به أو كان الحصول علي موافقته يتطلب مجهوداً مرهقاً أو كانت معالجة البيانات يقتضيها القانون أو وفقاً لاتفاق يكون صاحب البيانات طرفاً فيه أو للحفاظ على المصالح الحيوية للشخص المعني إذا كان من الناحية البدنية أو القانونية حيث نصت المادة السادسة على أنه: تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية: [١] موافقة الشخص المعني بالبيانات علي إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر، [٢] أن تكون المعالجة لازمة وضرورية تنفيذًا لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات ، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها، [٣] تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً علي حكم قضائي، [٤] تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات .

([1]) Cass. Crim , 14 mars 2006 , Bull.Crim, 2006, N° 69, p. 267.

وقد نصت اللائحة الأوربية على مشروعية المعالجة (Licéité du traitement) حيث نصت المادة السادسة على أنه تكون المعالجة قانونية فقط إذا تم استيفاء واحد على الأقل من الشروط التالية وإلى الحد الذي يتم فيه استيفاء([1]): [أ] وافق صاحب البيانات على معالجة بياناته الشخصية لغرض محدد أو أكثر؛ [ب] المعالجة ضرورية لأداء العقد الذي يكون موضوع البيانات طرفًا فيه أو لتنفيذ تدابير ما قبل التعاقدية المتخذة بناءً على طلب موضوع البيانات؛ [ج] المعالجة ضرورية للامتثال للالتزام القانوني الذي يخضع له المراقب؛ [د] المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر؛ [هـ] المعالجة ضرورية لأداء مهمة لتحقيق المصلحة العامة أو في ممارسة السلطة العامة المخولة للمراقب؛ [و] المعالجة ضرورية لأغراض المصالح المشروعة التي يسعى إليها المراقب أو طرف ثالث، ما لم يتم تجاوزها بالمصالح أو الحقوق والحريات الأساسية لصاحب البيانات والتي تتطلب حماية البيانات الشخصية، لا سيما عندما يكون الشخص المعني هو طفل.

[ب] المعالجة لأغراض محددة

يجب أن تكون المعالجة لأغراض محددة ومشروعة وواضحة وتتناسب مع الغاية المستهدفة منها وبكل أمانة وفي إطار مشروع وضروري، ويعتبر مبدأ الغاية من تجميع البيانات ومعالجتها هو أحد محاور البيانات الشخصية فلا يجوز تجميع

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

البيانات الشخصية إذا كان من يقوم بذلك لا يعلم بالهدف من هذا التجميع([1])، وأن تكون المعالجة تهدف إلى تنظيم أمور خاصة بالشخص المعنى، فلا تكون لها أغراض إعلانية أو ربحية أو تسويقية([2])، فعلي سبيل المثال المعلومات الشخصية بشخص من ذوى الإعاقة يجب أن تستهدف تحديد أطر علاجية له تقديم خدمات له مثل العمل أو إصدار بطاقة إثبات الإعاقة والخدمات المتكاملة أو وضعه في السجل الخاص بطالبي الخدمة أو التأهيل المجتمعي أو الدمج الشامل وتوفير المعدات له وغير ذلك مما نص عليها القانون رقم ١٠ لسنة ٢٠١٨ بشأنه حقوق الأشخاص ذوى الإعاقة.

ولم يحدد القانون ١٥١ لسنة ٢٠٢٠ ما يتعلق بالبيانات الجنائية المتعلقة ببعض الأشخاص ممن هم قد ارتكبوا جرائم وأصبحوا مواطنين صالحين وكيفية التعامل مع بياناتهم، وفي الحقيقة أن هذا المسألة تحتاج إلى إعادة نظر، لذا نري أن يكون ذلك من اختصاص مركز حماية البيانات الشخصية، فلا يجوز إعطاء بيانات جنائية خاصة بشخص مضي عليها فترة من الزمن إذا كان هذا الشخص قد أصبح مواطن صالح وهو ما يطلق عليه الحق في النسيان. وقد عرفته اللجنة الوطنية للمعلومات والحريات بفرنسا أو ما يعرف ب «La CNIL" الحق في النسيان الرقمي بأنه"

([1]) **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية– المرجع السابق– ص٤٠٦.

([2]) **اكرام سليمان قجم**: المرجع السابق– ص٢٢.

الإمكانية المخولة لأي شخص في التحكم في الأثار الرقمية الخاصة به وفي حياته الرقمية سواء أكانت عامة أو خاصة" ([1])

نصت المادة العاشرة من اللائحة الأوربية على معالجة البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية (Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions) حيث تضمنت تلك المادة أنه: لا يجوز إجراء معالجة البيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم ذات الصلة أو التدابير الأمنية بناءً على المادة ٦ (١) إلا تحت سيطرة سلطة عامة، أو إذا كانت المعالجة مسموح بها بموجب قانون الاتحاد أو قانون دولة ما. الدولة العضو التي توفر الضمانات المناسبة لحقوق وحريات أصحاب البيانات. لا يمكن الاحتفاظ بأي سجل كامل للإدانات الجنائية إلا تحت سيطرة السلطة العامة.

وقد أشارت الديباجة الخاصة باللائحة الأوربية لحماية البيانات([2]) إلى أن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة لأغراض الوقاية والكشف والتحقيق والملاحقة القضائية للجرائم الجنائية أو تنفيذ العقوبات الجنائية، بما في ذلك الحماية من التهديدات للأمن العام ومنع مثل هذه التهديدات وحرية حركة هذه البيانات، هي موضوع يحدد قانوناً من قبل دول الاتحاد. ولا ينبغي

([1]) :https://hunalibya.com/digital-life/9575/

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

أن تنطبق اللائحة على أنشطة المعالجة التي يتم تنفيذها لهذه الأغراض. ومع ذلك، يجب أن تخضع البيانات الشخصية التي تعالجها السلطات العامة بموجب هذه اللائحة، عند استخدامها لهذه الأغراض ويجوز للدول الأعضاء أن تعهد إلى السلطات المختصة بمهام لا يتم تنفيذها بالضرورة لأغراض منع الجرائم الجنائية أو تنفيذ العقوبات الجنائية أو كشفها والتحقيق فيها وملاحقتها قضائيًا، بما في ذلك الحماية من التهديدات الموجهة ضد الأشخاص ومنع مثل هذه التهديدات، بحيث تقع معالجة البيانات الشخصية لهذه الأغراض الأخرى، بقدر ما تقع ضمن نطاق تطبيق قانون الاتحاد، أما فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة للأغراض التي تقع ضمن نطاق هذه اللائحة، ينبغي أن تكون الدول الأعضاء قادرة على الاحتفاظ أو إدخال أحكام أكثر تحديدًا لتكييف تطبيق قواعد هذه اللائحة. ويجوز أن تحدد هذه الأحكام بشكل أكثر دقة المتطلبات المحددة لمعالجة البيانات الشخصية من قبل السلطات المختصة لتلك الأغراض الأخرى، مع مراعاة الهيكل الدستوري والتنظيمي والإداري للدولة العضو المعنية. عندما تقع معالجة البيانات الشخصية من قبل هيئات خاصة ضمن نطاق هذه اللائحة، ينبغي أن تنص على إمكانية للدول الأعضاء، في ظل ظروف معينة، أن تحدد بموجب القانون التزامات معينة وحقوق معينة حيث يشكل هذا التقييد إجراءً ضروريًا ومتناسبًا في مجتمع ديمقراطي لضمان مصالح محددة مهمة مثل الأمن العام، وكذلك منع الجرائم الجنائية وكشفها والتحقيق فيها وملاحقة مرتكبيها أو تنفيذ العقوبات الجنائية، بما في ذلك الحماية من التهديدات

للسلامة العامة ومنعها. وهذا مهم، على سبيل المثال، في مكافحة غسيل الأموال وغيرها([1]).

[د] مدة الحفظ محددة(تقييد الاحتفاظ)

أشار القانون وأشارت اللائحة الأوربية إلى ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها، وهذا يعني أنه لا تتجاوز المدة الضرورية لتحقيق الأهداف والأغراض التي تمت بشأنها فلا تتجاوز ذلك، وهذا يعني أيضاً حق الشخص المعني في التأكد من عدم احتفاظ القائم بالمعالجة بالاحتفاظ ببياناته وطلبه حذف البيانات وسحبها من القائم بالمعالجة. وقد أشارت الديباجة الخاصة باللائحة إلى أنه يجب أن تكون الأغراض المحددة لمعالجة البيانات الشخصية صريحة ومشروعة، ويتم تحديدها عند جمع البيانات الشخصية. يجب أن تكون البيانات الشخصية كافية وذات صلة ومحدودة بما هو ضروري للأغراض التي تتم معالجتها من أجلها. ويتطلب ذلك، على وجه الخصوص، التأكد من أن مدة الاحتفاظ بالبيانات تقتصر على الحد الأدنى الصارم. يجب معالجة البيانات الشخصية فقط إذا كان

([1]) قضت محكمة العدل الأوربية إلى أن صحة توجيه الاحتفاظ بالبيانات بهدف مكافحة الجرائم يحقق مصلحة عامة ولكن أن يكون ذلك دون تمييز أو تقييد أو استثناء في ضوء مكافحة الجرائم الخطرة (without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime) –

CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014.

الغرض من المعالجة لا يمكن تحقيقه بشكل معقول بوسائل أخرى. لضمان عدم الاحتفاظ بالبيانات لفترة أطول من اللازم، يجب أن يحدد المراقب مواعيد نهائية للمسح أو للمراجعة الدورية([1]).

قضت المحكمة الأوربية لحقوق الإنسان بعدم جواز الاحتفاظ ببيانات الشخص لأجل غير مسمي وأن الاحتفاظ ببصمات الأصابع وعينات الخلايا وملفات الحمض النووي كان غير متناسب وغير ضروري في مجتمع ديمقراطي، بعد أن انتهت الإجراءات ضد مقدمي الطلب بالبراءة ووقف الإجراءات التي سبق اتخاذها([2]). كما أثارت محكمة العدل الأوروبية مسألة غياب المعايير الموضوعية في توجيه الاحتفاظ بالبيانات (Directive 2006/24/EC –Data Retention Directive)، والتي على أساسها يجب تحديد الفترة الدقيقة للاحتفاظ بالبيانات – والتي يجب أن تتراوح من ستة أشهر كحد أدنى إلى ٢٤ شهرًا كحد أقصى – لضمان اقتصار هذه الفترة على ما هو ضروري تمامًا([3]).

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

([2]) ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008.

([3]) CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014.

[هـ] البيانات محددة ولا يتم معالجة كافة بيانات الشخص المعنى(تقليل البيانات)

وهذا يعني ألا يقوم المعالج بالحصول على كافة البيانات الشخصية للشخص المعنى بل يجب أن يكتفي بالبيانات التي تحقق الغرض الذي تتم من أجله المعالجة فعلي سبيل المثال إذا تعلق الأمر بإصدار بطاقة المسن الأولي بالرعاية وفقا للقانون ١٩ لسنة ٢٠٢٤ فيجب أن يكون ذلك بغرض تقديم الخدمات التأمينية والصحية له لذا فلا يجب أن يقوم القائم بالمعالجة بالحصول على بيانات شخصية لا تتعلق بالأمر بل يكتفي بالبيانات التي تسهل له الغرض القائم به. وقد أشارت الفقرة رقم ٧٨ في الديباجة الخاصة باللائحة العامة للبيانات الأوربية إلى ضرورة تقليل معالجة البيانات إلى الحد الأدني.

أضافت المحكمة أن التوجيه الأوربي لعام ٢٠٠٦ بشأن الاحتفاظ بالبيانات قد فشل في تلبية الضرورة التي نشأ من أجلها بشأن السماح للسلطات الوطنية بالحصول على فرص إضافية للتحقيق في الجرائم الخطيرة وملاحقتها، وبالتالي كان أداة قيمة للتحقيقات الجنائية. إلا أنه لم يضع قواعد واضحة ودقيقة تحد من مدى التدخل. وبدلاً من اشتراط وجود علاقة بين البيانات المحفوظة والجرائم الخطيرة، فإن التوجيه ينطبق على جميع البيانات الوصفية لجميع مستخدمي جميع وسائل الاتصال الإلكترونية. وبالتالي، يشكل تدخلاً في حقوق الخصوصية وحماية البيانات لجميع سكان الاتحاد الأوروبي تقريبًا، وهو ما يمكن اعتباره غير متناسب. ولم يتضمن التوجيه شروطًا لتقييد الأشخاص المخولين بالوصول إلى البيانات الشخصية، كما لم يخضع هذا الوصول لشروط إجرائية مثل شرط الحصول على موافقة سلطة إدارية أو محكمة قبل الوصول. وأخيرًا، لم يحدد التوجيه ضمانات واضحة لحماية البيانات المحفوظة. وبالتالي، فقد فشل في ضمان الحماية الفعالة للبيانات ضد خطر إساءة الاستخدام وضد أي وصول غير قانوني واستخدام للبيانات.

[م] عدم تعريض البيانات للفقد أو التدمير

وهذا يعني أن تحاط البيانات بقدر كبير من الحماية والسرية بحيث لا تتعرض للفقد أو التدمير من قبل الآخرين أو المحو أو التغيير، لذا يجب استخدام كافة التدابير الفنية والتنظيمية المناسبة لضمان عدم حدوث أي ضرر بالبيانات. وقد أشارت الديباجة الخاصة باللائحة الأوربية إلى ضرورة حماية البيانات من الاضرار بالسمعة أو فقدان سرية البيانات أو احداث ضرر بصاحب البيانات، كما أشارت الفقرة ٨٣ من الديباجة إلى أن ضمان الأمن ومنع أي معالجة تتم بشكل ينتهك هذه اللائحة، من المهم أن يقوم جهاز التحكم أو المعالج بتقييم المخاطر الكامنة في المعالجة وتنفيذ تدابير للتخفيف منها، مثل التشفير. ويجب أن تضمن هذه التدابير مستوى مناسبًا من الأمان، بما في ذلك السرية، مع الأخذ في الاعتبار حالة المعرفة وتكاليف التنفيذ فيما يتعلق بالمخاطر وطبيعة البيانات الشخصية المطلوب حمايتها. عند تقييم مخاطر أمن البيانات، فإن المخاطر التي تشكلها معالجة البيانات الشخصية، مثل التدمير أو الخسارة أو التغيير، أو الكشف غير المصرح به عن البيانات الشخصية المنقولة أو المخزنة أو المعالجة بطريقة أخرى أو الوصول غير المصرح به إلى هذه البيانات، عن طريق الخطأ أو بشكل غير قانوني، مما قد يؤدي إلى ضرر جسدي أو مادي أو معنوي([1]).

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

ثالثاً: معالجة البيانات السرية والحساسة

أشارت التشريعات إلى حساسية بعض البيانات «données sensibles» وضرورة وضع ضوابط خاصة بمعالجتها، وعليه فإن الأساس هو حظر معالجة أو نقل أو تخزين أو حفظ أو اتاحة البيانات الشخصية التي تكشف عن بيانات حساسة كالبيانات الجينية والبيانات البيومترية؛ إلا أنه استثناء من ذلك فيمكن معالجة تلك البيانات بترخيص من مركز حماية البيانات الشخصية والمشار إليه في الفصل التاسع في القانون ١٥١ لسنة ٢٠٢٠ والذي حدد حالات محددة وأعطى صاحب البيانات موافقة صريحة على معالجة تلك البيانات الشخصية لغرض محدد أو أكثر(١)، أو أن تكون المعالجة ضرورية لمصلحة عامة يحددها المركز مثل الطب الوقائي إذا كان الشخص مصاب بمرض خطير يعرض الآخرين للإصابة به أو يهدد الصحة العامة للمجتمع أو لحماية المصالح الحيوية لصاحب البيانات إذا كان غير قادر جسديًا أو قانونيًا على إعطاء الموافقة؛ وأن تكون المعالجة تتعلق بأمر مشروع حتى لا يحدث إضرار بصاحب البيانات، ومن خلال إعلامه بكافة البيانات التي سيتم معالجتها وأسباب ذلك والغرض من المعالجة، وكذلك إذا طلبت البيانات الجهات القضائية ودون علانية وفي الحدود القانونية والقضائية الخاصة بذلك، أو تكون بهدف تحقيق مصلحة صاحب البيانات مثل معالجة بيانات خاصة بشخص معاق حتى يمكن توفير

(١) الترخيص المسبق هو إجراء تقرره السلطة المختصة بحماية البيانات الشخصية وفق شروط وضوابط محددة- **رضا حميسي**: الضمانات القانونية لحماية البيانات الشخصية- كلية الحقوق والعلوم السياسية- جامعة قاصدي مرباح – ورقلة- الجزائر – ص٦٧.

أجهزة تأهيلية له أو لرعايته الصحية والاجتماعية وفي كل الحالات يجب احترام جوهر الحق في حماية البيانات وتوفير التدابير المناسبة والمحددة لحماية الحقوق والمصالح الأساسية لصاحب البيانات.

حيث نصت المادة ١٢ من القانون على أنه: يحظر علي المتحكم أو المعالج سواء كان شخصًا طبيعيا أو اعتباريًا جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز. وفيما عدا الأحوال المصرح بها قانونًا، يلزم الحصول علي موافقة كتابية وصريحة من الشخص المعني([1]). وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر. ويجب ألا تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر مشروطة بتقديم بيانات شخصية للطفل تزيد علي ما هو ضروري للمشاركة في ذلك .وذلك كله وفقًا للمعايير والضوابط التي تحددها اللائحة التنفيذية لهذا القانون.

وعليه فإن المشرع ترك المعايير والضوابط غير محددة حتى يترك المجال للائحة التنفيذية لوضعها باعتبارها أمور إجرائية، فلها أن تفرض إجراءات من شأنها تحقيق الصالح العام وأن تفرض ضرورات يحددها الوضع الراهن.

وقد نصت اللائحة الأوربية في عدد من القواعد الخاصة بمعالجة الفئات الخاصة من البيانات الشخصية(الحساسة) حيث نصت المادة ١/٩ من اللائحة

([1]) يشترط الموافقة الصريحة والمسبقة والكتابية على معالجة البيانات الشخصية من أهم الضمانات السابقة على المعالجة سواء من الشخص المعني أو من وليه إذا كان قاصرا أو محجورا عليه أو من ممثله القانوني- **رضا حميسي**: المرجع السابق- ص٦٧.

الأوربية على أن ([1]) المبدأ العام هو حظر معالجة البيانات الحساسة ثم جاءت المادة ٢/٩ لتضع استثناءات من حظر معالجة البيانات الحساسة تتمثل في: [١] موافقة صاحب البيانات صراحةً على معالجة البيانات([2])؛ [٢] تتم المعالجة بواسطة هيئة غير ربحية، [٣] تتعلق المعالجة ببيانات تم نشرها صراحةً من قبل صاحب البيانات؛ [٤] المعالجة ضرورية: للوفاء بالتزامات وممارسة الحقوق المحددة للمراقب أو صاحب البيانات في سياق التوظيف والضمان الاجتماعي والحماية الاجتماعية؛ لحماية المصالح الحيوية لصاحب البيانات أو أي شخص طبيعي آخر (عندما لا يستطيع صاحب البيانات إعطاء الموافقة)؛ لتأسيس أو ممارسة أو الدفاع عن المطالبات القانونية أو عندما تتصرف المحاكم بصفتها القضائية؛ لأغراض الوقاية أو الطب المهني: "لتقييم القدرة على العمل للموظف، أو التشخيص الطبي، أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية على أساس قانون الاتحاد أو قانون الدولة العضو أو بموجب عقد مع أحد المتخصصين في مجال الصحة"؛ لأغراض الأرشفة في المصلحة العامة، أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية. لأسباب تتعلق بالمصلحة العامة

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

([2]) أكد الدليل الأوربي لحماية البيانات إلى أن أول سبب يمكن للمعالجة أن تكون قانونية هو موافقة صاحب البيانات سواء كانت البيانات حساسة أو غير حساسة على أن تكون الموافقة صريحة.
Handbook on European, data protection law, 2018 edition

في مجال الصحة العامة؛ لأسباب تتعلق بالمصلحة العامة بشكل جوهري. [٥] إذا تمت المعالجة بواسطة أخصائي رعاية صحية يخضع لالتزام السرية المهنية، وفي النهاية أشارت إلى أنه يجوز للدول الأعضاء أن تبقي أو تفرض شروطًا إضافية، بما في ذلك القيود، فيما يتعلق بمعالجة البيانات الجينية أو البيانات البيومترية أو البيانات الصحية.

وضعت أشارت الفقرة ٧١ من الديباجة الخاصة باللائحة الأوربية لحماية البيانات إلى أنه يجب أن يكون لصاحب البيانات الحق في عدم الخضوع لقرار قد يتضمن إجراءً يتضمن تقييم بعض الجوانب الشخصية المتعلقة به، والذي يتم اتخاذه فقط على أساس المعالجة الآلية وينتج عنه آثار قانونية أو التي تؤثر بطريقة مماثلة بشكل كبير، مثل الرفض التلقائي لطلب الائتمان عبر الإنترنت أو ممارسات التوظيف عبر الإنترنت دون أي تدخل بشري. يشمل هذا النوع من المعالجة "التنميط" الذي يتكون من أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تهدف إلى تقييم الجوانب الشخصية المتعلقة بالشخص الطبيعي، ولا سيما تحليل أو التنبؤ بالجوانب المتعلقة بأداء صاحب البيانات في العمل، ووضعه الاقتصادي، صحتهم، أو تفضيلاتهم أو اهتماماتهم الشخصية، أو موثوقيتهم أو سلوكهم، أو موقعهم وحركاتهم، طالما أنها تنتج آثارًا قانونية تتعلق بالشخص المعني أو تؤثر بشكل كبير على نحو مماثل. ومع ذلك، يجب السماح باتخاذ القرار بناءً على هذه المعالجة، بما في ذلك التصنيف، حيثما يكون ذلك مصرحًا به صراحةً بموجب قانون الاتحاد أو الدول الأعضاء الذي يخضع له المراقب المالي، بما في ذلك لأغراض مراقبة ومنع

الاحتيال والتهرب الضريبي وفقًا لـ القواعد والمعايير والتوصيات الصادرة عن مؤسسات الاتحاد أو الهيئات الإشرافية الوطنية، ولضمان أمان وموثوقية الخدمة التي يقدمها مراقب البيانات، أو اللازمة لإبرام أو تنفيذ عقد بين صاحب البيانات ومراقب البيانات، أو إذا أعطى صاحب البيانات موافقة صريحة. على أية حال، يجب أن تكون المعالجة من هذا النوع مصحوبة بالضمانات المناسبة، والتي يجب أن تتضمن معلومات محددة عن صاحب البيانات بالإضافة إلى الحق في الحصول على تدخل بشري، للتعبير عن وجهة نظره، والحصول على تفسير للقرار المتخذ. اتباع هذا النوع من التقييم والطعن في القرار. هذا الإجراء لا ينبغي أن يهم الطفل.

من أجل ضمان معالجة عادلة وشفافة فيما يتعلق بصاحب البيانات، مع الأخذ في الاعتبار الظروف والسياق الخاص الذي تتم فيه معالجة البيانات الشخصية، يجب على المراقب استخدام الإجراءات الرياضية أو الإحصائية الكافية لأغراض التنميط، وتطبيق التقنية والتنظيمية المناسبة تدابير لضمان، على وجه الخصوص، تصحيح العوامل التي تؤدي إلى أخطاء في البيانات الشخصية وتقليل مخاطر الخطأ إلى الحد الأدنى، وتأمين البيانات الشخصية بطريقة تأخذ في الاعتبار المخاطر التي من المحتمل أن تؤثر على المصالح وحقوق الشخص المعني، وتمنع، من بين أمور أخرى، آثار التمييز ضد الأشخاص الطبيعيين على أساس الأصل العنصري أو الإثني، أو الآراء السياسية، أو الدين أو المعتقد، أو العضوية النقابية، أو الحالة الجينية أو الحالة الصحية، أو التوجه الجنسي، أو أي شيء آخر. العلاج الذي يؤدي

إلى تدابير تنتج مثل هذا التأثير. يجب السماح باتخاذ القرار الآلي والتوصيف بناءً على فئات خاصة من البيانات الشخصية فقط في ظل ظروف محددة([1]).

ويشار أن المشرع المصري لم يتناول التنميط الذي أشارت إليه اللائحة الأوربية في المادة ٤/٤ والمتعلقة بالتعريفات والذي يعني أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتكون من استخدام هذه البيانات الشخصية لتقييم جوانب شخصية معينة تتعلق بشخص طبيعي، ولا سيما لتحليل أو التنبؤ بالعناصر المتعلقة بالأداء في العمل، والوضع الاقتصادي، والصحة، والشخصية التفضيلات أو الاهتمامات أو الموثوقية أو السلوك أو الموقع أو تحركات ذلك الشخص الطبيعي([2])، ونري أنه يجب على المشرع تعديل النص وتعريفه أو توضيحه من خلال اللائحة التنفيذية.

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

([2]) «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

المبحث الثاني

حق الشخص المعني بالبيانات في المعالجة الصحيحة لبياناته

مقدمة:

وضعت التشريعات الوطنية وكذا اللائحة الأوربية لحماية البيانات الشخصية على كاهلها أهمية حماية البيانات الشخصية ووضعت الكثير من الشروط والضمانات حال معالجة البيانات الشخصية للشخص المعني بالبيانات(محل الحماية)، من بينها نزاهة ومشروعية المعالجة وأنها لأغراض محددة وواضحة وأن تكون دقيقة وأن تهتم بخصوصية وحساسية البيانات الشخص المعني، وحقه في اللجوء للقضاء وطلب التعويض عن الأضرار التي تقع عليه وانتهاك حقوقه، وقد أشار الفصل الثاني من القانون ١٥١ لسنة ٢٠٢٠ على حقوق الشخص المعني وحقه في التعويض عن الأضرار الناتجة عن انتهاك تلك الحقوق، كما تناول الفصل الثالث من اللائحة الأوربية حقوق صاحب البيانات.

وسوف نتناول في هذا المبحث حقوق الشخص المعني بالبيانات في المعالجة الصحيحة لبياناته على النحو الذي لا يضره، وذلك من خلال بيان لحقه في الخصوصية وعلاقتها بحماية بياناته الشخصية، وكذا حقه أثناء المعالجة، وكذا حقه في تعويض الأضرار الناتجة عن المعالجة الخاطئة للبيانات، وسوف نتناول ذلك من خلال ما يلي:

المطلب الأول: حق الشخص المعنى بالبيانات في الخصوصية

المطلب الثاني: حق الشخص المعني بالبيانات أثناء المعالجة

المطلب الثالث: تعويض الأضرار الناتجة عن المعالجة الخاطئة للبيانات

المطلب الأول

حق الشخص المعني بالبيانات في الخصوصية

تعريف الشخص المعني بالبيانات:

هو أى شخص طبيعي تتم معالجة بياناته الشخصية أو صاحب البيانات المعالجة، وهو الطرف الأساسي المحمي بالقانون، وقد أشار إليه المشرع بمسمي **الشخص المعني بالبيانات** وهو أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونيًا تدل عليه قانونًا أو فعلاً، وتمكن من تمييزه عن غيره، وهذا الشخص هو محور القانون، وقد عرفت المادة الرابعة من اللائحة الأوربية هذا الشخص بأنه (موضوع البيانات) أو الشخص الطبيعي الذي يمكن تحديد هويته هو الشخص الذي يمكن التعرف عليه بشكل مباشر أو غير مباشر، ولاسيما بالرجوع إلى معرف مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف عبر الإنترنت أو إلى واحد أو أكثر

من العوامل المحددة للعوامل الجسدية أو الفسيولوجية أو الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص الطبيعي([1]).

عرفت المادة الثالثة من القانون الجزائري رقم (١٨-٠٧) **الشخص المعني** بأنه كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة. كما عرفت المادة ١٦/١ من النظام السعودى صاحب البيانات الشخصية: الفرد الذي تتعلق به البيانات الشخصية".

تنص المادة الأولي من اللائحة الأوربية على (الغرض والأهداف- Objet et objectifs) حيث تنص على أنه([2]): [١] تضع هذه اللائحة القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والقواعد المتعلقة بحرية حركة البيانات الشخصية. [٢] تحمي هذه اللائحة الحقوق والحريات الأساسية للأشخاص الطبيعيين، ولاسيما حقهم في حماية البيانات الشخصية. [٣] لا يجوز تقييد أو حظر حرية حركة البيانات الشخصية داخل الاتحاد لأسباب تتعلق بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية.

([1]) راجع في ذلك المادة ١/٤ من اللائحة الأوربية والتي تنص على :

('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person؛

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

العلاقة بين الحق في الخصوصية والحق في حماية البيانات الشخصية:

يعتبر الحق في الخصوصية من الحقوق القديمة التي أكدت عليها الاتفاقيات الدولية لحقوق الإنسان، أما الحق في حماية البيانات الشخصية فهو حق حديث نشأ في السنوات الماضية([1])، فالخصوصية من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي فهي أساس بنيان كل مجتمع سليم([2])، وتعتبر فكرة الخصوصية من الأفكار الهلامية والمرنة، والتي تتغير بتغير الزمان والمكان، ومظاهرها ليست محددة المعالم، وليس كل ما يعتبر من قبيل الحياة الخاصة فى العصر الحالى هو بالضرورة ما كان فى العصر الماضى، وسيكون فى المستقبل، فاختلاف الأيديولوجيات فى كل عصر تضفي على كل عصر سماته الخاصة به، وفى ظل التوجهات العالمية الجديدة والحدود المفتوحة بين الدول وبعد أن أصبح العالم كله قرية كونية صغيرة، ومع وجود التكنولوجيا الحديثة نجد أن سمات العصر الحالي قد تغيرت كثيراً عن سابقه. فمع تزايد التقنيات والابتكارات الحديثة أصبح هناك تقييد لحركة الإنسان الذي أصبح تحت المجهر فيتم رصد تحركاته بسهولة وكذا تنقلاته؛ لذا فإنه يجب تحقيق الموازنة بين الحق في الخصوصية وحماية البيانات الشخصية وبين المصالح العامة

([1]) **عثمان بكر عثمان:** المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي- بحث منشور على شبكة الانترنت- ص٥.

([2]) See CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.

ومستلزمات الأمن القومي([١]). فالتدفق الكبير للمعلومات الموجود في الوقت الحاضر يهدد بشكل أكبر حق الأشخاص في الحياة الخاصة وذلك بسبب الكم الأكبر من الأدوات التكنولوجية الجديدة وازدياد استخدامها المتكرر وينبغي أن تتحمل الدولة مسئولية التكيف مع الصيغ التقليدية لحماية الحياة الخاصة في العصر الحالي([٢]).

ويشير البعض إلى أن الخطر قد يمس البيانات الشخصية في الحالات الآتية: [١] قيام المستفيد بعمل اشتراك ما بالمواقع الإلكترونية أو الشبكات الاجتماعية أو حتى لدى إبرامه لعقود الشراء عبر الإنترنت، حيث يضطر لتقديم بعض البيانات الخاصة به التي قد يتمَ استغلالها لأغراض تجارية تسويقية أو حتى لأغراض غير مشروعة. [٢] عندما يقوم الشخص بتصفح للمواقع التي يزورها فإنه يترك آثاراً ومعلومات خاصة به دون أن يعلم([٣]).

([١]) **ميادة مصطفي المحروقي**: المرجع السابق- ص١٤٨٦.

أشارت المحكمة الأوربية لحقوق الإنسان إلى أن الحق في الخصوصية والحق في حماية البيانات الشخصية بينهما ارتباط وثيق ولكنهما حقان متميزان- راجع في ذلك:

ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27 June 2017, para. 137.

([2]) **María Solange Maqueo Ramírez, Jimena Moreno González, Miguel Recio Gayo** :Protección de datos personales, privacidad y vida privada, la inquietante búsqueda de un equilibrio global necesario, , vol.30 no.1 Valdivia June 2017, http://dx.doi.org/10.4067/S0718-09502017000100004

([٣]) **خالد حسن أحمد**: المرجع السابق- ص١٣.

جاء قرار الجمعية العامة للأمم المتحدة بشأن الحق في الخصوصية في العصر الرقمي عام ٢٠١٣ ليدعم الحق في الخصوصية داعياً الدول لاتخاذ التدابير الازمة لوضع حد للأنشطة التي تنتهك هذا المبدأ الأساسي للمجتمع الديمقراطي ومعربة عن قلقها إزاء التأثير السلبي للمراقبة الالكترونية واعتراض الاتصالات الرقمية وجمع البيانات الشخصية على حقوق الإنسان([1]). حيث وضع الدستور حماية للحق في الحياة الخاصة حيث تنص المادة ٥٧ من الدستور على أنه: للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

كما نصت المادة ٩٩ من الدستور على أنه: 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 تعويضاً عادلاً لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي

([1]) قرار الجمعية العامة رقم (١٦٧/٦٨) بتاريخ ٢٠١٢/١٢/٣٠.

انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضماً إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون، وهذا ما أكدته المحكمة الدستورية(١)، وما قضت به محكمة النقض(٢). كما قضت محكمة البلدان الأمريكية

(١) قضت المحكمة بأنه: فإن ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي ألا يقتحمها أحد ضماناً لسريتها، وصوناً لحرمتها، ودفعاً لمحاولة التلصص عليها أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حداً مذهلاً، وكان لتنامي قدراتها على الاختراق أثراً بعيداً على الناس جميعهم حتى في أدق شئونهم، وما يتصل بملامح حياتهم، بل وببياناتهم الشخصية التي غدا الاطلاع عليها وتجميعها نهباً لأعينها ولآذانها. .... تصون مصلحتين قد تبدوان منفصلتين، إلا أنهما تتكاملان، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التي تكون – بالنظر إلى خصائصها وآثارها – أكثر اتصالا بمصيره وتأثيراً في أوضاع الحياة التي اختار أنماطها. وتبلور هذه المناطق جميعها – التي يلوذ الفرد بها، مطمئناً لحرمتها ليهجع إليها بعيدا عن أشكال الرقابة وأدواتها – الحق في أن تكون للحياة الخاصة تخومها بما يرعى الروابط الحميمة في نطاقها. ولئن كانت بعض الوثائق الدستورية لا تقرر هذا الحق بنص صريح فيها، إلا أن البعض يعتبره من أشمل الحقوق وأوسعها، وهو كذلك أعمقها اتصالا بالقيم التي تدعو إليها الأمم المتحضرة– القضية رقم ٢٣ لسنة ١٦ ق جلسة ١٩٩٥/٣/١٨.

(٢) قضت محكمة النقض بأنه: أصبح الإنترنت أداة جديدة للمعلوماتية والاتصال فهو ثورة في الاتصال الإلكتروني، وبهذا التطور السريع جدًا في نقل وتبادل المعلومات أصبح مجتمع القرن الحادي والعشرين هو مجتمع المعلومات، وفي هذا المجتمع ألغت سرعة سير وانتقال المعلومات الزمان والمكان .... منبع الخوف قادمًا من أن الإنترنت ليس له حدود ولا قيادة قانونية، وبعبارة أخرى ليس له شخصية قانونية معنوية تمثله في مواجهة المستعملين له أو في مواجهة الغير؛ لأنه عبارة عن اتحاد فيدرالي للشبكات في مجموعها يغطي تقريبًا كل الكرة الأرضية، وكان مما لاشك فيه أن بحث الحماية القانونية ضد هذه الأخطار لا يكون إلا من خلال القانون والذي تطور في هذا المجال بوضع القواعد القانونية التي تحمي اعتداء أي شخص على الحياة الخاصة للآخرين من خلال الإنترنت؛ إذ أصبحت الحياة الخاصة في غالبية دول العالم قيمة أساسية تستحق الحماية– الطعن ٩٥٤٢ لسنة ٩١ ق جلسة ١٦ / ٣ / ٢٠٢٢ مكتب فنى ٧٣ ق ٦٣ ص ٥٠٧

لحقوق الإنسان في قضية (أرتافيا موريللو وآخرون ضد بنما) أنه عندما يتعلق الأمر بالتدخل في الحياة الخاصة فمن الضروري في مثل هذه الحالات تقييم الوضع على النحو التالي: [١] ما إذا كان التدخل ينص عليه القانون، [٢] ما إذا كان يسعي إلى تحقيق هدف مشروع، [٣] ما إذا كان مناسباً وضرورياً ومتناسباً([١]).

ذهب البعض([٢]) إلى حد القول بان الحق الأصولي في الخصوصية هو جوهر الحرية بل يمكن أن يكون مرادفاً في معناه للحرية باعتبار أن الحرية مكنة المطالبة بالامتناع عن التدخل، ويفترض الحق في الخصوصية هذه المكنة أيضاً ولهذا يتلاقى مفهوما الحرية والخصوصية إلى حد بعيد باعتبار أنه يمنع على الآخرين بمقتضى الحق في الحياة الخاصة ملاحقة الفرد في حياته الخاصة، فان هذا الحق يتفق ومفهوم الحرية. فالحق في الخصوصية يعبر عن حرية فردية أو عامة مادام تحول مكنّه اقتضاء امتناع الدولة وغيرها أيضاً عن التدخل في مجال خاص محتجز ومتروك لمحض سلطانه، ولهذا نصت غالبية الدساتير في باب الحريات العامة على أن لحياة المواطنين الخاصة حرمة يحميها القانون.

([١]) تشير المبادئ التوجيهية للجهات القضائية بشأن الخصوصية وحماية البيانات الصادرة عن (unesco) إلى ضرورة توفير إطار عام للجهات القضائية لتقييم مسألتي الخصوصية وحماية البيانات بالمقارنة مع الحقوق الأخرى مثل حرية التعبير والحق في الخصوصية وهي تتضمن السوابق القضائية ذات الصلة من مختلف الهيئات الوطنية والدولية والإقليمية التي قد تساعد في فهم الجهات القضائية للأمور المطروحة، كما ترسم خطا متسقاً من حقوق الخصوصية إلى حقوق حماية البيانات والتحديات التي تواجه دعم هذه الحقوق في مواجهة التقنيات الجديدة.

([٢]) **نعيم عطية :** حق الافراد في حياتهم الخاصة ، مجلة ادارة قضايا الحكومة، العدد ٤ لسنه ٨١ ، أكتوبر – ديسمبر ١٩٧٧ ، ص٨٠ .

جاءت توصية الجمعية الاستشارية للمجلس الأوروبي فى يناير ١٩٧٠ لتعرف الخصوصية بأنها: قدرة الفرد على توجيه حياته كما يشاء مع أدنى حد من التدخل، في حين أوضحت لجنة الخبراء المنبثقة من المجلس الأوروبي لحقوق الإنسان صعوبة وضع تعريف عام شامل، فتركت للفقه المجال المفتوح لوضع عناصر الحياة الخاصة التى ليست محل اتفاق وجميعها مرنة وفضفاضة الى حد يفقدها فاعليتها فى فض مجالات التداخل بينها([١]). كما أشارت الأمم المتحدة إلى الخصوصية باعتبارها تتيح للفرد العديد من الحقوق منها نمو الفرد الحرّ وتعبيره عن شخصيته وهويته ومعتقداته، وقدرته على المشاركة في الحياة السياسية والاقتصادية والاجتماعية والثقافية. حيث قرر مجلس حقوق الإنسان بالأمم المتحدة في دورته ٢٨ بالقرار رقم (١٦/٢٨) في ٢٠١٥/٣/٢٦ المعني بالحق في الخصوصية في العصر الرقمي تعيين مقرر خاص مكلف بتعزيز وحماية الحق في الخصوصية([٢])، وقد نظر القرار السابق إلى هذا الحق من الزاوية الحقوقية كحق أصيل من حقوق الإنسان وليس من الزاوية القانونية.

([١]) التوصية رقم ٤٢٨ للجمعية الاستشارية للمجلس الأوربى فى ١٩٧٠/١/٢٣.

([٢]) وقد كلف مجلس حقوق الإنسان المقرر بعدد من المهام لتعزيز وحماية الحق في الخصوصية هي: [١] استعراض السياسات الحكومية المتعلقة باعتراض الاتصالات الرقمية وجمع البيانات الشخصية، [٢] تحديد الإجراءات التي تتطفل على الخصوصية بدون مبرر مقنع، [٣] مساعدة الحكومات على تطوير أفضل الممارسات لإخضاع المراقبة العالمية لسيادة القانون، [٤] توضيح مسؤوليات القطاع الخاص فيما يتعلق باحترام حقوق الإنسان، [٥] المساهمة في ضمان توافق الإجراءات والقوانين الوطنية مع الالتزامات الدولية في مجال حقوق الإنسان، كما كلفته بالاهتمام بالآثار المترتبة على الخصوصية في المجالات التالية: [١] المراقبة الجماعية، [٢] استخدام البيانات الشخصية والاحتفاظ بها، [٣] قواعد بيانات الحمض النووي والأدلة الجنائية، [٤] البيانات الضخمة والبيانات المفتوحة.

وقد حظي القرار المذكور بالترحيب، باعتباره أول قرار صادر عن الأمم المتحدة يؤكد أن حقوق الإنسان في العالم الرقمي يجب حمايتها وتعزيزها بالقدر ذاته، وبهما تتم حماية حقوق الإنسان في العالم المادي.

نص القرار على مجموعة من الحقوق متفرعة من الحق في الخصوصية هي: [١] **الحق في التخفي الرقمي** (Droit à l'anonymat numérique) ويعني أن لكل شخص الحق في التواجد على شبكة الإنترنت دون أن يكون مجبراً على كشف هويته الحقيقية شريطة أن لا يضر ذلك بالنظام العام وحقوق وحريات الغير. [٢] **الحق في النسيان الرقمي** (Droit à l'oubli numérique) ويعني أن يلتزم المسؤولون عن معالجة المعطيات الشخصية (مواقع التجارة الإلكترونية، المؤسسات العمومية...) بعدم حفظ تلك المعطيات لمدة تتجاوز الغاية التي جمعت من أجلها. كما يعني كذلك أن لكل شخص الحق في تعديل أو حتى سحب معلومات تخصه من شبكة الإنترنت (مواقع إلكترونية، مواقع التواصل الاجتماعي...) شريطة أن لا يحدث ذلك ضررا للأشخاص الذاتيين أو المعنويين الذين يحوزون هذه المعلومات. [٣] **الحق في الهوية الرقمية** (Droit à l'identité numérique) ويعني أن يكون لكل شخص الحق في التواجد كشخص رقمي (Homme numérique) على شبكة الإنترنت، إلى جانب وجوده كشخص حقيقي(Homme real). وترتبط بهذا الحق ضرورة تجريم انتحال الهوية الرقمية (انتحال البريد الإلكتروني، انتحال صفحة الفيس بوك، انتحال عنوان بروتوكول الإنترنت...).

تعرف الخصوصية في المجال الرقمي بأنها حق الفرد أن يحدد بنفسه متي وكيف وإلى أي مدى يمكن للمعلومات الخاصة به أن تصل للغير أو هي حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه وعملية معاملتها آلياً وحفظها وتوزيعها واستخدامها في صنع القرار الخاص به والمؤثر فيه سواء وضعت هذه المعلومات ببنوك المعلومات أو بالبريد الالكتروني أو حتى على شبكات التواصل الاجتماعي([1]).

ويعتبر مبدأ التناسب بين الحق في الخصوصية والحق في المعلومة واحدًا من المبادئ الأساسية التي تمكّن وتعزّز جدلًا ملموسًا بشأن القيود على التدخل في الحياة الخاصة وبين المصلحة العامة للمجتمع([2])، فالتناسب مبدأ أساسي في القانون الدولي يقضي بأن شرعية عمل ما تتحدَّد حسب احترام التوازن بين الهدف والوسيلة والطريقة المستخدمة لبلوغه وكذلك عواقب هذا العمل. ويعني هذا المبدأ ضمنًا الالتزام بتقدير السياق قبل تحديد شرعية عمل ما أو عدم شرعيته. وهذا التقييم هو مسؤولية من يقومون بالعمل. وفي حالة الخلاف أو الشك، تستطيع المحاكم تقييم الوقائع وبالتالي تحديد شرعيته. وتبرز أهمية هذا المبدأ في حالة حدوث تعارض بين مصلحتين،

([1]) **نبيلة رزاقي**: الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي- مجلة الدراسات القانونية المقارنة – الجزائر- المجلد السابع- العدد١- ٢٠٢٠ – ص١٩٩٥.

([2]) أشار البعض إلى أنه توافقاً مع مبدأ التناسب فإنه يجوز فرض القيود إذا كانت ضرورية وتفي بأهداف المصالح العامة المعترف بها أو الحاجة إلى حماية حقوق الآخرين وحرياتهم ويجب تنفيذها في حدود ما هو ضروري مع وجود قواعد واضحة ودقيقة تحكم نطاق وتطبيق التدبير المعني- **ميادة مصطفي المحروقي**: المرجع السابق- ص١٥٠٥.

وعادة ما يتعلق بتدخل الدولة في حقوق الأفراد، أو عندما تتعارض المصلحة العامة مع المصلحة الخاصة، حيث يدور اختيار التناسب بشكل عام حول ثلاث خطوات: [١] **الملائمة** (وتعني ما إذا كان التدخل مناسبا لتحقيق الهدف المرغوب)، [٢] **الضرورة** (وتعني أنه البديل الأقل تقييدا وتحقيق الحد الأدني للضرر)، [٣] **الهدف المشروع** (ويعني أن التدخل قائم ومحدد في التشريعات والاتفاقيات الدولية)، وقد أشار التعليق العام رقم ٣٤ الصادر عن الأمم المتحدة لسنة ٢٠١١ إلى ضرورة وجود ما يسمي بالتناسب الصارم بمعني أن يجب أن تكون متناسبة مع المصلحة المراد حمايتها.

ويمكن القول أن الحق في حماية البيانات ينبع من الحق في الخصوصية مع تمييزه بخاصتين رئيسيتين: [١] أنه ينطبق بشكل خاص على البيانات الشخصية حيث يضع شروطاً وحدوداً لمعالجتها بدلاً من النظر لقضايا الخصوصية من وجهة نظر شخصية، [٢] أن معالجة المعلومات الشخصية أصبحت منتشرة في كل مكان فحماية البيانات مهمة من أجل الحفاظ على مجموعة كبيرة من الحقوق والقيم بدءاً من تقرير المصير إلى عدم التمييز بما في ذلك حرية التعبير أيضاً.

ومما سبق يتضح مدى تأثير البيانات الشخصية المعالجة بطريقة خاطئة في الاضرار بحق الإنسان في الخصوصية والذي تأثر كثيرا في مجتمع أصبح صغيراً وأصبحت المعلومات متاحة أمام الجميع دون قيد أو شرط لذا فإن الأمر كان يتطلب التدخل التشريعي لحماية حقوق الشخص المعنى.

المطلب الثاني

حق الشخص المعني بالبيانات أثناء المعالجة

تكمن الحماية القانونية في قانون حماية البيانات الشخصية للأشخاص الطبيعيين دون الاعتباريين، وقد رسخ القانون واللائحة الأوربية على حقوق الشخص المعني بالبيانات، فوضعت قواعد خاصة بحقوقه، حيث تنص المادة الثانية من القانون ١٥١ لسنة ٢٠٢٠ على أنه([1]): لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا، ونصت الفقرة الثانية من تلك المادة على حقوق الشخص المعني بالبيانات على النحو التالي:

[١] العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

[٢] العدول عن الموافقة المسبقة علي الاحتفاظ ببياناته الشخصية أو معالجتها

[٣] التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية

[٤] تخصيص المعالجة في نطاق محدد.

[٥] العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

([1]) تنص المادة ٣٧ من القانون ١٥١ لسنة ٢٠٢٠ على أنه: يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، كل حائز أو متحكم أو معالج امتنع دون مقتض من القانون عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المادة (٢) من هذا القانون ويعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة (٣) من هذا القانون .

[٦] الاعتراض علي معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات. وتضيف الفقرة الثالثة من المادة على أنه وباستثناء البند (٥) من الفقرة السابقة، يؤدي الشخص المعني بالبيانات مقابل تكلفة الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه، ويتولي المركز إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه .

سنتناول تلك الحقوق الواردة بالقانون مع الحقوق الواردة باللائحة الأوربية([١]) وذلك على النحو التالي:

[أ] الحق في العلم والوصول للبيانات الشخصية محل المعالجة

يعني حق الشخص المعني في العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها، نص المشرع على هذا الحق ولم يورد كيفية العلم وكيفية وصول البيانات للمتحكم أو الحائز أو المعالج، كما أن المشرع لم يحدد هل يجب إخطار الشخص المعني بالبيانات بأن بياناته قيد المعالجة واطلاعه عليها، ولم يحدد كذلك طريقة اخطار الشخص المعني، وقد يكون المشرع قد ترك ذلك للائحة التنفيذية في أن تحدد ضوابط تحقق العلم وبياناته وعناصره، لذا يجب تحديد سبب وجود المعلومات الشخصية لدى

([١]) ينص الفصل الثالث من اللائحة الأوربية لحماية البيانات على حقوق صاحب البيانات وذلك في المواد من ١٢: ٢٣ .

www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

الحائز وكيفية اطلاع صاحب البيانات عليها. كما أشار المشرع حق الشخص المعني في الوصول لبياناته الشخصية والاطلاع عليها والحصول على نسخة منها بصيغة واضحة ومطابقة للمضمون([1]). عرفت المادة الرابعة من النظام السعودى الحق في العلم بأنه إحاطة الشخص المعني علما بالمسوغ النظامي لجمع بياناته الشخصية والغرض من جمعها. كما أشارت ذات المادة لحق الشخص المعني في الوصول إلى بياناته الشخصية المتوافرة لدى جهة التحكم، وفق الضوابط والإجراءات التي تحددها اللوائح. كما أشارت لحقه في طلب الحصول على بياناته الشخصية المتوافرة لدى جهة التحكم بصيغة مقروءة وواضحة، وفق الضوابط والإجراءات التي تحددها اللوائح.

وضعت اللائحة الأوربية في القسم الثاني والخاص بعلم صاحب البيانات تحت عنوان المعلومات والوصول للبيانات الشخصية حيث تشير([2]) المادة ١٣ إلى المعلومات التي يجب تقديمها عند جمع البيانات الشخصية من صاحب البيانات، وتنص المادة ١٤ على المعلومات التي يجب تقديمها عندما لا يتم جمع البيانات الشخصية من صاحب البيانات، كما تنص المادة ١٥ على حق الوصول لصاحب البيانات([3]).

([1]) **فهد بن عايد الشمري**: المرجع السابق- ص١٦٦١.

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

([3]) أشارت المحكمة الأوربية لحقوق الإنسان على التزام الدولة بمنح الشخص الحق في الوصول لمعلوماته بطريقة فعالة وسهلة وميسرة وفي غضون فترة زمنية معقولة واعتبرت مخالفة ذلك انتهاكا للمادة ٨ من الاتفاقية الأوربية لحقوق الإنسان.

CtHR, Haralambie v. Romania, No. 21737/03, 27 October 2009

[ب] الحق في محو البيانات:

أكدت التشريعات على حق الشخص المعني في طلب محو البيانات الخاصة به، وهو ما أشارت إليه المادة الثانية من القانون ١٥١ لسنة ٢٠٢٠ فيجب محو البيانات دون تأخير خاصة؛ إذا لم يعد هناك حاجة إلى تخزينها أو الاحتفاظ بها من جانب الشخص المختص، وهو ما يعرف في النظام السعودى في المادة ١١ بالحق في اتلاف البيانات لانعدام الحاجة إليها وأن وجودها لدى الحائز أصبح دون مقتضي فقد انتهي الهدف الذي جمعت وعولجت من أجله ومن ثم يجب أن تتلف تلك البيانات دون تأخير([1])، وكذلك إذا سحب موافقته السابقة على أن تكون الموافقة المسبقة تتعلق بما سبق من معالجة، فالأساسي القانوني كان هو قبول المعالجة وأن قد عدل عن موافقته، أو إذا كانت المعالجة لأسباب تتعلق بالصالح العام وقد انتهت الأسباب التي نشأت من أجلها، ويجب ألا يتم تخزين تلك البيانات إلا إذا دعت الضرورة لذلك سواء كانت لمصلحة عامة مثل حماية المجتمع من مرض خطير أو للطب الوقائي، وعلى مركز حماية البيانات الشخصية توقيع جزاءات وغرامات على المعالج الذي لا يلتزم بذلك، ومن حق الشخص المعني بالبيانات أن يلجأ للطرق القانونية في حالة عدم تنفيذ طلبه.

([1]) **طارق جمعه السيد راشد**: الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والقانون المقارن– المجلة القانونية والقضائية – وزارة العدل مركز الدراسات القانونية والقضائية– ع٢–٢٠١٧– ص٣٣، **فهد بن عايد الشمري**: المرجع السابق– ص١٦٦٥، **ميادة مصطفي المحروقي**: المرجع السابق– ص١٥٢٢.

ويشير البعض([1]) إلى أن الحق في المحو يثير العديد من المشاكل فهو ليس مطلق كونه يتداخل مع الحق في حرية التعبير والوصول إلى المعلومات وعليه فإنه يجب وضع معايير لاستخدام هذا الحق لإجراء التوازن بين الحق في الخصوصية وحرية الجمهور للوصول للمعلومات وحرية التعبير.

تنص المادة ١٧ من اللائحة الأوربية على حق الشخص المعني في محو البيانات الشخصية الخاصة به([2]): [١] يحق لصاحب البيانات أن يحصل من المراقب على محو البيانات الشخصية المتعلقة به، دون تأخير غير مبرر، ويلتزم المراقب بمحو هذه البيانات الشخصية دون تأخير لا مبرر له.

[ج] الحق في تخصيص المعالجة في نطاق محدد:

تنص المادة الثانية على حق الشخص المعني في تخصيص المعالجة في نطاق محدد، فقد يقرر الشخص المعني معالجة بياناته الشخصية بغرض التسويق الالكتروني المباشر، حيث نص المشرع في الفصل الثامن من القانون ١٥١ لسنة ٢٠٢٠ خاصة بالتسوق الالكتروني ووضع شروط خاصة لذلك حيث نصت المادة ١٧ على أنه يحظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص

([1]) **محمد أحمد سلامة مشعل**: الحق في محو البيانات الشخصية – دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوربي وأحكام المحاكم الأوربية – مجلة الدراسات القانونية والاقتصادية- جامعة مدينة السادات – ع٢- ٢٠١٧- ص٤١، **يحيى إبراهيم دهشان**: الحماية الجنائية للبيانات في ظل التحول الرقمي- مجلة الدراسات القانونية والاقتصادية- جامعة مدينة السادات- ع٣- ٢٠٢٣- ص١٥٢٠.

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

المعني بالبيانات، إلا بتوافر الشروط الآتية: [١] الحصول علي موافقة من الشخص المعني بالبيانات. [٢] أن يتضمن الاتصال هوية منشئه ومرسله. [٣] أن يكون للمرسل عنوان صحيح وكاف للوصول إليه. [٤] الإشارة إلي أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر. [٥] وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته علي إرسالها .

كما تنص المادة ١٨ من ذات القانون على أنه: يلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر بالالتزامات الآتية: [١] الغرض التسويقي المحدد، [٢] عدم الإفصاح عن بيانات الاتصال للشخص المعني بالبيانات، [٣] الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها أو عدم اعتراضه علي استمراره، بشأن تلقي الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال، وتحدد اللائحة التنفيذية القواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر. كما تنص الديباجة الخاصة باللائحة الأوربية على أنه عندما تتم معالجة البيانات الشخصية لأغراض التسويق المباشر، يجب أن يكون لصاحب البيانات الحق، في أي وقت ومجانًا، في الاعتراض على هذه المعالجة، بما في ذلك التنميط إلى الحد الذي يتعلق به مثل هذا التنقيب، سواء كان العلاج الأولي أو اللاحق. وينبغي لفت انتباه صاحب البيانات بشكل صريح إلى هذا الحق وتقديمه بشكل واضح ومنفصل عن أي معلومات أخرى. وعليه فإن الشخص المعني بالبيانات من حقه حال معالجة بياناته في التسوق الالكتروني المباشر على أن يقوم الحائز للبيانات بالالتزام بالقواعد التي نص عليها القانون.

[د] الحق في تقييد المعالجة:

وضعت المادة ١٨ من اللائحة الأوربية على الحق في تقييد المعالجة (Droit à la limitation du traitement) قواعد بشأن تقييد المعالجة فلصاحب البيانات الحق في طلب تقييدها بدلاً من محوها وفي هذه الحالة لا يجوز معالجتها واستثنت التخزين وبموافقة صاحب البيانات ولحماية البيانات الشخصية أو لإنشاء أو ممارسة أو الدفاع عن الحقوق القانونية أو لحماية حقوق شخص طبيعي أو اعتباري آخر، أو لأسباب مهمة تتعلق بالمصلحة العامة للاتحاد أو دولة عضو، ويجب إبلاغ صاحب البيانات بما تم حيال بياناته وقبل رفع تقييد المعالجة([1]).

كما تشير المادة ١٩ من اللائحة إلى التزام المراقب بإخطار المستلم «destinataire» المشار إليه بالمادة ٩/٤ من اللائحة الأوربية (ويعني الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الخدمة أو أي هيئة أخرى تتلقى اتصالات البيانات الشخصية، سواء كانت طرفًا ثالثًا أم لا. ومع ذلك، فإن السلطات العامة التي قد تتلقى بيانات شخصية في سياق مهمة معينة لتقصي الحقائق وفقًا لقانون الاتحاد أو قانون دولة عضو لا تعتبر مستلمة؛ تتوافق معالجة هذه البيانات من قبل السلطات العامة المعنية مع قواعد حماية البيانات المعمول بها اعتمادًا على أغراض المعالجة) بأى تصحيح أو ومحو للبيانات أو تقييد المعالجة، مالم يثبت استحالة اخطاره أو يقوم بجهد متناسب لتزويد صاحب البيانات بمعلومات عن المستلمين.

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

[د] الحق في منع نقل البيانات للآخرين

يقصد بمنع نقل البيانات للآخرين هو التزام الجهة القائمة بأعمال المعالجة بعدم منح الآخرين البيانات الشخصية الخاصة بالشخص المعني دون موافقة مسبقة منه، فالشخص المعنى قد وافق على قيام المتحكم والمعالج بالاطلاع على بياناته الشخصية واتخاذ الإجراءات التقنية والتنظيمية بشأنها فلا يجوز منحها للآخرين. تنص المادة ١٤ من القانون ١٥١ لسنة ٢٠٢٠ على البيانات الشخصية عبر الحدود على أنه يحظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلي دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوي من الحماية لا يقل عن المستوي المنصوص عليه في هذا القانون، وبترخيص أو تصريح من المركز. وتحدد اللائحة التنفيذية السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها.

وجاءت المادة ١٥ من ذات القانون لتضع استثناءات على النقل حيث تنص على أنه: استثناءً من حكم المادة (١٤) من هذا القانون، يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلي دولة لا يتوافر فيها مستوي الحماية المشار إليها في المادة السابقة ، وذلك في الحالات الآتية: [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 دول. [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 طرفًا فيه .

تنص المادة ٢٠ من اللائحة الأوربية على الحق في إمكانية نقل البيانات (Droit à la portabilité des données) وكذا القواعد الخاصة بحق الشخص المعني في نقل البيانات من وحدة تحكم لأخري([1]). كما أشارت الفقرة ١٠٢ من الديباجة الخاصة بالاتفاقية إلى أنه يجوز إبرام اتفاقيات بشأن تنظيم نقل البيانات على أن يتوافر مستوى مناسب من الحماية([2]). وكانت المفوضية الأوربية قد سمحت للشركات الأميركية التي تلتزم بالمبادئ وتسجل شهاداتها وتستوفي متطلبات الاتحاد

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

([2]) قضت محكمة العدل الأوربية أن قيام هيئة إدارية عامة بنقل بيانات شخصية إلى هيئة أخري يجب أن يتم النقل بعد إخطار الشخص المعني.

CJEU, C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others, 1 October 2015, paras. 28-46

الأوروبي، بنقل البيانات من الاتحاد الأوروبي إلى الولايات المتحدة. ويشار إليه ب"قرار الملاذ الآمن"(the Safe Harbor decision) أثار مشكلات قانونية([1]).

حدد حكم محكمة العدل الأوربية شروط يجب استيفائها لنقل البيانات هي([2]): [١] يجب على الطرف الثالث الذي يتم الكشف له عن البيانات أن يسعى إلى تحقيق مصلحة مشروعة، يعني هذا أن طلب المعلومات الشخصية لمقاضاة شخص ما لتسببه في إتلاف الممتلكات يشكل مصلحة مشروعة لطرف ثالث، [٢] يجب أن تكون معالجة البيانات الشخصية ضرورية لأغراض المصالح المشروعة التي يسعى إليها، يعد الحصول على معلومات شخصية مثل العنوان و/أو رقم الهوية ضروريًا تمامًا لتحديد هوية ذلك الشخص، [٣] يجب موازنة المصالح على أساس كل حالة على حدة، مع مراعاة عناصر مثل شدة انتهاك حقوق موضوع البيانات أو حتى سن موضوع البيانات في ظروف معينة.

مما سبق يتضح أن المشرع المصري لم يمنح الشخص المعني بالبيانات الحق في نقل بياناته الشخصية من متحكم إلى آخر داخل الدولة؛ ولكنه ربط هذا الحق بأن

([1]) قضت محكمة العدل الأوربية إلى أن وجود قرار من المفوضية يسمح بنقل البيانات لدولة أخري لا يلغي صلاحيات السلطات الاشرافية الوطنية في فحص شكوى بشأن مراقبة وضمان الامتثال لقواعد الاتحاد الأوربي بشأن حماية البيانات بموجب قرار الاتحاد الأوربي.

CJEU, C-362/14, Maximilliam Schrems v. Data Protection Commissioner [GC], 6 October 2015.

([2]) CJEU, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme', 4 May 2017.

يتم النقل عبر الحدود فمنح الشخص المعني الحق في نقل بياناته الشخصية وحددها بعدد من الحالات المستثناة كما سبق وذكرنا، وترك للائحة التنفيذية للقانون تحديد السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها.

[م] الحق في الاعتراض:

تنص المادة ٦/٢ من القانون ١٥١ لسنة ٢٠٢٠ على الحق في الاعتراض حيث تنص على أن الاعتراض يكون علي معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية، ويعتبر الحق في الاعتراض تطبيقاً لحق الشخص في احترام حرياته الأساسية وهي وسيلة فعالة لإعلان رفضه لأى إجراء يتعلق ببياناته الشخصية([1])، ولا يعتبر القبول المسبق للشخص على إجراء المعالجة لبياناته ألا يحق له الاعتراض اللاحق على تلك المعالجة. فقد يتم الاعتراض في مرحلة من مراحل المعالجة وذلك برفضه جمع بياناته أو معالجتها أو نقلها([2]).

([1]) **Sulliman OMARJEE** : Le data mining, Aspects juridiques de l›itelligenceartificielle au regard de la protection des donnéespersonnelles ،mémoire , faculté de droit , universitémontpellier I , Annéeuniversitaire 2001/2002 , et disponiblesurwww.droit-ntic.com, p.33.

([2]) **ميادة مصطفي المحروقي**: المرجع السابق- ص١٥٣٢.

تنص المادة ٢١ من اللائحة الأوربية على هذا الحق([1])، حيث تنص على حق صاحب البيانات الاعتراض في أي وقت، لأسباب تتعلق بوضعه الخاص، على معالجة البيانات الشخصية المتعلقة به ومن ثم لا يجوز للمراقب معالجة البيانات الشخصية ما لم يثبت أسبابًا مشروعة مقنعة للمعالجة التي تتجاوز مصالح وحقوق وحريات صاحب البيانات، أو لإنشاء الحقوق القانونية أو ممارستها أو الدفاع عنها. عندما تتم معالجة البيانات الشخصية لأغراض التسويق المباشر، يحق لصاحب البيانات الاعتراض في أي وقت على معالجة البيانات الشخصية المتعلقة به لأغراض التسويق المباشر وإذا اعترض صاحب البيانات على المعالجة لأغراض التسويق المباشر، فلن تتم معالجة البيانات الشخصية لهذه الأغراض، وعندما تتم معالجة البيانات الشخصية لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية يحق لصاحب البيانات الاعتراض، لأسباب تتعلق بوضعه الخاص، على معالجة البيانات الشخصية المتعلقة به، ما لم تكن المعالجة ضرورية لأداء مهمة ذات مصلحة عامة.

تشير الفقرة ٦٩ من الديباجة الخاصة باللائحة الأوربية إلى أنه عندما يمكن معالجة البيانات الشخصية بشكل قانوني لأن المعالجة ضرورية لأداء مهمة يتم تنفيذها لتحقيق المصلحة العامة أو في ممارسة السلطة العامة المخولة للمراقب، أو بسبب المصالح المشروعة للمراقب أو لطرف ثالث، ومع ذلك، يجب أن يكون لأصحاب البيانات الحق في الاعتراض على معالجة أي بيانات شخصية تتعلق

([1]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

بوضعهم الخاص. يجب أن يتحمل المراقب عبء إثبات أن مصالحه المشروعة المقنعة تتجاوز المصالح أو الحقوق والحريات الأساسية لصاحب البيانات.

[هـ] الحق في التعديل والتصحيح:

يحق للشخص المعني بالبيانات أن يطلب من المعالج تعديل بياناته أو الغائها إذا كانت غير صحيحة، ذلك أن البيانات بطبيعتها خاضعة للتغيير بسبب ما قد يشوب عملية الجمع والرصد والتسجيل من أخطاء غير مقصودة، لذا يحق لصاحب البيانات طلب تصحيح تلك البيانات، أو تكون البيانات ناقصة فيطلب صاحب البيانات استكمال النواقص من البيانات أو تعديلها إذا حدث تغيير في البيانات([1])، على أن يتم ذلك مع مراعاة أغراض المعالجة، ولم تحدد التشريعات المدة الزمنية لحق التصحيح وتفرض عبارة مدة زمنية معقولة([2]).

تنص المادة الثانية من القانون ١٥١ لسنة ٢٠٢٠ على هذا الحق وهو الحق في التصحيح أو التعديل أو إضافة بيانات جديدة أو تحديث البيانات، ومن ثم يحق للشخص المعني بالبيانات التأكد من صحة بياناته وسلامتها وعدم وجود أخطاء بها، كما تنص المادة ٤/٥ بشأن التزامات المعالج على أن محو البيانات الشخصية من قبله يكون بعد انقضاء مدة المعالجة أو تسليمها للمتحكم.

([1]) **فهد بن عايد الشمري**: المرجع السابق- ص١٦٦٣.

قضت محكمة العدل الأوربية بحق صاحب البيانات من التأكد من صحة البيانات ودقتها.

CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer، 7 May 2009.

([2]) **ميادة مصطفي المحروقي**: المرجع السابق- ص١٥٢٢.

تنص المادة ١٦ من اللائحة الأوربية على الحق في التصحيح (Droit de rectification) حيث تنص على أنه يحق لصاحب البيانات أن يحصل من المراقب، في أقرب وقت ممكن، على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به. مع الأخذ في الاعتبار أغراض المعالجة، يحق لصاحب البيانات إكمال البيانات الشخصية غير المكتملة، بما في ذلك عن طريق تقديم بيان تكميلي([1]).

تنص المادة الثامنة من النظام السعودى على الحق في طلب تصحيح البيانات الشخصية حيث تنص على أن: [١] لصاحب البيانات الشخصية طلب تصحيح بياناته الشخصية إذا كان المسوغ النظامي للمعالجة الموافقة أو المصلحة المشروعة أو تنفيذ اتفاق يكون صاحب البيانات الشخصية طرفا فيه. [٢] يجوز لصاحب البيانات الشخصية في حال عدم صحة بياناته الشخصية المتوافرة لدى جهة التحكم أن يطلب تقييد معالجة بياناته لمدة يمكن لجهة التحكم خلالها التحقق من صحة البيانات الشخصية، مع مراعاة عدم سريان حق صاحب البيانات الشخصية في الحصول على التقييد المذكور إذا كان تقديم تلك البيانات يتعارض مع أحكام النظام واللوائح. [٣] يكون لجهة التحكم طلب المستندات أو الوثائق الداعمة لطلب تصحيح

([1]) **Julien Le CLAINCHE**: la protection des donnéespersonnelles nominatives dans le cadre de la recherchedans le domaine de la santé , comparaison du droitfrançais et américain , mémoire de D.E.A , Faculté de droit , des sciences économiques et de gestion , univmontpellier I , et disponiblesurwww. droit-ntic.com , la date de mise en ligneest : 30 / 6 / 2001, p 3.

البيانات الشخصية متى ما كان ذلك ضروريا لتحديث أو تصحيح أو إتمام البيانات الشخصية، على أن يتم إتلاف تلك المستندات أو الوثائق بعد الانتهاء من عملية التحقق.

المطلب الثالث

تعويض الأضرار الناتجة عن المعالجة الخاطئة للبيانات

يصنف البعض([1]) قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠ بأنه من ضمن القوانين العقابية إذ يركز على ارتكاب الجرائم الواردة فيه؛ على الرغم من كونه قانون حمائى في المقام الأول هدفه الوقاية والمنع وليس الزجر والردع عبر تنظيم دقيق لمظاهر حماية البيانات الشخصية، ونري أن القانون قد جمع بين الهدفين فهو يهدف للحماية والمنع وأيضاً الزجر والردع باعتبار أن المشرع المصري قد وضع قوانين أساسية عامة، وترك القوانين المكملة للدستور تنظم كافة الأحداث والظواهر اللاحقة التي يتطلبها المجتمع، كما أن الطابع العام للقواعد القانونية أنها يجب أن تشمل الجزاء المادى حتى يمكن محاسبة المسئول. كما تنص اللائحة الأوربية في المادة ٨٤ على عقوبات توقع على المخالف([2]) حيث تنص على أنه: [١] تحدد الدول الأعضاء نظام العقوبات الأخرى المطبقة في حالة انتهاك هذه اللائحة، ولاسيما الانتهاكات التي لا تخضع للغرامات الإدارية المنصوص عليها في المادة ٨٣([3])،

([1]) راجع في ذلك **الدراسة النقدية** سابق الاشارة إليها– ص٢٦.

([2]) www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

([3]) أشارت المادة ٨٣ من اللائحة الأوربية إلى فرض غرامات إدارية ويجب أن تكون فعالة ومتناسبة ورادعة ويراعي فيها طبيعة الانتهاك وشدته ومدته ونطاقه ومستوى الضرر الواقع على الأشخاص المضرورين، وعما إذا كانت المخالفة ارتكبت عن عمد أو اهمال، وعما إذا كانت الجهة

وتتخذ جميع التدابير اللازمة لضمان تنفيذها. وأن تكون هذه العقوبات فعالة ومتناسبة ورادعة. [٢] يجب على كل دولة عضو إخطار اللجنة بالأحكام القانونية التي تعتمدها([١]). وقد أشارت اللائحة إلى مسئولية المتحكمين والمعالجين عن المعالجة غير القانونية وحق الأشخاص في طلب التعويض عن الأضرار المادية والمعنوية وأن مفهوم الضرر يجب تفسيره في ضوء أحكام محكمة العدل الأوربية، فإذا خالفوا الالتزامات الواردة باللائحة وتصرفوا خارج نطاق التعليمات كانوا ملزمين بالتعويض.

ومن المعروف أن حيث وضع القانون فلسفة تشريعية مزدوجة فهو يهدف لردع مرتكبي الجريمة وتجريم كافة أشكاله، وفرض عقوبات على جميع الأطراف المتورطة في الجريمة، وكذا حماية ضحايا تلك الجريمة من خلال تقديم المساعدة القانونية اللازمة وتيسير سبل اندماجهم في الحياة الاجتماعية؛ وتعافيهم من الضرر الجسدي والنفسي الذي أحاط بهم – هذا بخلاف القوانين الجنائية التي تستهدف تجريم مجموعة من الأفعال ووضع عقوبات لها – أما هذا القانون فإنه يهدف إلى وضع مواجهة شاملة مع تلك الظاهرة بهدف الوقاية والحماية وتقديم المساعدة للضحايا إلى جانب ملاحقة ومحاكمة مرتكبيها داخلياً وخارجياً([٢]).

المخالفة قد اتخذت تدابير للتخفيف من الأضرار ودرجة المسئولية، وعما إذا كان قد سبق له ارتكاب مخالفات مماثلة ودرجة تعاونها مع السلطات المشرفة في معالجة الانتهاك وتخفيف آثاره السلبية.

([١]) نص الدليل الأوربي على حق أصحاب البيانات في تقديم شكوى بشأن حدوث انتهاكات للائحة الأوربية بشأن حماية البيانات الشخصية وممارس حقهم في طلب تعويض عن الأضرار.

Handbook on European, data protection law, 2018 editio

([٢]) **خالد مصطفي فهمي**: النظام القانوني لمكافحة جرائم الاتجار بالبشر- دار الفكر الجامعي- الإسكندرية – ٢٠١١- ص١٥٤، يشير البعض إلى أن المشرع عندما ينظم جرائم لصيقة بالإنسان

يشير القانون ١٥١ لسنة ٢٠٢٠ على حق الشخص المضرور في طلب التعويض، فيحق لكل شخص اعتدى على بياناته الشخصية أن يطلب التعويض عن الضرر الذي لحق به من جراء هذا الاعتداء حيث تنص المادة ٣٥ على أنه: مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر، ومع عدم الإخلال بحق المضرور في التعويض، يعاقب علي الجرائم المنصوص عليها في المواد التالية بالعقوبات المقررة لها. كما تنص المادة ٨٢ من اللائحة الأوربية على الحق في التعويض والمسؤولية([1]). والتعويض هو التزام يفرضه القانون على محدث الضرر

فهو يحمي الشخصية الإنسانية– **فوزية عبد الستار**: شرح قانون العقوبات القسم الخاص– دار النهضة العربية– القاهرة– ٢٠٠٠– ص٣٥١.

([1]) حيث تنص على حق أي شخص أصيب بضرر مادي أو معنوي نتيجة مخالفة هذه اللائحة الحصول على تعويض وأن أي مراقب بيانات شارك في المعالجة يكون مسؤولاً عن الأضرار الناجمة عن المعالجة والتي تشكل انتهاكًا لهذه اللوائح. يتحمل المقاول من الباطن المسؤولية فقط عن الأضرار الناجمة عن المعالجة إذا لم يمتثل للالتزامات المنصوص عليها في هذه اللائحة والتي تقع على عاتق المقاولين من الباطن على وجه التحديد أو إذا تصرف خارج الأغراض القانونية للمراقب أو يتعارض معها. كما يُعفى المراقب أو المقاول من الباطن من المسؤولية إذا أثبت عدم نسبة الضرر إليه، وفي حالة مشاركة العديد من وحدات التحكم أو المعالجات أو حيث يشارك كل من وحدة التحكم والمعالج في نفس المعالجة، يكونان مسؤولين عن الأضرار الناجمة عن المعالجة، يكون كل من وحدات التحكم أو المقاولين من الباطن مسؤولاً عن الضرر بأكمله وذلك لضمان تعويض فعال للشخص المعني. وعندما يقوم مراقب البيانات أو المقاول من الباطن بإصلاح الضرر الذي لحق به بالكامل، يحق له المطالبة من مراقبي البيانات الآخرين أو المقاولين من الباطن الذين شاركوا في نفس المعالجة بحصة الإصلاح المقابلة لحصتهم من المسؤولية عن الضرر، وتُرفع الإجراءات القضائية المتخذة لممارسة الحق في الحصول على التعويض إلى المحاكم المختصة بموجب قانون الدولة العضو.

لأنه بخطئه سبب ضرراً للغير ولذا يلتزم بجبر الضرر. وهذا لا يمنعه من طلب وقف الاعتداء الواقع عليه ومنع الانتهاك وطلب التعويض عن الأضرار، وتتمثل حقوق الشخص المعنى بالبيانات في هذا الموضع في:

أولاً: الحق في وقف الاعتداء على البيانات الشخصية

ودون الخوض في المسئولية الجنائية الواردة بالقانون(١) واللائحة الأوربية، والتي تنشأ عن انتهاك البيانات الشخصية فإن أي اعتداء يقع على البيانات الشخصية يتطلب وقف الاعتداء وفقاً لنص المادة ٥٠ من القانون المدني والتي تنص على أن: لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر، وعليه فإن الاعتداء على البيانات الشخصية يمنح الشخص حق طلب وقف هذا الاعتداء أو الانتهاك ومنعه(٢)، ويعني وقف الاعتداء تحقيق الأمن والطمأنينة والاستقرار للفرد

---

www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données - RGPD

(١) تنص المادة (٤١) من القانون ١٥١ لسنة ٢٠٢٠ على أنه: يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل حائز أو متحكم أو معالج جمع أو أتاح أو تداول أو عالج أو أفشي أو خزن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو في غير الأحوال المصرح بها قانونًا . يشير البعض إلى أن المسئولية الجنائية تستهدف حماية المجتمع ضد الجريمة بينما المسئولية المدنية تستهدف تعويض وجبر الضرر- **حسام الدين كامل الأهواني**: مصادر الالتزام- دار النهضة العربية- القاهرة- بدون سنة نشر- ص٣١٦.

(٢) **حسام أحمد البهجي**: حماية الحق في حرمة الحياة الخاصة في ضوء حقوق الإنسان والمسئولية المدنية- دار الجامعة الجديدة- الاسكندرية- ٢٠٠٥- ص٣٩٠.

والتزام الدولة بحمايته وصيانته، حيث تعد القوانين الوضعية صمام الأمان؛ لحماية الحرية الشخصية للفرد من أي تجاوز أو اعتداء من قبل الآخرين، فالحرية ليس معناها أن يفعل الإنسان ما يشاء وكما يشاء ووقتما يشاء، ولكن الحرية تنتهي حينما تبدأ حرية الآخرين مع التقيد بعدم الإضرار بالآخرين وبأمن وطمأنينة المجتمع تحت مظلة رقابة قضائية مستقلة([1]).

تشير المادة ٣٤ من اللائحة الأوربية إلى أنه يجب اخطار الشخص المعني بالبيانات بخرق البيانات الشخصية له وضرورة اتخاذ كافة التدابير لمنع ذلك. كما تشير المادة ٣٠ من القانون ١٥١ لسنة ٢٠٢٠ إلى قيام مركز حماية البيانات الشخصية بإنذار المخالف للتوقف عن المخالفة وإزالة أسبابها أو آثارها خلال فترة محددة.

كانت محكمة العدل الأوربية قد أشارت إلى أن اتفاقية الملاذ الأمن تعرض الحقوق الأساسية لمواطني الاتحاد الأوروبي في حماية الخصوصية وحماية البيانات الشخصية والحق في الحصول على تعويض قانوني فعال للخطر، وأضافت المحكمة أن التشريعات الأمريكية سمحت لبعض السلطات العامة بالوصول إلى البيانات الشخصية المنقولة من دول الاتحاد إلى الولايات المتحدة ومعالجتها بطريقة تتعارض مع أغراض نقلها الأصلية وتتجاوز ما هو ضروري تمامًا ومتناسب مع حماية الأمن القومي. وفيما يتعلق بالحق في علاج فعال، لاحظت أن أصحاب البيانات ليس لديهم

([1]) **أحمد عبد الحميد أمين**: التعويض عن الخطأ الشخصي لمأمور الضبط القضائي- بحث منشور بمجلة الحقوق- جامعة المنيا- ٢٠١٨/٦/١- ص٦٢٨.

أي وسيلة إدارية أو قضائية للانتصاف لتمكينهم من الوصول إلى البيانات المتعلقة بهم وتصحيحها أو محوها، حسب الاقتضاء([1]).

ثانياً: المسئولية المدنية عن انتهاك البيانات الشخصية

يقصد بالمسئولية المدنية مجموعة القواعد التي تلزم من ألحق ضرر بالغير بجبر هذا الضرر عن طريق التعويض([2])، وقد وضع المشرع التعويض كوسيلة فعالة لتحقيق العدالة والتوازن بين الضرر الذي وقع على الشخص المعنى نتيجة الاساءة لبياناته ومصلحته في جبر هذا الضرر إذا توافرت أركان المسئولية. قضت محكمة النقض أن استخلاص الخطأ الموجب للمسئولية والضرر وعلاقة السببية من سلطة محكمة الموضوع ولها السلطة التامة في تحصيل فهم الوقائع في الدعوى واستخلاص الخطأ الموجب للمسئولية والضرر وعلاقة السببية بينهم([3]). والمسئولية المدنية الناشئة عن انتهاك البيانات الشخصية قد تكون عقدية أو تقصيرية([4]):

([1]) CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015.

([2]) **اكرام سليمان قجم**: المرجع السابق- ص٤٣.

([3]) الطعن رقم ٨٣٢٠ لسنة ٨١ ق جلسة ٢٠١٥/٦/٢١.

([4]) تنشأ المسئولية العقدية عن الاخلال بالتزام عقدى ويختلف باختلاف العقد فإذ أدى الاخلال إلى وقوع ضرر على المتعاقد الآخر كان من أخل بالالتزام مسئول مسئولية عقدية، أما المسئولية التقصيرية فتنشأ عن الاخلال بالتزام قانوني عام هو الالتزام بعدم الاضرار بالغير- **عبد الرزاق السنهوري**: الوسيط في شرح القانون المدني- ج١ نظرية الالتزام بوجه عام- مصادر الالتزام- طبعة منقحة- منشأة المعارف – الإسكندرية- ٢٠٠٧- ص٥٦٢، **حسام الدين كامل الأهواني**: المرجع السابق- ص٣١٩.

[١] المسئولية العقدية عن الاخلال بعقد حماية البيانات الشخصية:

تنشأ المسئولية العقدية نتيجة علاقة عقدية صحيحة لوجود اتفاق بين الشخص المعنى بالبيانات ومتحكم أو معالج على القيام استخدام البيانات لغرض محدد فخالف ذلك ونتج عن العقد أضرار بالشخص المعني، باعتبار الإخلال بالعقد واقعة مادية متى توافرت شروط المسئولية العقدية من خطأ موجب للمسئولية من جانب المتعاقد الآخر وضرر وعلاقة سببية بين الخطأ والضرر، وأن المسئول قد تسبب بخطئه في هذا الضرر([١])، وعليه فإن للشخص المعني حق إبطال العقد والتعويض، حيث أن أساس كل منهما مختلف. ويشترط لقيام المسئولية العقدية وجود عقد صحيح واخلال أحد المتعاقدين بشرط من شروط العقد، فالمسئولية العقدية هي جزاء الاخلال بالالتزامات الناشئة عن العقد([٢])، ويري الدكتور السنهوري أن المادة ٢٢١ مدني مصري قد حددت المسئولية العقدية واختصت الحق في التعويض بأن يكون عن الضرر المتوقع فقط إلا في حالة الغش أو الخطأ الجسيم، فيجوز التعويض عن الضرر غير المتوقع، وأن المتعاقدان لم يبرما التعاقد إلا على ما يتوقعانه من ضرر، ومن ثم فالضرر غير المتوقع لا يدخل في دائرة التعاقد فلا تعويض عنه إلا إذا ارتكب المدين الغش أو الخطأ الجسيم فإنه يلتزم بالتعويض عن كافة الأضرار([٣]).

([١]) حكم محكمة النقض جلسة ١٩٧٠/٦/٢ طعن رقم ١٣٤ لسنة ٣٦ ق رقم ١٥٤ ص٩٦١.

([٢]) **جميل الشرقاوى**: النظرية العامة للالتزامات – مصدر الالتزام- دار النهضة العربية- القاهرة- ١٩٩١- ص٥٣٥.

([٣]) **عبد الرزاق السنهوري**: المرجع السابق- ص٥٦٢.

أركان المسئولية العقدية للمتحكم أو المعالج

الركن الأول – الخطأ العقدى: وهو قوام المسئولية المدنية فإذا انتفي الخطأ فلا مسئولية ولا تعويض([١])، ويعرف بأنه عدم قيام المدين بتنفيذ التزامه الوارد بالعقد([٢])، أى الانحراف عن السلوك المألوف للشخص أو مخالفة قاعدة قانونية([٣])، فالمتحكم أو المعالج يلتزم بحماية البيانات الشخصية للشخص المعني فإذا لم يقم بتنفيذ التزامه، يكون قد خالف العقد([٤])، ويستوى في ذلك أن يكون عدم القيام بتنفيذ الالتزام ناشئ عن خطأ أو عمد أو إهمال، بل يتحقق الخطأ العقدى ولو كان عدم تنفيذ الالتزام لسبب أجنبي، حيث يشير البعض([٥]) إلى أن الالتزام ينقضي إذا أثبت المدين أن الوفاء أصبح مستحيلاً لسبب أجنبي لا يد له فيه، فانقضاء الالتزام يكون نتيجة لاستحالة التنفيذ ولعدم تحقق المسئولية العقدية لانعدام أحد أركانها. ووفقاً للقواعد العامة يقع على المدين عبء إثبات عدم قيام الدائن بتنفيذ الالتزام أو الاخلال به.

([١]) عرفت محكمة النقض الخطأ بأنه: الانحراف الذي ينطوى على الخروج عن الواجب العام المفروض على الكافة والذي يوجب على الشخص أن يتبع في سلوكه اليقظة والتبصر حتى لا يضر بالغير – جلسة ١٩٨٥/١٢/١٩ طعن رقم ١٠٤١ لسنة ٥٢ ق مكتب فني ٣٦ ج٢ ص١١٤٧.

([٢]) **حسام الدين كامل الأهواني**: المرجع السابق– ص٣٢٢.

([٣]) **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية –المرجع السابق– ص٢٢.

([٤]) فتعريض البيانات الشخصية للابتزاز الالكتروني واختراق الحسابات والازعاج الالكتروني والحصول على معلومات حساسة عن الشخص المعني يمثل تهديداً بالغ الخطورة وتشويها له – **خالد سويلم محمد**: الحماية القانونية للبيانات الشخصية الالكترونية– المجلة القانونية – جامعة القاهرة– كلية الحقوق فرع الخرطوم– المجلد ١٤– العدد٦– نوفمبر ٢٠٢٢– ص ١٨٩١.

([٥]) **عبد الرزاق السنهوري**: المرجع السابق– ص٥٣٦ وما بعدها.

الركن الثاني – الضرر: القاسم المشترك في المسئولية هو الضرر الذي يتم التعويض عنه، حيث يعتبر وقوع الضرر بالشخص المعنى نتيجة خطأ المتحكم أو المعالج هو أساس وبداية تحقق المسئولية، يعرف الضرر بأنه الأذي الذي يلحق المضرور نتيجة خطأ الغير([1])، كما يعرف بأنه الاخلال بمصلحة محققة ومشروعة للمضرور([2])، ووفقاً للقواعد العامة للمسئولية فلا تعويض إلا مع تحقق الضرر، فلابد من وجود ضرر حتى تتحقق المسئولية، ويقع عبء إثبات تحقق الضرر على المضرور، فمتي تحقق الضرر يحق للمضرور المطالبة بالتعويض عن الضرر سواء كان ضرراً مادياً أو أدبياً([3])، حتى ولو كان هناك شرط جزائي في العقد فإنه لا يجوز التعويض ولا يستحق الشرط الجزائي إلا بإثبات تحقق الضرر (وفقاً لنص المادة ١/٢٢٤ من القانون المدني المصري)، حيث يلتزم الشخص المعني بإثبات أن الضرر يرجع إلى إخلال المدين بالالتزامات الواردة بالعقد والقانون أى الالتزام بإثبات عدم قيام المتحكم أو المعالج بحماية البيانات الشخصية([4]). وأن الضرر قد وقع فعلاً أو محقق الوقوع أما الضرر المحتمل الوقوع فلا يستحق عنه التعويض([5]).

([1]) **عمر عبد الفتاح السيد**: التوازن المعرفي في العقود المدنية- رسالة دكتوره- كلية الحقوق – جامعة طنطا- ٢٠١٨- ص٢٧٩.

([2]) **حسام الدين كامل الأهواني**: المرجع السابق- ص٣٣٨.

([3]) راجع أركان المسئولية العقدية لدى- **عبد الرزاق السنهوري**: المرجع السابق- ص٥٥٦ وما بعدها، **حسام الدين كامل الأهواني**: المرجع السابق- ص٣٣٧ وما بعدها.

([4]) **عمر عبد الفتاح السيد**: المرجع السابق- ص٢٨٠.

([5]) **خالد مصطفي فهمي**: طبيب التجميل (ماهية العمل التجميلي- طبيعته القانونية- المسئولية المدنية وتعويض الأضرار)- دار الفكر الجامعي- الاسكندرية- ص٢٢٥.

الركن الثالث – علاقة السببية بين الخطأ والضرر: يجب أن يكون الخطأ هو السبب في الضرر([1])، فقد يكون هناك خطأ من المعالج أو المتحكم، وقد يكون هناك ضرر لحق بالشخص المعنى، دون أن يكون الخطأ هو السبب في تحقق الضرر، ويقع على المعالج أو المتحكم عبء نفي توافر رابطة السببية بأن يثبت وجود سبب أجنبي أو خطأ الغير أو خطأ المضرور هو السبب في تحقق الضرر. قضت محكمة النقض بأنه([2]): لا يكفي أن يكون هناك خطأ من الشخص بل يلزم أن يكون الضرر نتيجة حتمية ولازمة لهذا الخطأ ولولاه ما وقع الضرر. وتعددت النظريات التي تناولت كيفية التحقق من علاقة السببية أو انتفائها، ولكن وفقاً لما استقر عليه الفقه والقضاء فإن ركن السببية في المسئولية المدنية لا يقوم إلا على السبب المنتج الفعال المحدث للضرر دون السبب العارض الذي ليس من شأنه بطبيعته إحداث مثل هذا الضرر مهما كان قد أسهم مصادفة في إحداثه بأن كان مقترناً به([3]). قضت محكمة النقض بأن([4]): قيام رابطة السببية بين الخطأ والضرر وعدم قيامها من المسائل الموضوعية التي يفصل فيها قاضي الموضوع بغير معقب مادام حكمه مؤسساً على أسانيد مقبولة مستمدة من وقائع الدعوى. كما قضت محكمة النقض بأن([5]) لمحكمة الموضوع سلطة

([1]) **حسام الدين كامل الأهواني**: المرجع السابق– ص٣٩٣.

([2]) طعن رقم ٤٣٦ لسنة ٢٢ق جلسة ١٩٥٦/٦/١٤ مكتب فني٧– ج٢.

([3]) **عبد الرازق السنهوري**: المرجع السابق– ص٩٠٥ وما بعدها، طعن رقم ٨٤٨ لسنة ٦٨ ق – جلسة ١٩٩٩/١٢/٧– مكتب فني ٥٠ – جزء ٢ – ص١٢٤١.

([4]) طعن رقم ١٢٠٢ لسنة ٢٢ ق جلسة ٢٥/ ١١/ ١٩٥٢ مكتب فني ٤ ج ١ ص١٦٩.

([5]) الطعن ٩٥٤٢ لسنة ٩١ ق جلسة ١٦ / ٣ / ٢٠٢٢ مكتب فنى ٧٣ ق ٦٣ ص ٥٠٧

سلطة استخلاص توافر الخطأ الموجب للمسئولية والضرر وعلاقة السببية بينهما، ولا رقابة عليها في ذلك من محكمة النقض طالما جاء استخلاصها سائغًا، وحسبها أن تبين الحقيقة التي اقتنعت بها وأن تقيم قضاءها على أسباب تكفي لحمله. وعليه لابد من تحقق المسئولية المدنية بأركانها الثلاث، وأن تعويض الضرر كان بسبب ارتباط الخطأ بالضرر برابطة السببية([1]).

[٢] المسئولية التقصيرية للمسئول عن الاضرار بالشخص المعني

تقع المسئولية التقصيرية في الحالات التي لا يتوافر فيها شروط المسئولية العقدية([2])، فإذا خالف شخص شروط مشروعية معالجة البيانات الشخصية فإنه يكون مرتكباً لخطأً تقصيرياً هو معالجة البيانات الشخصية بطريقة غير مشروعة ومن ثم يلتزم بتعويض الشخص المعنى الذي تمت معالجة بياناته إذا ترتب على فعله إصابة صاحب البيانات بضرر([3]). كذلك تنعقد المسئولية إذا قام بتجميع البيانات دون علم صاحبها أو دون غاية محددة أو لغاية غير مشروعة أو من يقوم بتخزين البيانات أكثر من المدة اللازمة إذا ترتب عن أى من ذلك ضرر لمن تم تجميع بياناته. وقد يكون الخطأ التقصيري في حالة اختراق البيانات الشخصية والتشهير بصاحبها وابتزازه ونشر الصور والبيانات الشخصية، فهذا يعتبر اخلالاً بواجب قانوني عام هو عدم

([1]) **عادل جبري حبيب**: المفهوم القانوني لرابطة السببية وانعكاساته في توزيع عبء المسئولية المدنية – دار الفكر الجامعي– الاسكندرية– ٢٠٠٣– ص٢٤١.

([2]) **حسام الدين كامل الأهواني**: المرجع السابق– ص٣٢٤، كما يشير إلى أن القضاء الفرنسي يعتبر المسئولية تقصيرية في حالة التعسف في استعمال الحق حتى لو كان الحق ناشئاً عن عقد.

([3]) **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية –المرجع السابق– ص٢٢.

الاضرار بصاحب البيانات الشخصية([١]). والتعويض مقياسه هو الضرر المباشر الذى أحدثه الخطأ ويشتمل هذا الضرر على عنصرين جوهريين هما الخسارة التى لحقت المضرور والكسب الذى فاته وهذان العنصران هما اللذان يقومهما القاضي بالمال على ألا يقل عن الضرر أو يزيد عليه متوقعاً كان هذا الضرر أو غير متوقع متى تخلف عن المسئولية التقصيرية([٢]).

وقد يستند المضرور للخطأ العقدى أو للخطأ التقصيري الناتج عن عمل المعالج أو المتحكم فإذا استند لوجود خطأ تقصيري ثم تبين أن هناك عقد مع المسئول فلا غبار عليه إذا استند إليه، قضت محكمة النقض بأن([٣]) حق المضرور في التعويض منشأه جواز الاستناد إلي الخطأ العقدي ولو لأول مرة أمام محكمة الاستئناف ورغم الاستناد إلي الخطأ التقصيري فلمحكمة الموضوع أن تستند إلي الخطأ العقدي من تلقاء نفسها ولا يعتبر ذلك تغييراً لسبب الدعوي، حق المضرور فى التعويض إنما ينشأ إذا كان من أحدث الضرر أو تسبب فيه قد أخل بمصلحة مشروعة للمضرور فى شخصه أو فى ماله مهما تنوعت المسائل التى يستند إليها فى تأييد طلب التعويض فيجوز للمضرور رغم استناده إلى الخطأ التقصيرى الثابت أو المفترض أن يستند إلى الخطأ العقدى ولو لأول مرة أمام محكمة الاستئناف كما يجوز لمحكمة الموضوع رغم ذلك أن تستند فى حكمها بالتعويض إلى الخطأ العقدى متى ثبت لها

([١]) **اكرام سليمان قجم:** المرجع السابق- ص٨٥.

([٢]) **سامح عبد الواحد التهامي:** ضوابط معالجة البيانات الشخصية -المرجع السابق- ص٢٢.

([٣]) طعن رقم ١٤٩ لسنة ٣٠ ق – جلسة ١٩٦٨/٤/٢- مكتب فني ١٩- جزء ٢ – ص٦٨٩.

توافره لأن هذا الاستناد – وعلى ما جرى به قضاء محكمة النقض – يعتبر من وسائل الدفاع فى دعوى التعويض ولا يعتبر تغييرا لسبب الدعوى أو موضوعها مما لا تملكه المحكمة من تلقاء نفسها.

أركان المسئولية التقصيرية عن اخلال بحماية البيانات الشخصية

[١] الركن الأول هو الخطأ التقصيري أو فعل الاضرار، ففعل الاضرار خالف حقاً مقرراً بمقتضي القانون([١])، أو جاوز الحد الواجب الوقوف عنده أو التقصير في الحد الواجب الوصول إليه في الفعل أو الامتناع مما يترتب عليه الضرر، والاضرار يعني التعدى ولا يهم أن يكون التعدى إيجابياً أو سلبياً بالتقصير أو عدم التحريز، وإنما العبرة أن يكون الفعل من قبيل الانحراف عن السلوك المعتاد وذلك بمجاوزة ما يجوز إلى ما لا يجوز مما يؤدى لحدوث الضرر([٢]). ووفقاً لنص المادة ١٦٣ من القانون المدني فكل فعل سبب ضرراً للغير يلزم من ارتكبه بالتعويض، فالمشرع عاقب على حدوث الفعل ولم يضع شرطاً مسبقاً خاصة بالفاعل بأن يكون مميز أو غير مميز فهو يعاقب على الحدث دون المسئول عن الحدث فلو حدث الفعل من مجنون فهو والمسئول عنه ملزمان بتعويض الشخص المضرور، فالإضرار بالتسبب مقيد بوقوع التعدى، كما أن التعدى لا يشترط فيه أن يكون إيجابياً أو سلبياً ولكن السلوك قد تسبب في الضرر، فعلي سبيل المثال إذا كان المعالج يعلم أنه سوف تقع أضرار

([١]) **حسام الدين كامل الأهواني**: المرجع السابق– ص٣٨٤.

([٢]) الطعن رقم ٩٥٤٢ لسنة ٩١ قضائية، الصادر بجلسة ٢٠٢٢/٣/١٦. الطعن رقم ٤٨٦١ لسنة ٨٦ ق جلسة ٢٠١٧/٤/٢٢.

على الشخص المعنى ولم يمنعها ويخطر الشخص بالأضرار المحتملة فهو بعد احترازه قد تسبب في وقوع الضرر حتى لو كان تصرفه سلبياً.

عرفت محكمة النقض الخطأ التقصيري بأنه([1]) الانحراف عن أداء الواجب (مراعاة تقاليد المهنة والأصول العلمية الثابتة) مما يستوجب مسئوليته عن الضرر الذي يلحق بالشخص. فمتي أخل الشخص أو قصر في تنفيذ التزامه وهو قادر على تنفيذه نتيجة إهماله وعدم احترازه فهو مسئول عن تنفيذ الالتزام وفقاً لقواعد المسئولية، وفي مجال المسئولية التقصيرية الناتجة عن خطأ المرتكب في حق الشخص المعني، فمتي انحرف المخالف عن التعليمات والقواعد الخاصة بمعالجة البيانات الشخصية أو قام بها دون إذن مسبق من صاحب الشأن فإنه يسأل عن تعويض الأضرار التي لحقت بالشخص المعنى.

[٢] الركن الثاني هو حدوث الضرر، وتوافر الضرر هو جوهر المسئولية ولا يختلف الضرر سواء كان بسبب الخطأ العقدى أو الخطأ التقصيري، فأوجه الضرر التي ارتكبها المتسبب في الاعتداء على البيانات الشخصية سواء باختراق البيانات أو الحصول عليها بطريقة غير شرعية أو غيرها مثل جمع البيانات الشخصية للشخص المعني دون موافقته الاستحواذ على البيانات نشر البيانات أو إعادة النشر أو نشر بيانات حسابية أو معالجة الصوت والصورة للشخص مادامت قد تسببت في وقوع الضرر، وعلى القاضي أن يتأكد من وقوع أوجه المخالفة من جانب المتعدى،

([1]) الطعن ٢٤٩٨ لسنة ٥٨ ق جلسة ٢٠ / ٢ / ١٩٩٢ مكتب فني ٤٣ ج ١ ق ٧٨ ص ٣٦٢، الطعن ٢٤٤٦ لسنة ٥٨ ق جلسة ٢٨ / ٥ / ١٩٩٢ مكتب فني ٤٣ ج ١ ق ١٥٨ ص ٧٦٦.

والضرر هو كل ما يصيب الشخص في حق من حقوقه أو في مصلحة مشروعة له، سواء كان الايذاء في ماله أو جسده أو عرضه أو شعوره، فوظيفة المسئولية المدنية التقصيرية هي ضمان الضرر([1]). فالضرر هو المحور الذي تدور معه المسئولية المدنية وجوداً وعدماً وبدونه لا يمكن الحديث عن المسئولية([2]).

[٣] الركن الثالث هو علاقة السببية بين الخطأ والضرر، لا يكفي لقيام مسئولية المدعي عليه أن يثبت الشخص المعني أن ضرراً أصابه بل الضرر الذي لحق به قد نشأ عن فعل الاضرار الذي قام به المدعي عليه بمعني أن توجد علاقة مباشرة بين الخطأ والضرر([3])، فتوافر توافر رابطة السببية بين الخطأ والضرر الذي يصيب المضرور هي أساس المسئولية فإذا تداخلت أسباب أخري فإن رابطة السببية قد تنقطع، فعلاقة السببية تعد عنصراً لازماً لانعقاد الالتزام بالضمان([4])، تنص المادة ١٦٥ مدني على أنه: إذا أثبت الشخص أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه كحادث مفاجئ أو قوة قاهرة أو خطأ المضرور أو خطأ الغير كان غير ملزم بتعويض هذا الضرر ما لم يوجد نص أو اتفاق على غير ذلك، فيجب أن يكون

([1]) **عمر عبد الفتاح السيد**: المرجع السابق- ص٢٧٩، **خالد مصطفي فهمي**: الالتزام بالإعلام في التعاقد عن بعد- دار الفكر الجامعي- ٢٠١٩- الاسكندرية- ص٢١٦.

([2]) **محمد محيي الدين سليم**: نطاق الضرر المرتد- دار المطبوعات الجامعية- الاسكندرية- ٢٠٠٧- ص٥، **سامح عبد الواحد التهامي** : نطاق الحماية القانونية للبيانات الشخصية- مرجع سابق- ص٦٥٣.

([3]) **عبد الرزاق السنهوري**: المرجع السابق- ص١٢٢٠.

([4]) **عادل جبري حبيب**: المرجع السابق- ص٢٤١.

الخطأ هو السبب في الضرر، فإذا تعدد المسئولين عن الضرر الذي أصاب الشخص المعنى كأن كان هناك خطأ من جانب المدعي عليه والغير وخطأ المضرور فإنهم يتحملون المسئولية بالتضامن وفقا لنص المادة ١٦٩ من القانون المدني، وتقدير التعويض عن المسئولية التقصيرية ومدى مسئولية كل شخص في الضرر الواقع هو من إطلاقات محكمة الموضوع دون رقابة عليها من محكمة النقض([1]).

وهذا ما تشير إليه المادة ٨٢ من اللائحة الأوربية نصت على أنه يعفي الشخص المراقب أو المقاول من الباطن إذا أثبت أنه هناك سبباً أجنبيا هو الذي تسبب في الضرر، كما يحق للمسئول مطالبة كل المسئولين الآخرين وفق حصتهم في إصلاح الضرر الذي تحمله للمضرور وفقاً لقواعد المسئولية التضامنية.

[٣] التزام المسئول بتعويض الشخص المعنى

([1]) قضت محكمة النقض بأنه إذا كان المضرور قد أخطأ وساهم بخطئه في إحداث الضرر الذي أصابه فإنه يجب أن يراعي في تقدير التعويض المستحق له، فلا تحكم له على الغير إلا بالقدر المناسب لخطأ هذا الغير ويترتب على ذلك توزيع مبلغ التعويض بينه وبين الغير، وبناء على عمليه تشبه المقاصة لا يكون الغير ملزماً إلا بمقدار التعويض المستحق عن كل ضرر منقوصاً منه ما يجب أن يتحمله المضرور بسبب الخطأ الذي وقع منه- الطعن رقم ٩٥٤٢ لسنة ٩١ قضائية، الصادر بجلسة ٢٠٢٢/٣/١٦، وأضافت المحكمة أن تقدير التعويض هو من إطلاقات محكمة الموضوع بحسب ما تراه مناسبًا مستهدية فى ذلك بكافة الظروف والملابسات فى الدعوى، وراجع أيضا حكم محكمة النقض الطعن رقم ٣٠٧ لسنة ٥٨ق جلسة ١٩٩٤/١٢/٢٥ مكتب فني ٤٥ ج٢ ق٣٠٩ ص١٦٥٠.

يعرف التعويض بأنه جبر الضرر الذي لحق بالمضرور وإزالته([1]) أو إصلاح ضرر لحق بشخص هو المضرور سواء كان ضرراً جسدياً أو نفسياً بتقديم مبلغ من المال بهدف محو آثار الضرر أو التخفيف منها، فهدفه حماية المضرور بجبر الضرر الذي أصابه بخلاف العقوبة الجنائية التي تستهدف زجر الجاني عما اقترفه من جريمة ومنعا لغيره من الاقتداء به([2])، ولقاضي الموضوع سلطة واسعة في فهم وتكييف الوقائع المادية وتقدير مقدار الضرر، ومن ثم تحديد مقدار التعويض بدون معقب عليه من محكمة النقض مادام تقديره يتفق مع القواعد والعناصر الخاصة بالتعويض والتي نص عليها المشرع.

تنص المادة ٢٢١ مدني على أنه: [١] إذا لم يكن التعويض مقدّراً في العقد أو بنص في القانون فالقاضي هو الذي يقدّره، ويشمل التعويض ما لحق الدائن من خسارة وما فاته من كسب، بشرط أن يكون هذا نتيجة طبيعية لعدم الوفاء بالالتزام أو للتأخر في الوفاء به، ويعتبر الضرر نتيجة طبيعية إذا لم يكن في استطاعة الدائن أن يتوقّاه ببذل جهد معقول. [٢] ومع ذلك إذا كان الالتزام مصدره العقد، فلا يلتزم المدين الذي لم يرتكب غشاً أو خطأً جسيماً إلا بتعويض الضرر الذي كان يمكن توقّعه عادةً وقت التعاقد.

([1]) **حسام لطفي**: النظرية العامة للالتزام– أحكام الالتزام– ٢٠١٣– ص٦٠ وما بعدها.

([2]) **أحمد شوقي عبد الرحمن**: النظرية العامة للالتزام– العقد والإرادة المنفردة– منشأة المعارف – الإسكندرية– ٢٠٠٠– ص٣٤٩.

قضت محكمة النقض بأن تقدير التعويض سلطة للمحكمة- شرطه- قيامه على أساس سائغ ومتكافئ مع الضرر. كما أضافت المحكمة أن التعويض- مقياسه- الضرر المباشر الذي أحدثه الخطأ – عنصراه – الخسارة التي لحقت بالمضرور والكسب الذي فاته وهذان العنصران هما اللذان يقومهما القاضي بالمال على ألا يقل عن الضرر أو يزيد عليه – متوقعًا كان هذا الضرر أو غير متوقع – متى تخلف عن المسئولية التقصيرية([1]).

وعليه فإن التعويض هو ثمرة المسئولية أو الأثر المترتب على المسؤولية المدنية متى توافرت أركانها وبموجبها أصبح مرتكب الفعل الضار ملزما بتعويض المضرور عما اصابه من ضرر، حيث تنص المادة ١٦٣ من القانون المدني على أن: كل خطأ سبب ضررا للغير يلزم من ارتكبه بالتعويض.

وخلاصة القول أن الحق في التعويض عن الالتزام بحماية البيانات الشخصية هو حق ثابت وفقاً لقواعد المسئولية المدنية بصفة عامة أو من خلال قواعد القانون ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية أو اللائحة الأوربية لحماية البيانات وكذا كافة التشريعات المقارنة.

([1]) الطعن ٩٥٤٢ لسنة ٩١ ق جلسة ١٦ / ٣ / ٢٠٢٢ مكتب فنى ٧٣ ق ٦٣ ص ٥٠٧

الخاتمة والنتائج والتوصيات

أولاً: الخاتمة

بعد أن انتهينا من هذه الدراسة فقد اتضح لنا مدى تعاظم دور التكنولوجيا، والتي أصبحت منبراً للمعلومات والبيانات وصارت البيانات الشخصية متاحة بشكل كبير ويتم تداولها على النحو الذي يمكن أن يضر بأصحابها، بل أصبحت المواقع لا تقدم الخدمة لطالبها إلا بعد الحصول على كامل بياناته، وبدأت تلك المواقع باستغلال تلك البيانات في غير الأغراض التي بثت من أجلها الأمر الذي أدى لانتهاك خصوصية الشخص، ولما كانت حماية البيانات الشخصية لكل فرد تشكل أساساً لاحترام حقوقه وحرياته باعتباره السند لمجموعة من الحقوق المتصلة به وأن الهدف ليس حماية البيانات الشخصية فحسب بل حماية الحقوق والحريات الأساسية لأصحاب تلك البيانات في ظل تجميع الكثير من الجهات لبيانات الأشخاص بما يمس بمصلحة صاحب تلك البيانات. ومن هذا المنطلق نص القانون المصري على إنشاء مركز حماية البيانات الشخصية لتكون مهامه الرقابة على تنفيذ القانون، وإصدار التراخيص والتصاريح والاعتمادات للشركات التي تقوم بمعالجة واستخدام البيانات الشخصية للمستخدمين، وكذلك توجيه الإرشادات اللازمة لتوجيه القانون، وهو ما يواكب التطور الإلكتروني ويحافظ على الحريات الفردية.

لذا فإننا نأمل أن يساهم التشريع في احداث موازنة بين آليَّات حقوق الأفراد في حماية بياناتهم الشخصيَّة، وبين السَّماح بمعالجة البيانات والمعلومات والاحتفاظ بها

في ظلِّ الفضاء الإلكتروني، في ظل انتشار مفاهيم البيانات الضَّخمة والذَّكاء الصِّناعي. بحيث يؤسِّس القانون أطراً تنظيميَّة لحفظ البيانات الشخصيَّة، وإجراء المعالجة عليها ضمن قيود والتزامات واضحة، الأمر الذي يسهم في تعزيز الثِّقة اللازمة في الانخراط بالاقتصاد الرَّقمي والمساهمة في تشجيع التِّجارة والخدمات الإلكترونيَّة. كما يأتي القانون لبناء بيئة مواتية لتأمين سلامة الفضاء السِّيبراني ودعم استقراره، ولتحديد الالتزامات والواجبات المفروضة على المسؤول عن البيانات الشَّخصيَّة، ومعالجها، ومتلقِّيها، والجزاءات والعقوبات التي تفرض على المخالفين لأحكام القانون، ويُنشأ بموجب القانون مركز لحماية البيانات الشخصيَّة يهدف إلى حماية البيانات الشخصية وتنظيم معالجتها واتاحتها. وعليه تناولنا الموضوع في أطر الحماية المدنية التي أسداها المشرع في مصر أو أوروبا أو في الدول العربية والتي تهدف جميعها إلى حماية خصوصية البيانات المعالجة إلكترونيا، وقد تناولنا في هذه البحث بعض أوجه الحماية القانونية للبيانات الشخصية والتي أشار إليها القانون ١٥١ لسنة ٢٠٢٠ واللائحة الأوربية لسنة ٢٠١٦ وبعض التشريعات العربية، وذلك من خلال ثلاث مباحث بدأناها بمحث تمهيدى عن ماهية البيانات الشخصية ونطاق تطبيقها ومبحث أول عن معالجة البيانات الشخصية ومبحث ثاني عن حقوق الشخص عن المعالجة الخاطئة لبياناته.

ثانياً: النتائج

[١] ترتبط حماية البيانات الشخصية بحقوق الإنسان وخاصة حقه في الحياة الخاصة، ويجب أن تكون موافقته مشروطه بعدم الاعتداء على تلك الحقوق. حيث

تعتبر حماية البيانات الشخصية هي تعزيز لحماية الحقوق والحرَّيات العامة التي نصَّ عليها الدّستور، وترسيخ وحماية للبيانات الشخصيَّة في ظلِّ سهولة جمعها والاحتفاظ بها ومعالجتها، دون موافقة صريحة من صاحبها.

[٢] أهمية منع الاعتداء على حقّ المواطنين في حماية الحياة الخاصة بهم وبياناتهم الشخصيَّة وخصوصيَّتهم المقرَّرة بموجب أحكام الدّستور والقانون.

[٣] هدف وضع قانون لحماية البيانات الشخصية هو وضع إطار تشريعي يكفل للمستخدم حماية بياناته التي خضعت للمعالجة الإلكترونية، وذلك من خلال الحفاظ على عدة حقوق فرعية تابعة للحق في الخصوصية، مثل: الحق في معرفة طبيعة البيانات التي يمتلكها الحائز على البيانات والمعالج لها، كما يسمح للمعني بالبيانات تقديم شكوى ضد مستخدمي البيانات، ومقاضاتهم إذا استدعى الأمر.

[٤] اهتم المشرع المصري بوضع قانون لحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ولكن مازال هناك قصور في القانون الأمر الذي يتطلب إعادة مراجعته، ومراجعة دور مركز حماية البيانات الشخصية.

[٥] يخاطب القانون الشركات والمؤسسات التي تتعامل مع قواعد البيانات الخاصة بالمستخدمين، ويحدد على أساس ذلك المعايير التي تحكم العلاقة بين المستخدمين والشركات الرقمية.

[٦] اهتمت التشريعات في مختلف دول العالم بحماية البيانات الشخصية وهناك توافق واضح بينها في الكثير من الضوابط والشروط مع اللائحة الأوربية.

[٧] حق الشخص في حماية بياناته الشخصية واتخاذ الإجراءات القانونية ضد المخالفين، والتزام الدولة بحماية تلك البيانات ومعاقبة كل شخص يعتدى عليها.

[٨] حماية البيانات الشخصية تتعلق بشخص طبيعي دون الأشخاص المعنوية.

[٩] معالجة البيانات الشخصية يجب أن تتم بواسطة مختصين نظراً لخطورة تلك المعالجة والأضرار التي قد تنتج عنها.

[١٠] التزام كافة الجهات المتعاملة مع البيانات الشخصية باتخاذ الضوابط والشروط اللازمة بشأن الحفاظ على أمن وأمان وسلامة البيانات الشخصية وعدم تعرضها للاختراق أو الاتلاف.

ثالثاً: التوصيات

[١] الإسراع في وضع اللائحة التنفيذية للقانون والتي طال انتظارها.

[٢] ضرورة وضع قواعد ملزمة لسلوكيات وأخلاقيات التعامل مع البيانات الشخصية على المستوى الوطني، مع مراعاة قواعد السلوك التي نصت عليها المادة ٤٠ من اللائحة الأوربية.

[٣] ضرورة التوافق مع المجتمع الدولي في وضع اتفاقيات دولية واتفاقيات تعاون مع الدول ذات المصالح المشتركة.

[٤] إعطاء صلاحيات أكثر لمركز حماية البيانات الشخصية وفتح مقار أخرى له بالمحافظات تحت إشراف متخصصين ولا يكتفي بمقر وحيد.

[٥] ضرورة ادراج موضوع حماية البيانات الشخصية في المناهج الدراسية ضمن مادة حقوق الإنسان لطلبة المدارس والجامعات.

[٦] ضرورة إنشاء دوائر خاصة داخل المحكمة الاقتصادية تختص بحماية البيانات الشخصية على أن تستعين بخبراء مختصين في هذا الشأن. ومنح القضاة المختصين دورات بشأن معالجة القضايا الخاصة بالبيانات الشخصية.

[٧] لم يوضح المشرع في القانون الفرق بين الترخيص والتصريح ونري ضرورة أن يوضح ذلك في اللائحة التنفيذية.

[٨] لم يحدد المشرع طريقة اخطار الشخص المعني ونري أن اللائحة التنفيذية يجب أن تحدد ضوابط تحقق العلم وبياناته وعناصره، كما أنه يجب أن يحدد سبب وجود المعلومات الشخصية لدى الحائز وكيفية اطلاع صاحب البيانات عليها.

[٩] يجب وضع شروط واضحة وصريحة يطلع عليها كل شخص قبل إدراج بياناته الشخصية على أن تراجع تلك الشروط من جانب جهة اختصاص للتأكد من إلمام الشخص بها.

[١٠] لم يتناول المشرع التنميط الذي أشارت إليه اللائحة الأوربية والذي يعني أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتكون من استخدام هذه البيانات الشخصية لتقييم جوانب شخصية معينة تتعلق بشخص طبيعي، ولا سيما لتحليل أو التنبؤ بالعناصر المتعلقة بالأداء في العمل، والوضع الاقتصادي، والصحة، والشخصية التفضيلات أو الاهتمامات أو الموثوقية أو السلوك أو الموقع أو تحركات ذلك الشخص الطبيعي، ونري أنه يجب على المشرع تعديل النص وتعريفه وتوضيحه من خلال اللائحة التنفيذية.

قائمة المراجع

المراجع العربية:

١. **أحمد شوقي عبد الرحمن**: النظرية العامة للالتزام- العقد والإرادة المنفردة- منشأة المعارف – الإسكندرية- ٢٠٠٠.

٢. **أحمد عبد الحميد أمين**: التعويض عن الخطأ الشخصي لمأمور الضبط القضائي- بحث منشور بمجلة الحقوق- جامعة المنيا- ٢٠١٨/٦/١.

٣. **إكرام سليمان قجم**: الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن- رسالة ماجستير مقدمة لكلية القانون جامعة قطر- ٢٠٢١.

٤. **الصالحين محمد العيش**: حماية البيانات الشخصية في القانون الأوربي: مجلة كلية القانون الكويتية العالمية- س١١-ع٣-يونيو ٢٠٢٣.

٥. **تامر محمد الدمياطي**: الرضاء الرقمي بمعالجة البيانات الشخصية- مجلة القانون والتكنولوجيا كلية القانون الجامعة البريطانية بالقاهرة- مج٢- ع١- ابريل ٢٠٢٢.

٦. **حسام أحمد البهجي**: حماية الحق في حرمة الحياة الخاصة في ضوء حقوق الإنسان والمسئولية المدنية- دار الجامعة الجديدة- الاسكندرية- ٢٠٠٥.

٧. **حسام لطفي**: النظرية العامة للالتزام- أحكام الالتزام- ٢٠١٣.

٨. **حسام الدين كامل الأهواني:** مصادر الالتزام- دار النهضة العربية- القاهرة- بدون سنة نشر.

٩. **جبالي أبو هشيمة كامل:** حماية البيانات الشخصية في البيئة الرقمية- بحث مقدم إلى مؤتمر العصر الرقمي واشكالياته القانونية- كلية الحقوق جامعة أسيوط- الفترة من ١٢-١٣/٤/٢٠١٦ .

١٠. **جميل الشرقاوي:** النظرية العامة للالتزامات – مصدر الالتزام- دار النهضة العربية- القاهرة- ١٩٩١.

١١. **خالد حسن أحمد:** الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية- دار الكتب والدراسات العربية – الإسكندرية- ٢٠٢٠ .

١٢. **خالد سويلم محمد:** الحماية القانونية للبيانات الشخصية الالكترونية- المجلة القانونية – جامعة القاهرة- كلية الحقوق فرع الخرطوم- المجلد ١٤- العدد٦- نوفمبر ٢٠٢٢.

١٣. **خالد مصطفي فهمي:** الالتزام بالاعلام في التعاقد عن بعد- دار الفكر الجامعي- ٢٠١٩- الاسكندرية.

١٤. **خالد مصطفي فهمي:** النظام القانوني لمكافحة جرائم الاتجار بالبشر- دار الفكر الجامعي- الإسكندرية – ٢٠١١.

١٥. **خالد مصطفي فهمي**: طبيب التجميل (ماهية العمل التجميلي- طبيعته القانونية- المسئولية المدنية وتعويض الأضرار)- دار الفكر الجامعي- الاسكندرية.

١٦. **دراسة نقدية لقانون حماية البيانات الشخصية**- اعداد مركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية – القاهرة- ٢٠٢٠.

١٧. **رضا حميسي**: الضمانات القانونية لحماية البيانات الشخصية- كلية الحقوق والعلوم السياسية- جامعة قاصدي مرباح – ورقلة- الجزائر.

١٨. **سامح عبد الواحد التهامي**: ضوابط معالجة البيانات الشخصية- مجلة كلية القانون الكويتية العالمية- س٣-ع٩-مارس ٢٠١٥.

١٩. **سامح عبد الواحد التهامي**: نطاق الحماية القانونية للبيانات الشخصية والمسئولية التقصيرية من معالجتها- مجلة البحوث القانونية والاقتصادية- العدد ٦٧- ديسمبر ٢٠١٨.

٢٠. **طارق جمعه السيد راشد**: الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والقانون المقارن- المجلة القانونية والقضائية – وزارة العدل مركز الدراسات القانونية والقضائية- ع٢-٢٠١٧.

٢١. **عادل جبري حبيب**: المفهوم القانوني لرابطة السببية وانعكاساته في توزيع عبء المسئولية المدنية – دار الفكر الجامعي- الاسكندرية- ٢٠٠٣.

٢٢. **عبد الرزاق السنهوري**: الوسيط في شرح القانون المدني- ج١ نظرية الالتزام بوجه عام- مصادر الالتزام- منشأة المعارف – الإسكندرية- ٢٠٠٧.

٢٣. **عثمان بكر عثمان**: المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي- بحث منشور على شبكة الانترنت.

٢٤. **عمر عبد الفتاح السيد**: التوازن المعرفي في العقود المدنية- رسالة دكتوره- كلية الحقوق – جامعة طنطا- ٢٠١٨.

٢٥. **عمرو طه بدوى**: التنظيم القانوني لمعالجة البيانات الشخصية: دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية- دار النهضة العربية- القاهرة- ٢٠٢٠.

٢٦. **فهد بن عايد الشمري**: الاطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية- مجلة البحوث الفقهية والقانونية- العدد ٤٣ – أكتوبر ٢٠٢٣.

٢٧. **فوزية عبد الستار**: شرح قانون العقوبات القسم الخاص- دار النهضة العربية- القاهرة- ٢٠٠٠.

٢٨. **محمد أحمد سلامة مشعل**: الحق في محو البيانات الشخصية – دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوربي وأحكام المحاكم الأوربية – مجلة الدراسات القانونية والاقتصادية- جامعة مدينة السادات – ع٢- ٢٠١٧.

٢٩. **محمد محيي الدين سليم**: نطاق الضرر المرتد- دار المطبوعات الجامعية- الاسكندرية- ٢٠٠٧.

٣٠. **ميادة مصطفي المحروقي**: الحماية الجنائية لبيانات الأفراد الشخصية المعالجة الكترونيا- المجلة القانونية- جامعة القاهرة – فرع الخرطوم- المجلد رقم ١٦- العدد٧- مايو ٢٠٢٣.

٣١. **نبيلة رزاقي**: الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي- مجلة الدراسات القانونية المقارنة – الجزائر – المجلد السابع- العدد ١- ٢٠٢٠ – ص١٩٩٥.

٣٢. **نعيم عطية :** حق الافراد في حياتهم الخاصة ، مجلة ادارة قضايا الحكومة، العدد ٤ لسنه ٨١ ، أكتوبر – ديسمبر ١٩٧٧.

٣٣. **يحيي إبراهيم دهشان:** الحماية الجنائية للبيانات في ظل التحول الرقمي- مجلة الدراسات القانونية والاقتصادية- جامعة مدينة السادات- ع٣-٢٠٢٣.

المراجع الأجنبية:

- **Baffard WILLIAM**: Le système de traitement des infractions constatées personnelles ،mémoire de DEA informatique et droit ،faculté de droit université de Montpellier I, 2003.

- **Guillaume Desgens-Pasanau, RGPD**: entre incertitudes et occasions manquées, Dalloz, IP/IT, août / septembre 2016 .

- **Handbook on European**, data protection law, 2018 edition

- **Julien Le CLAINCHE**: la protection des donnéespersonnelles nominatives dans le cadre de la recherchedans le domaine de la santé , comparaison du droitfrançais et américain , mémoire de D.E.A , Faculté de droit , des sciences économiques et de gestion , univmontpellier I , et disponiblesurwww. droit-ntic.com , la date de mise en ligneest : 30 / 6 / 2001.

- **María Solange Maqueo Ramírez, Jimena Moreno González, Miguel Recio Gayo** :Protección de datos personales, privacidad y vida privada, la inquietante búsqueda de un equilibrio global necesario, , vol.30 no.1 Valdivia June 2017.

- Nathalie MALLET-POUJOL, protection de la vie privée et des données à caractére personnel, étude disponible sur, la date de mise en ligne est: mai 2007.

- **Sulliman OMARJEE** : Le data mining, Aspects juridiques de l›itelligenceartificielle au regard de la protection des donnéespersonnelles ،mémoire , faculté de droit , universitémontpellier I , Annéeuniversitaire 2001/2002 , et disponiblesurwww.droit-ntic.com.

مواقع على الانترنت:

- www.cnil.fr › fr › reglement-europeen-protection-donneesLe règlement général sur la protection des données – RGPD.

- http://dx.doi.org/10.4067/S0718-09502017000100004

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

- https://hunalibya.com/digital-life/9575/

- موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة- www.unodc.org

مشروع لائحة تنفيذية لقانون حماية البيانات الشخصية

- تسري أحكام القانون ١٥١ لسنة ٢٠٢٠ مع تطبيق أحكام هذه اللائحة إعمالا القواعد التي نص عليها القانون، فيما أحال إليه القانون للائحة لتنظيمه ووضع قواعده.
- تسري أحكام هذه اللائحة على البيانات الشخصية للأشخاص الطبيعيين

مادة١: تحديد السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين للبيانات الشخصية

مادة٢: تحديد السياسات والإجراءات والضوابط والمعايير الفنية لالتزامات المتحكم

مادة٣: تحديد السياسات والإجراءات والضوابط والشروط والتعليمات القياسية لالتزامات المعالج.

مادة٤: تحديد الإجراءات والضوابط الخاصة بالإبلاغ والاخطار

مادة٥: وضع شروط القيد وإجراءات وآليات التسجيل بسجل قيد مسئولي حماية البيانات الشخصية

مادة٦: تحديد المعايير والشروط الفنية التي يجب أن تستوفيها البيانات الشخصية حتى يعد الدليل الرقمي المستمد منها نفس حجية الاثبات لنظيره الخطي

مادة٧: تحديد السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو اتاحة البيانات الشخصية عبر الحدود

مادة٨: تحديد معايير وضوابط معالجة التحكم في البيانات الشخصية الحساسة بما فيها بيانات الأطفال.

مادة٩: تحديد الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لإتاحة البيانات خارج حدود جمهورية مصر العربية.

مادة١٠: تحديد القواعد والضوابط المتعلقة بالتسويق الالكتروني المباشر.

مادة ١١: الالتزام بالحصول على موافقة كتابية من الشخص المعني بالبيانات الشخصية حال عرض بيانات لجهات خارجية.

مادة ١٢: وزير العدل لتكليف دوائر مختصة بالمحاكم الاقتصادية لحماية البيانات الشخصية.

مادة ١٣: تكليف الجهات المختصة بوضع مناهج دراسية بشأن البيانات الشخصية وطرق حمايتها والتعامل معها.

مادة ١٤: وزير الداخلية لتخصيص إدارة لحماية البيانات الشخصية وتعلن بوسائل الاعلام ويتم تقديم الشكاوى المتعلقة بتلك البيانات إليها بالتنسيق مع مركز حماية البيانات الشخصية.

مادة ١٥: مركز حماية البيانات الشخصية لاعداد خطة خمسية وبرامج وسياسات لحماية البيانات الشخصية مع وضع مدونة سلوك لذلك.