

ضوابط جمع ومعالجة البيانات الشخصية

فى ظل الإدارة الإلكترونية

تأليف

الدكتور وليد رمضان عبد الرازق محمود

دكتوراه فى القانون العام

كلية الحقوق جامعة بنى سويف

عضو الجمعية المصرية للإقتصاد السياسى والتشريع

والمحامى لدى جميع المحاكم

أهمية البحث :-

يتناول هذا البحث الضوابط التشريعية لجمع ومعالجة البيانات الشخصية بطريقة مشروعة وملائمة لأغراض تجميعها حيث لم يكتف المشرع المصري بالنص على ضرورة جمع البيانات بطريقة مشروعة، وإنما اشترط أيضاً، في المادة الثالثة (فقرة أولى، بند ٣) "أن تُعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها". ويعني هذا الشرط عدم جواز جمع أو تجهيز أو تسجيل أية بيانات شخصية أو معلومات بأساليب أو بطرق غير مشروعة أو بغير رضا الشخص المعنى أو من ينوب عنه لذلك يحظر على القائمين على معالجة البيانات القيام بجمعها أو تسجيلها بأساليب أو بطرق غير مشروعة مع بيان مدة الاحتفاظ بالبيانات الشخصية و أن تكون صحيحة وسليمة ومؤمنة مع بيان حقوق الشخص المعنى بالبيانات المعالجة إلكترونياً .

منهج البحث :

تقوم الدراسة على المنهج التحليلي المقارن من خلال عرض ضوابط جمع البيانات الشخصية وبيان أوجه القصور التشريعي وتقديم المقترح الملائم لمعالجة البيانات في البيئة الرقمية مع الحفاظ على حقوق الشخص صاحب البيانات المعالجة إلكترونياً

كفلت دول العالم الحماية الدستورية والقانونية للحياة الخاصة للأفراد، ويأتي ذلك نتيجة لتوجه هذه الدول بتشريعاتها نحو توفير حماية فعالة للحق في الحياة الخاصة وتجاوب معها القضاء وأيدها الفقه نظراً لما تتمتع به الحياة الخاصة من أهمية كبرى على كيان الفرد والمجتمع معاً راجع في ذلك أستاذنا الدكتور / احمد فتحي سرور - الحماية الدستورية للحقوق والحريات - دار الشروق - القاهرة ٢٠٠٠ ص ٣٣ . فهناك الكثير من التهديدات المعلوماتية التي قد تطول البنى التحتية والتي قد تشكل مخاطر حقيقية على الخصوصية واتلاخيرة يقصد بها حق الشخص في أن يتحكم بالمعلومات التي تخصه وقد جرى التعامل معها كحق لمنع إساءة استخدام البيانات التي تعالج ألياً أو إلكترونياً راجع في ذلك منى تركى الموسرى " الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها " مجلة العلوم الاقتصادية - كلية بغداد للعلوم الاقتصادية - العراق - عدد خاص ٢٠١٣ ص ٣٠٧ . واتفق مع الرأي القائل أن معالجة البيانات الشخصية تتمثل في كل عملية يكون من شأنها جمع البيانات أو تسجيلها أو حفظها أو تنظيمها أو تغييرها أو استغلالها واستعمالها أو نشرها وتوزيعها ولكي تصبح المعالجة مشروعة وقانونية يتعين أن تتوافر لها شروط معينة بحيث إذا توافرت أصبح القائم بها بمنأى عن سيف المسؤولية وأضحت معالجته للبيانات عمل مشروع راجع د/ سامح عبد الواحد التهامي - الحماية القانونية للبيانات الشخصية - دراسة القانون الفرنسي، القسم الأول، مجلة الحقوق جامعة الكويت، المجلد ٣٥ ، العدد ١١ ، ٢٠١١ ، ص ٤١٥ وما بعدها ص ٥٠٤ وهناك بعض الآثار القانونية الناشئة عن معالجة البيانات الشخصية تتمثل في حقوق صاحب البيانات بمعرفة حقوقه على تلك البيانات ومعرفة إلتزامات المعالج والمتاحم والحائز ومعاينة من يخالف قواعد حماية تلك البيانات بما يوفر الحماية للبيانات الشخصية وعدم توافر تلك الضوابط تصبح هذه البيانات متاحة ويمكن استخدامها في أغراض غير مشروعة وغير قانونية .

خطة البحث :

المبحث الاول :- ضوابط جمع ومعالجة البيانات الشخصية فى ظل الإدارة الإلكترونية

المطلب الأول : أن يتم جمع البيانات الشخصية لأغراض مشروعة ومحدد ومعلنة للشخص المعنى

المطلب الثانى : أن تكون صحيحة وسليمة ومؤمنة

المطلب الثالث : أن تعالج بطريقة مشروعة وملائمة للأغراض التى تم تجميعها من أجلها

المطلب الرابع : الأيتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها

المبحث الثانى : التزامات المتحكم والمعالج والحائز وحقوق صاحب البيانات

المطلب الأول : إلتزامات المتحكم

المطلب الثانى إلتزامات المعالج

المطلب الثالث : حقوق صاحب البيانات المعالجة

مقدمة :-

يُعد إصدار قانون حماية البيانات الشخصية المصري خطوة تشريعية بالغة الأهمية في مضمار تأمين البيانات الشخصية للمواطنين، وخاصة مع خلو التشريعات القائمة من إطار قانوني ينظم حماية البيانات الشخصية المعالجة إلكترونياً أثناء جمعها أو تخزينها أو معالجتها. ويعبر القانون عن صور حق الأشخاص في حماية بياناتهم الشخصية، ويُجرم جمع البيانات بطرق غير مشروعة أو بدون موافقة أصحابها، وتجريم معالجتها بطرق تدليسية أو غير مطابقة للأغراض المُصرح بها من قبل صاحب البيانات وتنظيم نقل ومعالجة البيانات عبر الحدود بما يعود بالنفع على المواطنين وعلى الاقتصاد القومي، بما يسهم في حماية الاستثمارات والأعمال، كما يتوافق مع المعايير الدولية في مجالات حماية البيانات الشخصية، وذلك من خلال القواعد والمعايير والاشتراطات التي يفرضها، ويباشر الإشراف عليها مركز حماية البيانات المنشأ لهذا الغرض.

حيث أدت تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع بزوغ تكنولوجيا إنترنت الأشياء، والحوسبة السحابية، والذكاء الاصطناعي وغيرها، إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبوق، مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد^(١) وسوف نتناول في هذا البحث دراسة ضوابط جمع ومعالجة البيانات الشخصية وتوضيح الشروط الزم توافرها لكي تتم معالجة البيانات الشخصية وماهى حقوق الشخص صاحب البيانات .

(١)- راجع: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يولية ٢٠١٩ ، ص ٨ وما بعدها، متاح على الموقع التالي: <https://www.elwatannews.com/data/iframe/pdf/25021748.pdf> - في الحقيقة، إن الحياة الرقمية يترتب عليها العديد من المشكلات المتعلقة بالوجود القانوني في هذه الحياة الافتراضية. ومن جهة أخرى، فإذا كان القانون، فيما سبق، يحركه الاقتصاد والسياسة، فإن القانون في زمن الحياة الرقمية يحركه أيضاً الاقتصاد والسياسة. فليس خافياً على أحد أن اقتصاديات العالم الافتراضي قد وصلت لأرقام تجاوزت بكثير كل التوقعات. إن من بين أهم مصادر الثروة في الحياة الرقمية "تجارة المعلومات"، ويدخل في هذه التجارة، علي وجه الخصوص، التجارة المتعلقة بالبيانات الشخصية. ليس هذا فحسب، فالبيانات الشخصية تستعمل كذلك سياسياً وعسكرياً وأمنياً. وحينما أصبح إستغلال البيانات الشخصية " ظاهرة" بالمعنى الحقيقي لمصطلح " ظاهرة" في علم الاجتماع القانوني، وارتبط بها العديد من الأنشطة الإنسانية، كان لزاماً على القانون التدخل لضبط هذه الظاهرة من خال التشريع . فحق الخصوصية المعلوماتية يعني فالحفاظ على أسرار الإنسان هو جوهر وأساس ضمانه حرية الخصوصية ضد انتهاك الغير، وهنا يظهر دور القواعد القانونية التي تُؤطر وتحكم وتنظم مسائل هذه الحماية، من خال ما تسنه من تشريعات تكفل ضمان عدم المساس بها أو إفشائها. ويعتبر الحق في حماية البيانات الشخصية وصونها وعدم إفشائها للغير، من أهم وأعظم صور الحق في الخصوصية) راجع في ذلك - د. شريف يوسف خاطر: حق الاطاع على البيانات الشخصية في فرنسا، مجلة كلية القانون الكويتية العالمية، السنة الثالثة، العدد التاسع، مارس ٢٠١٥ م، ص ٢٨١ ، ٢٨٢ ، ٢٨٣ . وقد أولت التشريعات الدولية المختلفة اهتماماً متعاضماً لحماية حق الأفراد في الخصوصية نظراً لاعتماد أنماط الحياة المعاصرة باطراد على البنى التكنولوجية في مختلف أوجه الإدارة والإتصال، ما نتج عنه تعاضماً في كمية البيانات التي توحدتها الدولة والمؤسسات الخاصة، ما استدعى أن ينظر المشرع بوجه العناية إلى الكيفية التي يتم بها جمع، وحفظ، ومعالجة البيانات التي يمكن أن تحتوي على معلومات خاصة بالأفراد؛ وما قد ينتج عن إساءة استخدامها من انتهاك لخصوصيتهم، وذلك في حاجة ملحة تضمن خصوصية المواطنين؛ بحيث يجرم جمع البيانات الشخصية بطرق غير مشروعة، ومعالجتها بطرق تدليسية، ونقلها عبر الحدود الجغرافية، ويجرم إفشائها؛ ما قد يعرض المواطنين لانتهاك حرمة حياتهم الخاصة وحقوقهم في الخصوصية الإيعان العالمي لحقوق الإنسان الصادر عام ١٩٤٨ : حيث يرسخ الحق في الخصوصية، بشكل واضح في المادة ١٢ م

المبحث الاول

ضوابط جمع ومعالجة البيانات الشخصية

المطلب الاول

أن يتم جمع البيانات الشخصية لأغراض

مشروعة ومحدد ومعلنة للشخص صاحب البيانات

تمهيد :

لقد كانت البيانات الشخصية قبل ذلك منعزلة ومتفرقة والتوصل إليها صعب ،وقد تمكنت تقنية المعلومات الجديدة من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية والشركات الخاصة . ويمكن مقارنة المعلومات المخزنة في ملف بمعلومات في قاعدة بيانات ويمكن نقلها عبر البلد في ثوان (١) فقد تطورت البيانات الشخصية مع تطور الإنترنت فلم يعد المتاح منها الاسم ،واللقب ، والعنوان البريدي ، بل ازدادت وتنوعت لتشمل صورة الشخص وصوته ، علاوة على طائفة أخرى من البيانات التي تتعلق بقدرته المكانية وسلوكياته وميوله وأذواقه والأشد من ذلك كله البيانات التي تتعلق بجسم الانسان " البيانات البيومترية " (٢)

(١)- د/ عبد الهادي فوزى العوضى : الحق في الدخول في طى النسيان على شبكة الإنترنت ص ٩١ -

(٢)- والبيانات البيومترية هي علم التحقق التقاني من هوية الإنسان عن طريق مكونات الأجسام البشرية ، أى من خلال قياس التحليل الإحصائي للخصائص المادية والسلوكيات للأفراد ويستخدم هذا المصطلح للإشارة إلى البيانات المجمع من الأفراد من خلال سماتهم البيولوجية أو الفيزيائية كبيانات مسح شبكية العين وقزحية العين وبصمات الأصابع والوجه ، وتمييز الصوت وهندسة اليد والحمض النووي DNA راجع في ذلك د/ عثمان بكر عثمان المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي ص ٨ .

ويقصد بالبيانات الشخصية : أى بيانات متعلقة بشخص طبيعى محدد ، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأى بيانات أخرى كالاسم أو الصوت أو الصورة أو رقم تعريفى أو محدد للهوية عبر الإنترنت ، أو أى بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الإجتماعية راجع فى ذلك المادة رقم (١) من قانون حماية البيانات الشخصية المصرى رقم ١٥١ لسنة ٢٠٢٠م . وعرفها التوجيه الأوربي الصادر عن البرلمان الأوربي فى ٢٤ من أكتوبر ١٩٩٥م بأنها " كل معلومة أيا كانت طبيعتها ،وبما فى ذلك الصوت والصورة تتعلق بشخص معرف أو قابل للتعريف ويعتبر الشخص قابل للتعريف ، إذا أمكن تعريفه بشكل مباشر أو غير مباشر لاسيما من خلال رقم التعريف الشخصى أو واحد أو أكثر من العناصر المميزة له راجع فى ذلك د/محمد سامى عبد الصادق: شبكات التواصل الاجتماعي ومخاطر إنتهاك الحق فى الخصوصية ، دار النهضة العربية القاهرة ، ٢٠١٦م ص ٣٨ . وعرفها المشرع الفرنسى فى المادة الثانية من القانون رقم ٨٠١ لسنة ٢٠٠٤م الخاص بحماية البيانات الشخصية " يعتبر بياناً شخصياً أى معلومة تتعلق بشخص طبيعى محدد هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة سواء تم تحديد هويته بالرجوع إلى رقمه الشخصى أو بالرجوع إلى أى شىء يخصه راجع فى ذلك د/ عثمان بكر عثمان المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي - كلية الحقوق جامعة طنطا بدون تاريخ نشر ص ٨ . وكما عرفتها المادة رقم (١) من قانون حماية البيانات الشخصية الإماراتى " أى بيانات متعلقة بشخص معين والتي يمكن من خلالها التعرف على هذا الشخص أو بيانات أو معلومات فى حوزة أو قد تصبح فى حوزة جامع البيانات والتي يمكن من خلالها التعرف على شخص معين وتشمل البيانات الشخصية ذات الطبيعة الحاساسة " . وعرفها المشرع البحريني بأنها " أية معطيات فى أى صورة تخص فرداً معرّفاً أو قابلاً بطريق مباشر أو غير مباشر لان يعرف ، وذلك بوجه خاص من خلال رقمه هويته الشخصية أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية " راجع فى ذلك المادة رقم (١) من القانون رقم ٣٠ لسنة ٢٠١٨م قانون حماية البيانات الشخصية البحريني .

لقد أدت تكنولوجيا المعلومات إلى اعتماد المعاملات اليومية للأفراد على الحاسب الألى ، وأدى ذلك إلى ظهور مايسمى ببنوك المعلومات (١) وتعنى الأخيرة "تكوين قاعدة بيانات تفيد موضوعاً معيناً وتهدف لخدمة غرض معين ، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية (الحواسيب) إخراجها فى صورة معلومات تفيد مستخدمين مختلفين فى أغراض معينة (٢)

ويضع قانون حماية البيانات الشخصية التزامات أساسية على الأفراد والجهات التى قد تحوز البيانات الشخصية للمستخدمين ،سواء كانت حيازة البيانات لأسباب تتعلق بطبيعة عملها أو لأى سبب آخر . ويفرق القانون بين هذه الالتزامات ، حسب طبيعة الأشخاص اللين يتعاملون مع البيانات الشخصية كالحيازة والتحكم والمعالجة المختلفة للبيانات الشخصية

ولذلك أويد كباحث الرأى الفقهي القائل : لقد ظهرت مع التكنولوجيا مايسمى ببنوك المعلومات ، ويقصد بها تكوين قاعدة بيانات موضوعاً معيناً ، وتهدف لخدمة غرض معين ، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها فى صورة معلومات ، تفيد مستخدمين مختلفين فى أغراض متعددة ، فيما تحتوى عليه من معلومات عن الفرد ومايخزن عنه من بيانات تشكل عنصر تضيق ، وتقليل انطلاقات الفرد وإبداعه ومشاركته فى شئون الحياة العامة ، والسبب الرئيسى أو الاساسى فى ذلك ، يرجع إلى أنه أصبح محوراً لعمليات آلية مختلف مختلفة تمسه فى كل جانب من جوانب حياته المتشعبة . الحاسوب يقوم بجمع وتخزين ومعالجة ونشر المعلومات الشخصية للأفراد ولكل أمر من هذه الامور ، يشكل خطراً أو آخر على حياة الانسان الخاصة ، ويهددها ، لذا فإن الفرد يصبح أسيراً للمعلومات التى جمعتها هذه الألة عنه ورصدت كل تحرك من تحركات حياته (٣).وأؤكد كباحث أن الهدف من القانون وضع سياسة تشريعية واضحة تتعلق بقطاع الاتصالات وتكنولوجيا المعلومات ، وأرى كباحث أن هذا القانون (قانون حماية البيانات الشخصية) سوف يساعد مصر أن تصبح فى قمة البيئة الرقمية .

وذلك لمواجهة تفاقم الاعتداءات على البيانات الشخصية بما استدعى تدخلاً من جانب المشرع وكذلك الحماية الدستورية . حيث ان خصوصية جرائم الاعتداء على الحياة الخاصة او البيانات الشخصية أظهرت مشكلة المكافحة الاجرائية للجريمة المعلوماتية . الامر الذى دفع المشرع للسعى لمواكبة التطور الذى لحق بالجريمة المعلوماتية .

(١)- د/ محمد عزت عبد العظيم ،الجرانم المعلوماتية الماسة بالحياة الخاصة ، دار النهضة العربية – القاهرة ٢٠١٨ م ص ١٢٩ .

(٢)- بونس عرب : المخاطر التى تهدد الخصوصية وخصوصية المعلومات فى العصر الرقمية اتحاد المصارف العربية الطبعة الأولى ٢٠٠٢ م ص ٩ . (٣)- د/ محمد رشيد حامد – الحماية الجزائية للمعلومات الشخصية فى مواجهة أخطار البنوك – رسالة ماجستير – كلية الحقوق – جامعة آل البيت - ص (٤) . وبما أن البيانات ذات الطابع الشخصي هي أحد أهم الحقوق اللصيفة بالشخصية والمرتبطة بالحياة الخاصة للفرد، فإن المعالجة الآلية لهذه البيانات تتطلب أخذ الاحتياطات اللازمة، واحترام الإجراءات الخاصة الواجب إتباعها أثناء هذه العملية، ومنها احترام الغرض الذى من أجله تم السماح القانوني بمعالجة هذه البيانات ولا تتعداه إلى غيره من الأغراض،وقد جرم قانون العقوبات الفرنسي هذا الفعل وعاقب عليه.راجع فى ذلك د. بولين أنطونيوس أيوب، المرجع السابق،ص ٤٠١ . لقد أدت تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع بزوغ تكنولوجيا إنترنت الأشياء، والحوسبة السحابية، والذكاء الاصطناعي وغيرها، إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبوق، مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد) راجع: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يولية ٢٠١٩ ، ص ٨ وما بعدها، متاح على الموقع التالى:

ويعتبر جمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعنى من أهم ضوابط جمع وتخزين البيانات الشخصية في ظل القانون ١٥١ لسنة ٢٠٢٠م فلا يجوز جمع البيانات الشخصية إلا بهدف مشروع سواء كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة .

وقد حرص المشرع المصري على ذلك حيث أكد أنه يلتزم معالج البيانات الشخصية بالآتي :-

١- إجراء المعالجة الإلكترونية وتنفيذها طبقاً للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقاً للحالات المشروعة والقانونية وبناء على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أى ذى صفة بحسب الأحوال ، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموعها وطبيعتها ونوع البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد له (١)

(١)-المادة رقم (٥) من ا قانون حماية البيانات الشخصية المصبررقم ١٥١ لسنة ٢٠٢٠م - ونظراً لاهتمام الدولة فى الوقت الحاضر بتشجيع الاستثمارات فى مجال صناعة مراكز البيانات العملاقة، هادفةً لأن تصبح مصر ممراً رقمياً عالمياً، ولما كان ذلك يتطلب وجود بيئة تشريعية مناسبة، فقد حرصت الحكومة وأعضاء مجلس النواب على إعداد وصياغة مشروع قانون حماية البيانات الشخصية بما يضمن خصوصية المواطنين والعمل على تهيئة المناخ الاستثماري في مصر، وحتى يكون متسقاً مع اللائحة العامة لحماية البيانات GDPR الصادرة عن الاتحاد الأوروبي باعتبارها التغيير الأكثر أهمية في تنظيم خصوصية البيانات على المستوى العالمي خال العشرين عاماً الماضية، ولتأثر الكيانات غير الأوروبية التي تستخدم خدمات الانترنت بأحكامها دخلت اللائحة العامة لحماية البيانات GDPR حيز التنفيذ يوم ٢٥ مايو ٢٠١٨م ، وتنطبق على جميع المؤسسات داخل وخارج الاتحاد الأوروبي التي تتعامل مع بيانات سكان منطقة الاتحاد الأوروبي وتعالجها. ويكمن الغرض من اللائحة في 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، بدءاً من أصحاب العمل ووصولاً إلى الشركات التي يشتري هؤلاء الأشخاص أو يستخدمون منتجاتها وخدماتها. كما تفرض GDPR 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. فعلى سبيل المثال أعلنت شركة ميكروسوفت العملاقة عبر موقعها عن التزامها تجاه الامتثال للقانون العام لحماية البيانات (GDPR)، راجع الموقع التالي:

<https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview>

وقد حرص المشرع المصري على أن تكون فلسفة وأهداف إصدار قانون حماية البيانات لشخصية: جاء مشروع القانون متوخياً الأهداف الآتية:-

■ ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً. ■ وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين، ومكافحة انتهاك خصوصيتهم. ■ تطبيق إطار معياري يتواءم مع التشريعات الدولية لحماية البيانات الشخصية للأفراد، وحرياتهم، واحترام خصوصيتهم. ■ 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. ■ إلزام المؤسسات والجهات والأفراد المتحكمين في البيانات الشخصية، والمعالجين لها بتعيين مسؤول لحماية البيانات الشخصية داخل مؤسساتهم وجهاتهم، بما يسمح بضمان خصوصية بيانات الأفراد، واقتضاء حقوقهم المنصوص عليها في هذا القانون. ■ تقنين وتنظيم أنشطة استخدام البيانات الشخصية في عمليات الإعان والتسويق على الانترنت، وفى البيئة الرقمية بشكل عام. ■ وضع إطار إجرائي لتنظيم عمليات نقل البيانات عبر الحدود وضمان حماية بيانات المواطنين وعدم نقلها أو مشاركتها مع دول لا تتمتع فيها البيانات بالحماية. ■ تنظيم العمليات المعالجة إلكترونياً للبيانات الشخصية، وإصدار تراخيص لمن يقوم بها، وعلى الأخص فيما يتعلق بالبيانات الشخصية الحساسة "ذات الطابع الخاص". ■ إنشاء مركز حماية البيانات الشخصية كهيئة عامة يكون مختصاً بتنظيم والإشراف على تنفيذ أحكام القانون. راجع: تقرير اللجنة المشتركة حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، سالف الإشارة إليه، ص ٩، ١٠ ..

وفى البحرين نص المشرع على شروط هامة لمشروعية جمع البيانات ومنها تحظر جمع البيانات دون موافقة صاحبها ما لم تكن هذه المعالجة ضرورية لآى مما يأتى :

- ١- تنفيذ عقد يكون صاحب البيانات طرفاً فيه.
- ٢- اتخاذ خطوات بناءً على طلب صاحب البيانات بهدف إبرام عقد.
- ٣- تنفيذ التزام يرتبه القانون، خلافاً للالتزام عقدي، أو صدور أمر من محكمة مختصة النيابة العامة.
- ٤- حماية المصالح الحيوية لصاحب البيانات.
- ٥- مبالغة المصالح المشروعة لمدير البيانات أو أي طرف ثالث يُفصح له عن البيانات ما

لم يتعارض ذلك مع الحقوق والحريات الأساسية لصاحب البيانات. (١) ونتفق مع الرأي الفقهي الراجح الذى يرى انه يجب أن يكون لجمع البيانات ومعالجتها أغراض أو أهداف مشروعة ومحددة وواضحة ومعلنة للشخص المعنى، على نحو ما صرحت المادة الثالثة (فقرة أولى بند ١) من قانون حماية البيانات الشخصية، ويُعد هذا الشرط من الشروط الجوهرية التي ينبغي توافرها سواء أكان ذلك بالنسبة للمعالج أو المتحكم أو الغير الذي ترسل اليه البيانات، ويجب أن يظل هذا الشرط قائماً خال فترة الجمع أو المعالجة أو الاحتفاظ بالبيانات، كما يجب أن يظل متوافراً أيضاً بعدها (٢) وجدير بالذكر أن المعالجة تكون مشروعة متى كانت لا ترمي الى الإساءة للأشخاص أو التشهير بهم، ومن ذلك على سبيل المثال، اذا كانت المعالجة لازمة لأغراض منع أو كشف الجرائم بناءً على طلب من جهات التحقيق، أو كانت مطلوبة أو مصرحاً بها بموجب أي قانون أو كان ذلك بقرار صادر من المحكمة، أو إذا كانت البيانات ضرورية لتقدير أو تحصيل الضرائب أو الرسوم، أو إذا كانت لحماية مصلحة حيوية للشخص المعنى بالبيانات (٣)

(١) المادة رقم (٤) من قانون حماية البيانات الشخصية البحريني رقم (٣٠) لسنة ٢٠١٨م
(٢) راجع: د. سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية - دراسة القانون الفرنسي، القسم الأول، مجلة الحقوق جامعة الكويت، المجلد ٣٥، العدد ١١، ٢٠١١، ص ٤١٥ وما بعدها؛ د. عمرو طه بدوي: مرجع سابق، ص ١٠٩ وما بعدها.
(٣) د. عمرو طه بدوي: مرجع سابق، ص ١١٠ .
(٤) ويُلاحظ على مسلك المشرع المصري توسعه بشكل كبير فى استبعاد طائفة كبيرة من البيانات الشخصية من نطاق الحماية التي يضيفها هذا القانون الجديد على البيانات، رغم حاجتها لإضفاء الحماية عليها، ودون مبرر أو علة، ومن ذلك البيانات الشخصية لدى البنك المركزى، والبيانات المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية ولدى جهات الأمن القومى، حيث كان من الأولى وضعها تحت مظلة الحماية فوق ضوابط تراعى خصوصيتها، وليس استبعادها على إطلاقها. ومن جهة أخرى، تفتح هذه المادة الباب واسعاً لاستبعاد البيانات لدى جهات الأمن القومى (المتعددة)، بالإضافة إلى "ما تقدره هذه الجهات لاعتبارات أخرى"، أي اعتبارات خاف الأمن القومى وهي بالطبع كثيرة! - يُشار إلى سابقة رفض لجنة الاتصالات وتكنولوجيا المعلومات بمجلس النواب ووزارة الاتصالات طلب البنك المركزي باستثنائه والجهات التابعة له من مشروع قانون "حماية البيانات الشخصية"، تأسيساً على أن القطاع المصرفي في العالم يخضع لحماية مضافة للبيانات لأنها بطبيعتها بيانات حساسة، وأن فلسفة مشروع القانون تكمن فى تنظيم حماية البيانات وليس وضع سرية على البيانات. وتعليقاً على ذلك صرح البعض - ممن شاركوا فى إعداد مشروع القانون - بأن هذا الاستثناء يُفرغ القانون من مضمونه ويجعله با قيمة ويمثل عدم استيعاب لفلسفة حماية البيانات الشخصية التي تعد حقاً أصيلاً للمواطن. ولكن ظهر القانون فى النهاية بعد مناقشته فى المجلس متضمناً هذا الاستثناء! راجع بوابة جريدة الأهرام، بتاريخ ١٧ / ٦ / ٢٠١٩ على الموقع التالى:

جمع ومعالجة البيانات بطريقة مشروعة وملائمة لأغراض تجميعها، حيث لم يكتف المشرع المصري بالنص على ضرورة جمع البيانات بطريقة مشروعة، وإنما اشترط أيضاً، فى المادة الثالثة (فقرة أولى، بند ٣) "أن تُعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها". ويعني هذا الشرط عدم جواز جمع أو تجهيز أو تسجيل أية بيانات شخصية أو معلومات بأساليب أو بطرق غير مشروعة أو بغير رضا الشخص المعنى أو من ينوب عنه (١).

لذلك يحظر على القائمين على معالجة البيانات القيام بجمعها أو تسجيلها بأساليب أو بطرق غير مشروعة. وحتى يسوغ القول بأن عملية جمع البيانات قد تمت بطريقة مشروعة، فإنه يجب أن يتم إعام الشخص المعنى بالبيانات عن وجود تجميع لهذه البيانات وعن طريقة التجميع والغرض من التجميع وأنواع البيانات التي تم تجميعها (٢).

(١)- د. عمرو طه بدوي: مرجع سابق، ص ١٠٥ .

(٢)- د. سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية، مرجع سابق، ص ٤٠٤ - . (الخاصة بالمبادئ المتعلقة بمعالجة البيانات الشخصية)، بند أ، على أن تكون البيانات قد تم معالجتها بطريقة مشروعة lawfully و عادلة fairly وبطريقة شفافة transparent بالنسبة لصاحب البيانات) المشروعة lawfulness والعدالة fairness والشفافية transparency. ومن ثم تتطلب عملية معالجة البيانات أن تجري بدقة وأمانة من المتحكم أو المعالج وعدم استخدام أية وسائل إحتيالية أو غير مشروعة لجمع ومعالجة البيانات، وكذلك يحظر القيام بجمع بيانات شخصية لأغراض غير مشروعة، أو مخالفة للنظام العام، أو بيانات شخصية غير صحيحة، أو غير ضرورية لنشاط المعالجة. وراجع أيضاً المادة ٤ من القانون المغربي المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، حيث تشير فقرتها الثانية إلى ما يلي: "... غير أن الرضى لا يكون مطلوباً إذا كانت المعالجة غير ضرورية: (أ) لاحترام التزام قانوني يخضع له الشخص المعنى أو المسؤول عن المعالجة؛ (ب) لتنفيذ عقد يكون الشخص المعنى طرفاً فيه أو لتنفيذ إجراءات سابقة للعقد تتخذ بطلب من الشخص المذكور؛ (ج) للحفاظ على المصالح الحيوية للشخص المعنى إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه؛ (د) لتنفيذ مهمة تدخل ضمن الصالح العام أو ضمن ممارسة السلطة العمومية التي يتولاها المسؤول عن المعالجة أو أحد الأعيان الذي يتم إطلاعها على المعطيات؛ (هـ) لإنجاز مصلحة مشروعة يتوخاها المسؤول عن المعالجة أو المرسل إليه مع مراعاة عدم تجاهل مصلحة الشخص المعنى أو حقوقه وحرياته الأساسية". في مجال صناعة مراكز البيانات العملاقة، هادفة لأن تصبح مصر ممراً رقمياً عالمياً، ولما كان ذلك يتطلب وجود بيئة تشريعية مناسبة، فقد حرصت الحكومة وأعضاء مجلس النواب على إعداد وصياغة مشروع قانون حماية البيانات الشخصية بما يضمن خصوصية المواطنين والعمل على تهيئة المناخ الاستثماري في مصر، وحتى يكون متسقاً مع اللائحة العامة لحماية البيانات GDPR الصادرة عن الاتحاد الأوروبي ٢٠١٨ ، وتتنطبق على جميع المؤسسات داخل وخارج الاتحاد الأوروبي التي تتعامل مع بيانات سكان منطقة الاتحاد الأوروبي وتعالجها. ويكمن الغرض من اللائحة في 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 GDPR 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. باعتبارها التغيير الأكثر أهمية في تنظيم خصوصية البيانات على المستوى العالمي خال العشرين عاماً الماضية، ولتأثير الكيان غير الأوروبية التي تستخدم خدمات الانترنت بأحكامها - فعلى سبيل المثال أعلنت شركة ميكروسوفت العملاقة عبر موقعها عن التزامها تجاه الامتثال للقانون العام لحماية البيانات (GDPR) ، راجع الموقع التالى:

<https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview>

تجدر الإشارة إلى أن الحماية القانونية للبيانات الشخصية في فرنسا، وفقاً للفصل الثاني من قانون (١٨ - ١٩٧٨) (والمعدل وفقاً للتعديلات بموجب القانون رقم) ٢٠٠٤-٧٠١ الصادر فى ٦ أغسطس ٢٠٠٤ قد نصت على شروط معينة لضمان مشروعية جمع ومعالجة البيانات الشخصية، وهي كما يلي م(٨:١) عدالة ومشروعية طريقة جمع ومعالجة البيانات الشخصية. ٢- وضوح وتحديد أهداف وأغراض جمع المعلومات، وأن يكون هناك توافق بين طريقة جمع المعلومات وغرض جمعها. ٣- أن تكون طريقة جمع المعلومات كافية ومناسبة وذات صلة بالقياس للغرض الذي تم من أجله جمعها ومعالجتها. لمزيد من التفصيل فى هذا الخصوص، راجع: د. وليد السيد سليم: ضمانات الخصوصية فى الانترنت، دار الجامعة الجديدة، ٢٠١٢ ، ص ٥٨٨ وما بعدها. ونشير إلى قرار رقم ١٣٠ الصادر عن مندى البيانات العالمى ٢٠١٨م بدولة الإمارات العربية المتحدة

ومما تجدر الإشارة إليه أنه لايجوز الحصول على معلومات تتعلق بالحياة إلا بعد موافقة صاحب الشأن ، وذلك بصرف النظر عن نشرها أو عدم نشرها وللشخص أن يعترض على إدخال معلومات تم الحصول عليها بطريق غير مشروع . ولايتوافر الرضا إلا إذا كان صحيحاً غير معيب ويتوافر الغش إذا كانت المعلومات التي يقدمها الشخص لا تتناسب مع الميزة التي يسعى إليها فعدم التناسب ينطوى على غش يعيب الرضا (١) واتفق كباحث مع الرأي القائل بأن الحصول على البيانات بطرق مشروعة من أهم الضوابط المقررة في مجال جمع البيانات وضرورة أن يكون الحصول عليها قد تم بطريقة مشروعة خالية من الاحتيال والغش (٢). ولذلك ذهب راي راجح إلى وجوب تحديد الهدف من جمع المعلومات والأشخاص الذين يحق لهم الاطلاع عليها ، كما يلزم إيضاح حقوق من يدلى بالبيانات ولهذا يجب على الجهة القائمة على جمع المعلومات إيضاح كافة الأمور للشخص . ولايجوز الحصول على المعلومات عن طريق التجسس أو التصنت التيلفوني (٣).

(١)- د/ سامى الشوا الغش المعلوماتى كظاهرة اجرامية مستحدثة ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائى القاهرة من ٢٥- ٢٨ اكتوبر ١٩٩٣م ص ٤٦

(٢)- د/ طارق عزت رجا قانون حقوق الانسان بين النظرية والتطبيق فى الفكر الوضعى والتشريعية الاسلامية كلية الحقوق جامعة المسيرة الكبرى طبرق الجماهيرية الليبية - دار النهضة العربية ٢٠٠٤م ٢٠٠٥م ص ١٨٨

(٣)- د/عفيفى محمود التطورات الحديثة فى تكنولوجيا المعلومات مرجع سابق ص ٧١ - لقد أدت تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع بزوغ تكنولوجيا إنترنت الأشياء، والحوسبة السحابية، والذكاء الاصطناعي وغيرها، إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبق، مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد - راجع: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشؤون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يولية ٢٠١٩ ، ص ٨ وما بعدها، متاح على الموقع التالى:

<https://www.elwatannews.com/data/iframe/pdf/25021748.pdf>

ونظراً لاهتمام الدولة فى الوقت الحاضر بتشجيع الاستثمارات فى مجال صناعة مراكز البيانات العملاقة، هادفةً لأن تصبح مصر ممراً رقمياً عالمياً، ولما كان ذلك يتطلب وجود بيئة تشريعية مناسبة، فقد حرصت الحكومة وأعضاء مجلس النواب على إعداد وصياغة مشروع قانون حماية البيانات الشخصية بما يضمن خصوصية المواطنين والعمل على تهيئة المناخ الاستثماري فى مصر، وحتى يكون متسقاً مع اللائحة العامة لحماية البيانات GDPR الصادرة عن الاتحاد الأوروبي ()، باعتبارها التغيير الأكثر أهمية فى تنظيم خصوصية البيانات على المستوى العالمى خال العشرين عاماً الماضية، ولتأثر الكيانات غير الأوروبية التى تستخدم خدمات الانترنت بأحكامه - دخلت اللائحة العامة لحماية البيانات GDPR حيز التنفيذ يوم ٢٥ مايو ٢٠١٨ ، وتنطبق على جميع المؤسسات داخل وخارج الاتحاد الأوروبي التى تتعامل مع بيانات سكان منطقة الاتحاد الأوروبي وتعالجها. ويكمن الغرض من اللائحة فى تقوية حماية البيانات ومنح الأشخاص قدرًا أكبر من التحكم فى الطريقة التى يتم بها استخدام وتخزين ومشاركة معلوماتهم الشخصية من قِبل المؤسسات التى لها حق الوصول إليها، بدءًا من أصحاب العمل ووصولاً إلى الشركات التى يشتري هؤلاء الأشخاص أو يستخدمون منتجاتها وخدماتها. كما تفرض GDPR على المؤسسات أن تضع حيز التنفيذ عناصر فنية وتنظيمية للتحكم فى الأمان والمصممة لتفادي فقدان البيانات، أو تسريب المعلومات، أو الاستخدامات الأخرى غير المصرح به للبيانات - فعلى سبيل المثال أعلنت شركة ميكروسوفت العملاقة عبر موقعها عن التزامها تجاه الامتثال للقانون العام لحماية البيانات (GDPR) (، راجع الموقع التالى:

<https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview>

المطلب الثاني

أن تكون صحيحة وسليمة ومؤمنة

اشترط المشرع أن تكون لجمع البيانات ومعالجتها والاحتفاظ بها ضرورة توافر الشروط الآتية:
أن تكون صحيحة وسليمة ومؤمنة" (١) بيد أن صياغة هذا النص توجي لأول وهلة باشتراط
الصحة والسلامة والتأمين لعمليات الجمع والمعالجة، بيد أن المقصود بها هو أن تكون
"البيانات" صحيحة وسليمة ومؤمنة، حتى يمكن جمعها ومعالجتها.

(١)- المادة رقم (٣) من القانون ١٥١ لسنة ٢٠٢٠م قانون حماية البيانات الشخصية المصري - وقد راعت اللائحة الأوروبية هذا الأمر، في المادة ٥ منها) الخاصة بالمبادئ المتعلقة بمعالجة البيانات، في البند د، مع اختلاف في الصياغة، فنصت على ضرورة أن تكون البيانات بالشخصية دقيقة accurate ، ويجرى تحديثها kept up to date عند الضرورة؛ ويجب اتخاذ الإزم لضمان محو أو تصحيح البيانات الشخصية غير الدقيقة دون تأخير، مع مراعاة الأغراض التي تتم معالجتها من أجلها) ("الدقة"). accuracy" ويقضي ذلك من المعالج أو المتحكم قبل البدء في جمع أو معالجة البيانات الشخصية، أن يتحقق من أن البيانات التي تم جمعها أو معالجتها ذات صلة بالأغراض المشروعة أو كافية لتحقيقها، كما يجب التحقق من أن تلك البيانات دقيقة ومكتملة وحديثة بما يفى بالأغراض المشروعة. كما يتطلب هذا الإلتزام التحقق من دقة البيانات أو المعلومات الشخصية والمسجلة لديه بأنظمة المعلومات والمتعلقة بالشخص المعنى بالبيانات وإستكمالها وتحديثها بانتظام والقيام بمحو أو تعديل أي بيانات أو معلومات تتعلق بها. كذلك تشير اللائحة الأوروبية في المادة ٥ بند ج، إلى ضرورة أن تكون البيانات الشخصية ملائمة adequate وذات صلة ومحددة limited لما هو ضروري بالنسبة للأغراض التي تتم معالجتها من أجلها) (الحد الأدنى من البيانات). data minimization وبالنسبة للإلتزام بسامة المعالجة security of processing أأزم المشرع المصري في المادة الرابعة) بند ٦) من قانون حماية البيانات الشخصية "اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظاً على سريتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قبل أي إجراء غير مشروع". . يرجع الفضل في حماية الخصوصية على الصعيد الدولي لجهود المنظمات الدولية والإقليمية، والتي كان لها الأثر البين في صياغة النظام القانوني لخصوصية البيانات الشخصية ونجد أهم جهود المنظمات الدولية والإقليمية في مجال حماية لخصوصية البيانات الشخصية، واضحة فيما يلي:- أ. الإعان العالمي لحقوق الإنسان الصادر عام ١٩٤٨ : حيث يرسخ الحق في الخصوصية، بشكل واضح في المادة ١٢ منه التي تنص على أن: "لا يجوز تعريض أي شخص للتدخل التعسفي في خصوصياته أو في شئونه الأسرية أو المنزلية أو في مراسلاته، ولا حتى إثارة حمت تستهدف شرفه وسمعته. ويمتلك كل إنسان الحق في الحصول على حماية القانون ضد مثل هذا التدخل أو تلك الهجمات ب - قرار الجمعية العامة للأمم المتحدة بشأن الحق في الخصوصية في العصر الرقمي عام ٢٠١٣ : حيث اعتمدت الجمعية العامة في ٢٠ ديسمبر ٢٠١٣، بالإجماع، وبدون تصويت، القرار رقم (٦٨ / ٦٧) بشأن الحق في الخصوصية في العصر الرقمي، ليدعم بقوة "احترام وحماية الحق في الخصوصية"، داعياً جميع الدول إلى اتخاذ التدابير اللازمة لوضع حد للأنشطة التي تنتهك هذا "المبدأ الأساسي للمجتمع الديمقراطي، ومعرية عن قلقها إزاء التأثير السلبي للمراقبة الإلكترونية واعتراض الاتصالات الرقمية وجمع البيانات الشخصية، على حقوق الإنسان. ج - المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD) عام ١٩٨٠ : وهي مجموعة قواعد لحماية الخصوصية ولضمان نقل البيانات ذات الطبيعة الشخصية عبر الحدود، وتبني مجلس المنظمة هذه القواعد وصدقت عليها العديد من الدول، وتعد تلك المبادئ إرشادية غير ملزمة بحيث لا يتم توقيع جزاءات على الدول الأعضاء حال مخالفتها، ولكن لا يمكن أغفال أهمية ما أفرزته هذه المبادئ من قواعد تشريعية وإدارية تتعلق بالحصول على البيانات عبر وسائل عادلة ومشروعة، واستخدامها في الاغراض المحددة سلفاً والتي تم على أساسها جمع البيانات وذلك بعد موافقة أصحابها، هذا بالإضافة إلى مبدأ الوفاية الأمنية للبيانات الشخصية خال مراحل الجمع والتخزين والنقل والمعالجة، ومبدأ مشاركة الأفراد بحيث يحق للمواطنين الاطاع على البيانات الخاصة بهم وأحقيتهم في تعديلها ومحوها. د - توجيهات الاتحاد الأوروبي بشأن معالجة البيانات الشخصية: فقد سعي الاتحاد الأوروبي لتوحيد قواعد حماية الخصوصية اعتباراً من عام ١٩٧٦ ، حيث أصدر التعليمات رقم ٨ / ٤ / ٧٦ المتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات The protection of the individual against the technical evolution of informatics ، والتعليمات رقم ٨ / ٥ / ٧٩ المتعلقة بحماية 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 ينص التوجيه الأوروبي رقم ٩٥ / ٤٦ في مادته السادسة على المبادئ الأساسية لحماية البيانات حيث يقرر ضرورة مراعاة التعامل مع البيانات الشخصية وشروطها. - اتفاقية مجلس أوروبا: Council of Europe : وتعنى بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، وتعد تلك الاتفاقية ملزمة للدول الأطراف، وتتضمن عدة مبادئ تمثل الحدود الدنيا للقواعد التي يجب أن يتضمنها تشريع الدول الموقعة على الاتفاقية، وتتشابه هذه المبادئ مع تلك التي تقرها المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD)

وفى ذلك أيضا نص القانون البحريني - أن تكون البيانات صحيحة ودقيقة، وتخضع لعمليات التحديث عندما يكون لذلك مقتضى. (١) وقد حرص المشرع المصري أيضا على التأكد من صحة البيانات الشخصية واتفقها وكفايتها مع الغرض المحدد لجمعها وتصحيح أى خطأ بالبيانات الشخصية فور إبلاغه أو علمه به (٢)

(١)- الماد رقم (٣) من قانون رقم (٣٠) لسنة ٢٠١٨ قانون حماية البيانات البحريني - الجريد الرسمية العدد: ٣٣٧٥ - الخميس ١٩ يوليو ٢٠١٨ (٢)- المادة رقم (٤) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م - لقد أدت تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع بزوغ تكنولوجيا إنترنت الأشياء، والحوسبة السحابية، والذكاء الاصطناعي وغيرها، إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبوق، مما سمح للشركات والمؤسسات الخاصة والعامّة باستخدام البيانات الشخصية للأفراد على نطاق واسع نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد راجع: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكتب لجان الشؤون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يولية ٢٠١٩، ص ٨ وما بعدها، متاح على الموقع التالي:

<https://www.elwatannews.com/data/iframe/pdf/25021748.pdf>

ومن مبادئ الأمم المتحدة التوجيهية فى هذا الأمر ما يلى ١- مبدأالمشروعية ،٢- مبدأ الصحة ، ٣- مبدأ الغاية ،٤-مبدأ وصول الأشخاص المعنيين إلى الكمفات ،٥-مبدأ عدم التمييز ،٦- مبدأ الأمن ،٧- مبدأ الرقابة والعقوبات ٨- مبدأ تدفق البيانات عبر الحدود (المبدىء التوجيهية لتنظيم استخدام البيانات المجهزة إلكترونياً - الأمم المتحدة ، المجلس الاقتصادى والاجتماعى ٢٠ فبراير ١٩٩٠م

ومن توجيهات الإتحاد الأوربى : وضع الإتحاد الأوربى عدة مبادئ فى جمع البيانات إلكترونياً ومنها : ١- مبدأ المعالجة المشروعة للبيانات ، ٢مبدأ الهدف المحدد والمحصور ،٣- مبدأ نوعية البيانات بما يشمل علاقة البيانات بالغرض المحدد والتخلص منها عند إنتائها ،٤-مبدأ المعالجة العادلة بما يضمن الشافية ويعزز الثقة ،٥- مبدأ المسؤولية والمحاسبة . راجع فى ذلك

European Union Agency for Fundamental Rights, and Council of Europe, Handbook on European data protection

.law, Luxembourg: Publications Office of the European Union, 2014, pp 61-76

ويحظر تخزين البيانات الاسمية التى من شأنها أن تظهر مباشرة أو غير مباشرة الأصل العرقى أو الآراء السياسية أو الفلسفية أو الدينية أو الإلتواء النقابى للشخص أو تتعلق بصحته أو علاقته الجنسية فلايجوز أن يتضمن الاسنبيان أى سؤال يتضمن هذه الامور ، كما لايجوز تخزينها فى حالة الحصول عليها بطريق مشروع . ولايجوز أن يتضمن طلب الاستخدام أسئلة عن الإلتواء النقابى والآراء السياسية راجع فى ذلك د/ عفيفى محمود التطورات الحديثة فى تكنولوجيا المعلومات مرجع سابق ص ٢٦٩ . ولذلك نحرص التشرىعات المقارنة على حظرها حتى ولولم تتصل مباشرة بالحياة الخاصة ، وذلك حماية للحريات عموما . إن معالجة البيانات الشخصية تتمثل فى كل عملية يكون من شأنها جمع البيانات أو تسجيلها أو حفظها أو تنظيمها أو تغييرها أو استغلالها واستعمالها أو نشرها وتوزيعها . ولكى تصبح المعالجة مشروعة وقانونية يتعين توافر بعض الشروط راجع د/ سامح عبد الواحد التهامى مرجع سابق ص ٥٠٤ . بحيث إذا توافرت أصبح أصبح القائم بها بمنأى عن سيف المسؤولية وأضحت معالجتها للبيانات عمل مشروع ، معالجة البيانات الشخصية نشاط لايجوز مزاولته إلا بعد الحصول على تصريح أو ترخيص أو إذن مسبق من الجهة الإدارية المختصة بذلك.وقد أشارت بعض التشرىعات إلى مجموعة من البيانات التى يجب أن يضمنها طلب الترخيص كاسم المسؤل عن معالجة البيانات الشخصية ولقبه ومقره ،أهداف المعالجة ومواصفاتها أصناف المعالجة ومكانها وتاريخ بدايتها ، البيانات الشخصية المطلوب معالجتها ومصدرها ، الأشخاص أو الجهات التى يمكنهم من الإطلاع على المعطيات بحكم عملهم مكان حفظ المعطيات الشخصية موضوع المعالجة ومدته ،الجهات المسفيدة من المعطيات موضوع المعالجة التدابير المتخذة للحفاظ على سرية المعطيات وأمانها الإلتزام بمباشرة معالجة المعطيات الشخصية وفق المقصبيات الواجبة قانونا راجع قانون البيانات الشخصية التونسى ٦٣ لسنة ٢٠٠٤ . وأكد المشرع التونسى على " أن تخضع كل عملية معالجة معطيات شخصية إلى تصريح مسبق يؤدع بمقر الهيئة الوطنية لحماية المعطيات الشخصية " ويقدمطلب الحصول على الترخيص أو الإذن من قبل المسؤل عن المعالجة أو ممثله القانونى ،ولايعفى التصاريح من المسؤولية إزاء الغير وقد اعتبرت بعض التشرىعات أن تقديم طلب الحصول على التصريح دون اعتراض من قبلالجهة الإدارية خلال أجل معين من تاريخ تقديمه قبولا الفصل السابع من ذات القانون. وأقر المشرع التونسى عقوبة السجن والغرامة لكل من تعمد معالجة البيانات دون تقديم التصريح أو استمر فى المعالجة بعد منعه أو سحب الترخيص مع المسؤولية المدنية عن الأضرار

المطلب الثالث

أن تعالج بطريقة مشروعة وملائمة

للأغراض التي تم تجميعها من أجلها

لم يكتف المشرع المصري بالنص على ضرورة جمع البيانات بطريقة مشروعة، وإنما اشترط أيضاً، في المادة الثالثة (فقرة أولى، بند ٣) "أن تُعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها". (١) ويعني هذا الشرط عدم جواز جمع أو تجهيز أو تسجيل أية بيانات شخصية أو معلومات بأساليب أو بطرق غير مشروعة أو بغير رضا الشخص المعنى أو من ينوب عنه (٢) لذلك يحظر على القائمين على معالجة البيانات القيام بجمعها أو تسجيلها بأساليب أو بطرق غير مشروعة. وحتى يسوغ القول بأن عملية جمع البيانات قد تمت بطريقة مشروعة، فإنه يجب أن يتم إعام الشخص المعنى بالبيانات عن وجود تجميع لهذه البيانات وعن طريقة التجميع والغرض من التجميع وأنواع البيانات التي تم تجميعها (٣)

وفي الإتجاه نفسه نصت اللائحة الأوروبية، في المادة ٥ (الخاصة بالمبادئ المتعلقة بمعالجة البيانات الشخصية)، بند أ، على أن تكون البيانات قد تم معالجتها بطريقة مشروعة *lawfully* وعادلة *fairly* وبطريقة شفافة *transparent* بالنسبة لصاحب البيانات (المشروعية *lawfulness* والعدالة *fairness* والشفافية). *transparency* ومن ثم تتطلب عملية معالجة البيانات أن تجري بدقة وأمانة من المتحكم أو المعالج وعدم استخدام أية وسائل إحتيالية أو غير مشروعة لجمع ومعالجة البيانات، وكذلك يحظر القيام بجمع بيانات شخصية لأغراض غير مشروعة، أو مخالفة للنظام العام، أو بيانات شخصية غير صحيحة، أو غير ضرورية لنشاط المعالجة

وقد نص القانون البحريني كذلك على - ١ أن تكون معالجتها منصفة ومشروعة. - ٢ أن تكون قد جُمعت لغرض مشروع ومحدد وواضح، و ألا تتم معالجتها لاحقاً، و ألا يتم إجراء معالجة لاحقة لها على نحو لا يتوافق مع الغرض الذي جُمعت من أجله، ولا تُعدُّ معالجة غير متوافقة مع الغرض الذي جُمعت من أجله البيانات المعالجة اللاحقة لها التي تتم حصراً لأغراض تاريخية أو إحصائية أو للبحث العلمي، وبشرط ألا تتم لدعم اتخاذ أيِّ قرار أو إجراء ب [ش] أن فرد محدد. - ٣ أن تك ون كافية وذات [صلة] وغير مفرطة بالنظر للغر [ض] من جُمعها أو الذي تمت المعالجة اللاحقة لأجله. (٤)

(١)- المادة رقم (٣) فقرة ٣ من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م

(٢)- د. عمرو طه بدوي: مرجع سابق، ص ١٠٥ .

(٣)- د. سامح عيد الواحد التهامي: الحماية القانونية للبيانات الشخصية، مرجع سابق، ص ٤٠٤ .

(٤)- المادة رقم (٣) من قانون حماية البيانات الشخصية البحريني قانون رقم (٣٠) لسنة ٢٠١٨م

ولذلك نتفق مع الرأي الفقهي القائل بأنه يجب أن يكون البيان المراد تسجيله متنسباً وضرورياً للغرض المقصود ، كما يجب أن يكون الهدف مرتبطاً بمهمة ووظيفة الجهة القائمة على الحاسب الآلي ، مع مراعاة مقتضيات الحفاظ على الحق في الخصوصية ، فإذا كان يجب على وزارة الاتصالات أن توضح المكالمات التليفونية الأرقام التي تم الاتصال بها إلا أنه حفاظاً على سرية الاتصالات يجب إخفاء بعض أرقام تليفون المشترك المطلوب (١).

(١) مايسل موقف التريع الفرنسي واتجاهات القضاء المتعلقة بحماية المعلومات الشخصية – المجلة الدولية للقانون المقارن ١٩٨٧ ص ٥٧١ وما بعدها - يشهد العالم تطوراً غير مسبوق في مجال تكنولوجيا المعلومات وتبادل المعلومات الرقمية، وقد صاحب هذا التطور مسألة حماية البيانات، حيث تُعد قضية خصوصية البيانات من أكثر القضايا المتعلقة بالمخالفات الرقمية راجع في ذلك (١) د. علاء عيد طه: الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية (٢٠١٦) الصادرة عن البرلمان الأوروبي، / وتداولها (دراسة في ضوء اللائحة التنظيمية رقم ٦٧٩ . ١٤٤١ / ٥ ٢٠٢٠ م، ص ٣) (مجلة جامعة الملك سعود ، الحقوق والعلوم السياسية، مج (٣٢) - وفي فرنسا أكدت وأيدت محكمة النقض الفرنسية الحكم الصادر من محكمة استئناف ريمس بمعاقبة شخصين أحدهما بالسجن لمدة ستة أشهر وغرامة ٥٠ ألف يورو والثاني بغرامة ٢٠٠٠ يورو بسبب القيام بمعالجة بيانات شخصية دون الحصول على إذن ، نقض فرنسي الدائرة الجزائية جلسة ١٨ يناير ٢٠١٧ مأخوذ من الموقع الإلكتروني التالي <https://www.legifrance.gouv.fr/recguri-gudi.reprise-true-fastreqid-15050935377page3>

ويتضح مما سبق أن معالجة البيانات لا تكون مشروعاً وصحيحة إلا إذا أعطى صاحب البيانات موافقته على معالجتها وفقاً لغرض من المعالجة ومعنى ذلك أنه لا يمكن القيام بمعالجة البيانات إلا إذا كان الشخص المعنى قد عبر بما لا يدع مجالاً للشك عن رضاه عن العملية أو مجموع العمليات المزمع إنجازها راجع المادة (٤) من قانون معالجة البيانات الشخصية المغربي فالموافقة على معالجة البيانات يجب أن تكون بعيدة تماماً عن استعمال الحيل أو العنف أو التهديد لذلك فقد نص المشرع التونسي في المادة ٨٨ على " يعاقب بالسجن مدة عام وبخطية قدرها عشرة آلاف دينار كل من حمل شخصاً على إعطاء موافقته على معطياته الشخصية باستعمال الحيلة أو العنف أو التهديد " ونص المرح التونسي أيضاً على " لا يمكن معالجة المعطيات الشخصية إلا بموافقة صريحة وكتابية للمعنى بالأمر وإذا كان قاصراً أو محجور عليه أو غير قادر على الامضاء تخضع الموافقة للقواعد العامة القانونية وللمعنى بالأمر أو وليه الرجوع في الموافقة في كل وقت " فالأذن الذي يعطيه صاحب البيانات لمعالجة بياناته يمتد ليشمل أي صور التعبير الحر والواضح والمحدد الذي يبديه بعد تلقيه المعلومات ويسمح بمعالجة بياناته الشخصية . ونصت المادة ٤٣ من القانون العماني رقم (٦٩) لسنة ٢٠٠٨ على " يجوز لأي جهة حكومية أو مقدم خدمات تصديق أن يجمع بيانات شخصية مباشرة من الشخص الذي تجمع عنه البيانات أو من غيره بعد الموافقة الصريحة لهذا الشخص ، ولا يجوز جمع البيانات أو معالجتها أو استخدامها لأي غرض آخر دون الموافقة الصريحة للشخص المجموعة عنه البيانات " . ونظراً لأهمية الحصول على موافقة صاحب البيانات قبل القيام بمعالجتها حيث أن موافقته على المعالجة أو رفضه من الأمور الثابتة التي يتعين أخذها بعين الاعتبار فقد اتجهت بعض التشريعات إلى منع القائم بالمعالجة من القيام بها بغير رضاه الشخص أو من ينوب عنه حيث أكدت المادة (٣٥) من القانون التونسي على الآتي " يحظر على الجهات المذكورة بالمادة (٣٢) ما يلي أ- جمع أو تسجيل أي بيانات أو معلومات شخصية من تلك المنصوص عليها في المادة (٣٢) بغير رضاه الشخص أو من ينوب عنه " كما أوجب القانون التونسي إعلام الأشخاص الذين تم جمع بياناتهم مسبقاً بطلب كتابي متضمن نوع البيانات المراد معالجتها ، وأهداف المعالجة ، ومدة حفظها ، واسم الشخص الطبيعي أو المعنوي المستفيد من البيانات واسم المسؤول عن المعالجة حيث نص في الفصل ٢٧ من القانون التونسي " على أن لا يمكن معالجة المعطيات الشخصية إلا بالموافقة الصريحة والكتابية للمعنى بالأمر راجع في ذلك قانون حماية المعطيات الشخصية التونسي لرقم ٤٣ لسنة ٢٠٠٤ . وهناك بعض الحالات التي يستغنى فيها عن الموافقة كالحالة التي تعود فيها معالجة البيانات بالمصلحة عليه وتعذر الاتصال به أو كان الحصول على موافقته يتطلب مجهوداً مرهقاً أو إذا كانت معالجة البيانات يقتضيها القانون أو اتفاق يكون صاحب البيانات طرفاً فيها كما هو الحال في حالة تنفيذ عقد يكون الشخص المعنى طرفاً فيه أو لتنفيذ إجراءات للشخص المعنى إذا كان من الناحية البدينية أو القانونية غير قادر على التعبير عن رضاه أو لتنفيذ مهمة تدخل ضمن الصالح العام أو لانجاز مصلحة مشروعة يتوخاها المسؤول عن المعالجة مع مراعاة عدم تجاهل مصلحة الشخص المعنى أو حقوقه وحرياته الأساسية " راجع في ذلك المادة (٤) من القانون ٨ الصادر في فبراير ٢٠٠٩ م حماية المعطيات الشخصية بالمغرب . وقد نص المشرع المغربي أيضاً في المادة ٥٥ من القانون المغربي رقم (٨) لسنة ٢٠٠٩ م يعاقب بالحبس والغرامة كل من احتفظ بالبيانات الشخصية لمدة تزيد عن المدة المنصوص عليها في القانون أو التصريح أو الأذن " . ونصت المادة (١٣) من اللائحة الأوروبية رقم (٦٧٩) الصادرة سنة ٢٠١٦ م على المراقب عند قيامه بجمع البيانات الشخصية المتعلقة بصاحب تلك البيانات أن يخطر بعبءه معلومات منها على سبيل المثال أغراض المعالجة، اليمسقيدين وأن يقدم المراقب وقت الحصول على البيانات بعض المعلومات التي تتعلق بتفاصيل الاتصال الخاصة بموظف حماية البيانات وممثل المراقب .

المطلب الرابع

تأقيت تخزين البيانات بمدة محددة للوفاء بالغرض المحدد لها

حظر المشرع المصري، في المادة الثالثة من قانون حماية البيانات الشخصية، الفقرة الرابعة بند ٤، أن يتم الاحتفاظ بالبيانات التي يتم معالجتها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها (١) فالاحتفاظ بالبيانات لا يجوز أن يكون أبدياً بل يكون مؤقتاً ومحدداً لمدة معينة، ويعنى ذلك أنه يتعين على المعالج أن يقوم بحفظ البيانات التي تمت معالجتها لمدة زمنية معينة بحيث لا تتجاوز المدة المطلوبة للأغراض التي جمعت من أجله (٢).

وتأكيداً على هذا الشرط اتجهت اللائحة الأوروبية، في المادة ٥ بند ٥، إلى ضرورة أن يتم معالجة البيانات في شكل يسمح بتحديد هوية صاحب البيانات لمدة معينة، لا تزيد عما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها. ومع ذلك أجازت المادة نفسها (بند ٥)، لأغراض معالجة البيانات الشخصية، تخزين البيانات الشخصية لفترات أطول، لأغراض الأرشفة من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية، مع مراعاة التنفيذ الفني والتنظيمي المناسب واتخاذ التدابير المطلوبة للحفاظ على حقوق وحرريات صاحب البيانات.

وأؤكد كباحث أن النص السابق أصابه القصور والعيور حيث لم يحدد المشرع المصري ضابطاً معيناً لتحديد مدة الاحتفاظ بالبيانات وكان يجب تحديد مدة الاحتفاظ بالبيانات، وكذلك ان يفرض المشرع عقوبة وجزاء في حال الاحتفاظ بالبيانات لمدة أطول من المدة المحددة. وتتفق مع الراى الفقهي الذى يؤكد على أن تأقيت الاحتفاظ بالبيانات الشخصية من المبادئ والضوابط الأساسية اللازمة لحماية حقوق الشخصية الاحتفاظ بالبيانات الشخصية لمدة محددة، فلا يحتفظ بالبيانات إلا للمدة المحددة في طلب إنشاء الحاسب أو لمدة تزيد على المدة اللازمة لتحقيق الغرض من تجميع البيانات واحتياجات البرنامج (٣)

(١)- المادة رقم (٣) فقرة ٤/ من قانون ١٥١ لسنة ٢٠٢٠م

(٢)- د. عمرو طه بدوي: مرجع سابق، ص ١٠٢، ١٠٣.

(٣)- أستاذنا الدكتور محمد حسام محمود لطفى الحماية القانونية لبرامج الحاسب الإلكتروني - دار الثقافة للطباعة والنشر - القاهرة ١٩٨٧ ص ١٣٤ - الاحتفاظ بالبيانات يكون مؤقتاً ومحدداً لمدة معينة والأ يحتفظ بها لمدة تزيد على المدة الضرورية لتحقيق تلك الأغراض ويلتزم القائم بالمعالجة بالاحتفاظ بالبيانات لمدة معينة وإعلام الشخص الذى ستجمع عن بياناته الشخصية بها مسبقاً وهذا مناص عليه القانون التونسي لرقم ٤٣ لسنة ٢٠٠٤ فى الفصل الحادى والثلاثون . ومشروعية معالجة البيانات تقتضى عدم المساس بالأمن أو النظام العام أو أن تكون منافية للأخلاق أو الآداب العامة حيث أكدت المادة ٥١ من القانون المغربى " يمكن للجنة الوطنية حسب الحالات وبون أجل سحب توصيل التصريح أو الأذن إذا تبين بعد إجراء المعالجة موضوع التصريح أو الأذن المنصوص عليهما فى المادة ١٢ من هذا القانون أن هذه المعالجة تمس بالأمن العام أو النظام العام أو منافية للأخلاق أو الآداب العامة راجع قانون رقم ٨ لسنة ٢٠٠٩ حماية المعطيات الشخصية بالمغرب وأكدت المادة ٤٨ من قانون المعاملات الإلكترونية العماني حيث نصت على أن "لا يجوز معالجة البيانات الشخصية بواسطة أى مسيطر على البيانات إذا كانت للمعالجة تسبب ضرراً للأشخاص الذين جمعت عنهم البيانات أو تنال من حقوقهم أو حرياتهم " كما نصت المادة ٥٤ من القانون المغربى رقم ٨ لسنة ٢٠٠٩ يعاقب بالحبس والغرامة كل من تولى جمع بيانات ومعطيات غير مشروعة

وفى القانون البحريني لا تبقى في صورة تسمح بمعرفة صاحب البيانات بعد استنفاد الغرض من جمعها أو الذي تتم المعالجة اللاحقة لأجله. وتُحفظ البيانات التي يتم تخزينه لفترات أطول لأغراض تاريخية أو إحصائية أو للبحث العلمي في صورة مجهولة بتحويله ، وذلك بوضعها في صورة لا تُمكن من نسبة هذه البيانات إلى صاحبه او يتعيّن إن تُعدّر ذلك تفسير هوية أصحابها.(١)

(١)المادة (٣) من قانون حماية البيانات الشخصية البحريني رقم ٣٠ لسنة ٢٠١٨ م - وتجدر الإشارة إلى أن المشرع المصرى فى قانون حمايةالبيانات الشخصية أخفق واصاب عمله القصور يُلاحظ: أن نص المادة (٣ فقرة أولى، بند ١) اقتصر على حالة جمع البيانات، ولم يذكر المعالجة أو الاحتفاظ بالبيانات فى هذه الفقرة، علماً بأن صدر الفقرة بنص على ضرورة توافر بعض الشروط فى حالة الجمع والمعالجة والاحتفاظ بالبيانات أن يراعى القانون ضبط هذا الشرط، بأن تجمع البيانات "وتعالج ويحتفظ بها" لأغراض مشروعة ومحددة ومعلنة للشخص المعنى بالبيانات. ولذلك أرى كباحت أنه يجب أن يقوم المشرع بتعديل البند الثالث من المادة الثالثة من القانون بإضافة كلمة سرية اليه على أن تعالج بطريقة مشروعة و ملائمة للأغراض التي يتم تجميعها لأجلها وبما يحافظ على سريتها. كما نصت المادة (٨) من قانون المعلوماتية الفر نسي ع لى أنه: " يحظر جمع أو معالجة البيانات ذات الطابع الشخصي ، و التي من شأنها أن تكشف بشكل مباشر أو غير مباشر عن الأصول العرقية أو الأراء السياسية أو الفلسفية أو والعقيدة الدينية أو والانتماء النقابي للشخص أو التي تتعلق بصحته او بحياته الجنسية راجع فى ذلك محمد سامى عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق فى الخصوصية، درا النهضة العربية مرجع سباق، ص ٤ . إن تجميع البيانات وإعادة بيعها أصبحت الركيزة الأساسية للربح للشركات مالكة المواقع من خلال إعادة بيعها للمواقع الإلكترونية أخرى وهو ما تعكف عليه مواقع مثل افييس بوك حتى تقوم بتجميع البيانات الشخصية ذات الميول الاقتصادية للشركات العالمية المرتبطة بتلك البيانات بل تقوم بإعادة بيعها لمنظمات نشطة فى مجالات سياسات الدول لها أغراضها الخاصة على سبيل المثال بيانات افييس يقبلها أكثر من ٣٥ ملايين موقع حول العالم من خلال الدخول إلى الموقع بعد مصادقة الحساب على افييس بوك راجع فى ذلك ٣٥ وسيم شفيق النظام القانونى لوسائل التواصل الاجتماعى دراسة مقارنة حول الحرية الشخصية والاختصاص مرجع سابق ص٦٨ ،ومما لا شك فيه أن مصلحة الفرد فى الحفاظ بأسراره الشخصية ودقائق حياته والمعلومات التي تتعلق بحياته الخاصة ، ومصلحة المجتمع فى تقويم سلوك الفرد ومعرفة المعلومات عنه ، تكون أساساً لوضع برامج التنمية ومدى مطابقة سلوكه للنظام الاجتماعى والقانونى للدولة . راجع فى ذلك أستاذنا الدكتور / أسامة عبد الله قايد الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية ٢٠٠٨ ص ٣٠ وتوفير البيانات والمعلومات له دور كبير فى التخطيط التكنولوجى بحيث إذا أتيج عبر شبكة الإتصالات يمكن الحصول عليه بسهولة ، ويطلق على ذلك التخطيط التكنولوجى الإلكتروني ، كونه يختلف عن التقليدى من حيث أنه عملية ديناميكية فى إتجاه الأهداف الواسعة والمرنة والحالية وقصيرة الأمد وقابلة للتجديد والتطور المستمر ، لما تستند عليه من معلومات وبيانات دائمة التدفق ، من مصادرها المختلفة ومن ضمنها الموظفون العموميون أنفسهم فى الجهاز الإدارى للدولى راجع فى ذلك د/ ناجح احمد عبد الوهاب – التطور الحديث للقانون الإدارى فى ظل نظام الحكومة الإلكترونية رسالة دكتوراه كلية الحقوق – جامعة القاهرة ٢٠١١ ص ٢٧١ .

المبحث الثاني

التزامات المتحكم والمعالج والحائز

وحقوق صاحب البيانات

تمهيد :

يؤدي كل من المتحكم والمعالج دوراً بالغ الأهمية وشديد الأهمية في نطاق معالجة البيانات الشخصية، لدرجة يمكن القول معها أنها في قلب القانون الجديد وجوهر أحكامه. فضلاً عن ذلك اشترط القانون على الممثل القانون للشخص الاعتباري لأي متحكم أو معالج تعيين شخص يكون مسؤولاً عن حماية البيانات الشخصية، وألقى المشرع على عاتقه لفييف من الالتزامات. وقد أدت الثورة التكنولوجية إلى إظهار مزايا نسبية عديدة لتطبيقاتها العلمية في مختلف مجالات الحياة الانسانية ، بما في ذلك نوعي الخدمات والسلع ، التي توفرها المؤسسات العامة والخاصة على السواء للمجتمع . وتمثل هذه الثورة فرصة متميزة للأفراد والحكومات ومنظمات الأعمال لتحسين جودة الحياة الأنسانية ، ونة عينتها كما أن حجم الاستثمار المتزايد في قطاع التكنولوجيا يتطلب تعظيم الفوائد المرجوة منه وتسخيرها لتسهيل الحياة والرفاهية الانسانية عموماً (١)

وفي هذا المبحث سوف نتحدث

المطلب الثاني التزامات المعالج

المطلب الأول : التزامات المتحكم

المطلب الثالث : حقوق صاحب البيانات المعالجة

(١) - د/أشرف محمد عبده - الحكومة الإلكترونية، وتطبيقاتها في البلدان العربية - دار الكتب والدراسات العربية - ٢٠١٨م - ص ٥٤ - أنشأ المعهد الفيدرالي للاتصالات (IFT) في عام ٢٠١٦ بنك بيانات للاتصالات والبث الإذاعي يعتبر سابقاً، بين السلطات التنظيمية، من حيث الشمول ومرونة المكونات النمطية. وبنك بيانات الاتصالات المكسيكية (BIT) هو موقع إلكتروني حديث جداً يعتمد على منطق ذكاء الأعمال. وهو فريد من نوعه، سواء من حيث سلسلة البيانات المتاحة (عدد المؤشرات والتواتر الزمني) أو الإمكانيات المتاحة لمعاملة واستغلال وتصوير وتصدير البيانات والتقارير انطلاقاً من التطبيق المستخدم. فهو يوفر تقارير ربع سنوية وسنوية (سلسلة تاريخية لبيانات الصناعة عموماً) من قبيل الناتج المحلي الإجمالي، الإيرادات، الاستثمار الوطني والأجنبي المباشر، العمالة، الأسعار، مؤشرات التركيز، وخدمات الشبكات المتنقلة والثابتة، وخدمات التلفزيون المفتوح والتلفزيون المدفوع، والراديو، بالإضافة إلى خدمات الجملة الرئيسية لفترات زمنية طويلة (بعضها منذ عام ١٩٧١) وبمستويات تفصيل منخفضة. ويمكن أيضاً تصور جميع البيانات من جانب المشغلين والدولة الفيدرالية بل وحتى البلديات. ومنذ عام ٢٠١٨ ، يتضمن البنك BIT أيضاً معلومات تتعلق بحيازة الطيف الراديوي بحسب المشغل ونطاق التردد وتصميم البنك BIT يسمح بالفاذ إليه من قبل طائفة من المستعملين، من الأساسيين إلى المتخصصين. ومن شأن مرونة بنك البيانات أن تمكن المستعملين من اختيار عينات فرعية من المؤشرات، وترشيح المتغيرات، واختيار السلاسل الزمنية، وإجراء العمليات الرقمية على سلسلة البيانات المتوفرة، فضلاً عن إضافة/إزالة/طرح المتغيرات في جدول ما أو رسم بياني ما. ويفضل مجموعة متنوعة من الأشكال والرسوم والأنماط والمقاييس، يمكن للمستخدم بسهولة تحديد قوالب الجداول والأشكال والتنبؤات. ويمكن بسهولة تصور البيانات والأرقام على أجهزة الحاسوب أو الهواتف الذكية أو الحواسيب اللوحية، وتنزيلها في شكل تقارير موحدة أو استعلامات مخصصة تبعاً لرغبة المستعملين المتخصصين. ومعايير المقارنة الدولية متاحة أيضاً. حيث من الممكن مقارنة المكسيك بين الاقتصادات ذات نصيب الفرد المماثل من الناتج المحلي الإجمالي وشركاء المكسيك التجاريين الرئيسيين (الأرجنتين والبرازيل وكندا وشيلي والصين وكولومبيا وتركيا والولايات المتحدة). ولا تقتصر المقارنات على خدمات الاتصالات الثابتة والمتنقلة التقليدية فحسب، بل تشمل أيضاً تغلغل الاشتراكات السمعية البصرية المستقلة عن المشغل. وبالإضافة إلى ذلك، وبالشراكة مع Regulatel (رابطة الهيئات التنظيمية لا من أمريكا اللاتينية ومنطقة البحر الكاريبي فحسب بل من أوروبا - إيطاليا والبرتغال وإسبانيا - أيضاً)، يتلقى المعهد IFT ويعالج إحصاءات ربع سنوية من ٢٢ بلداً (بما فيها المصدر: () Banco de Información de Telecomunicaciones :https://bit.ift.org.mx/BitWebApp/

المطلب الأول

التزامات المتحكم

أولاً: التزامات المتحكم :

المتحكم وفقاً لقانون حماية البيانات الشخصية هو أى شخص طبيعي أو اعتباري يكون له بحكم أو بطبيعة عمله الحق في الحصول على البيانات الشخصية ، وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه (١) ويضع قانون حماية البيانات الشخصية التزامات أساسية على الأفراد والجهات التي قد تحوز البيانات الشخصية للمستخدمين ، سواء كانت حيازة البيانات لأسباب تتعلق بطبيعة عملها أو لأى سبب آخر . ويفرق القانون بين هذه الالتزامات ، حسب طبيعة الأشخاص الذين يتعاملون مع البيانات الشخصية كالحيازة والتحكم والمعالجة المختلفة للبيانات الشخصية.

ولذلك أويد كباحث الرأى الفقهي القائل : لقد ظهرت مع التكنولوجيا مايسمى ببنوك المعلومات ، ويقصد بها تكوين قاعدة بيانات موضوعاً معيناً ، وتهدف لخدمة غرض معين ، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات ، تفيد مستخدمين مختلفين في أغراض متعددة ، فيما تحتوى عليه من معلومات عن الفرد ومايخزن عنه من بيانات تشكل عنصر تضيق ، وتقليل انطلاقات الفرد وإبداعه ومشاركته في شئون الحياة العامة ، والسبب الرئيسي أو الاساسى في ذلك ، يرجع إلى أنه أصبح محوراً لعمليات آلية مختلف تمسها في كل جانب من جوانب حياته المتشعبة . الحاسوب يقوم بجمع وتخزين ومعالجة ونشر المعلومات الشخصية للأفراد ولكل أمر من هذه الامور ، يشكل خطراً أو آخر على حياة الانسان الخاصة ، ويهددها ، لذا فإن الفرد يصبح أسيراً للمعلومات التي جمعتها هذه الألة عنه ورصدت كل تحرك من تحركات حياته (٢)

(١)- المادة رقم (١) من قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠م

(٢)- (د/ محمد رشيد حامد - الحماية الجزائية للمعلومات الشخصية في مواجهة أخطار البنوك - رسالة ماجستير - كلية الحقوق - جامعة آل البيت - ص (٤) . وبما أن البيانات ذات الطابع الشخصي هي أحد أهم الحقوق للصيقة بالشخصية والمرتبطة بالحياة الخاصة للفرد، فإن المعالجة الآلية لهذه البيانات تتطلب أخذ الاحتياطات اللازمة، واحترام الإجراءات الخاصة الواجب إتباعها أثناء هذه العملية، ومنها احترام الغرض الذي من أجله تم السماح القانوني بمعالجة هذه البيانات ولا تتعداه إلى غيره من الأغراض، وقد جرم قانون العقوبات الفرنسي هذا الفعل وعاقب عليه.راجع في ذلك د. بولين أنطونيوس أيوب، المرجع السابق، ص ٤٠١- وأرى كباحث أن الإدارة الإلكترونية أعطت لجهة الإدارة صلاحيات كبيرة في مواجهة مراقبة الأفراد على شبكة المعلومات وذلك بواسطة برامج خاصة تمكنهم من رصد تحركات الأفراد ومن هذه المجالات التعرض للخصوصية ومنها خصوصية البيانات . لذلك هب رأى فقهي إلى أن خصوصية البيانات الرقمية هي المعاملات التي تتم عن طريق الألة أو وسيط إلكتروني بداية من ماكينة الصراف الألى وصولاً إلى جهاز الحاسب الألى ، ومع التطور التكنولوجي السريع صارت معظم معاملاتنا ، في الحياة اليومية تتم بشكل رقمي .

تضمن قانون حماية البيانات الشخصية المصري التزامات على المتحكم (١) كالاتي :

(١)- الحصول على البيانات الشخصية أو تلقيها من الحائز او من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعنى بالبيانات أو في الاحوال المصرح بها قانوناً .

تُلقي هذه الفقرة على عاتق المتحكم التزاماً بالتأكد من موافقة الشخص المعنى بالبيانات وإثبات هذه الموافقة) . وقد وضع المشرع الأوروبي نفس الالتزام على عاتق المتحكم

في المادة السابعة منه، حيث يجري نصها على أن:-١- عندما تعتمد المعالجة على الموافقة، يجب أن يكون المتحكم قادراً على إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية.-٢- إذا كانت موافقة صاحب البيانات مقدمة في سياق إعان مكتوب يتعلق أيضاً بأمر أخرى، فيجب تقديم طلب الموافقة بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، وفي شكل واضح يسهل الوصول إليه، وباستخدام لغة واضحة ومفهومة، وأي جزء من هذا الإعان يشكل انتهاكاً لهذه اللائحة لن يكون ملزماً.-٣- يحق لصاحب البيانات سحب موافقته في أي وقت، ولن يؤثر سحب الموافقة على قانونية المعالجة، طالما كان هناك سابقة موافقة. وجدير بالذكر في هذا الصدد وجود اتفاق بين مسلك كل من المشرعين المصري والأوروبي على أن الحصول على موافقة الشخص المعنى بالبيانات على المعالجة يقع على عاتق المتحكم، إلا أنهم اختلفوا في طريقة اشتراط ذلك.

(١)-المادة رقم (٤) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م وتجدر الإشارة إلى نص قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م في المادة رقم (٢) منه على الآتي : أولاً يلتزم مقدمو الخدمة بما يأتي :١- حفظ وتخزين سجل النظام المعلوماتي أو أى وسيلة لتقنية المعلومات ، لمدة مائة وثمانون يوماً متصلة . وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي : (أ)- البيانات التي تمكن من التعرف على مستخدم الخدمة

(ب)- البيانات المتعلقة بمحتوى ومضمون الطام بالمعلوماتي المتعامل فيه متى كانت تحت سطرة مقدم الخدمة .

(ج)- البيانات المتعلقة بحركة الاتصال .

(د) البيانات المتعلقة بالأجهزة الطرفية للاتصال .

(هـ) - أى بيانات أخرى يصدر بتحديد قرار من مجلس إدارة الجهاز . ٢- المحافظة على سرية البيانات التي تم حفظها وتخزينها ، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة ، ويشمل ذلك البيانات الشخصية لأى مستخدمى خدمته ، أو أى بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون ، أو الأشخاص والجهات التي يتواصلون معها .٣- تأمين البيانات والمعلومات بما يحافظ على سريتها ، وعدم اختراقها أو تلفها . ثانياً : مع عدم الإخلال بأحكام قانون حماية المستعملك ، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته ولاى جهة حكومية مختصة ، بالشكل والطريقة التي يمكن الوصول إليها بصورة مباشرة ومباشرة ،البيانات والمعلومات الآتية : ١- اسم مقدم الخدمة وعنوانه ٢- معلومات الاتصال المتعلقة بمقدم الخدمة ،بما في ذلك عنوان الاتصال الإلكتروني .٣-بيانات الترخيص لتحديد هوية مقدم الخدمة ، وتحديد الجهة المختصة التي يخضع لإشرافها . ٤- أى معلومات أخرى يقدر الجهاز اهميتها لحماية مستخدمى الخدمة ويصدر بتحديد قرار من الوزير المختص .وتجدر الإشارة إلى أن المشرع المصري أكد على أهمية التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات ، حيث أكد " تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلدان الاجنبية ، فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها ، أو تطبيقاً لمبدأ المعاملة بالمثل ، يتبادل المعلومات ، بما من شأنه أن يكفل تفاعل ارتكاب جرائم تقنية المعلومات ، والمساعدة على التحقيق فيها وتبني مرتكبها راجع قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م - الجريد الرسمية - العدد (٣٢) مكرر فى ١٤ أغسطس ٢٠١٨م . وفى الجزائر تضمن اعطى القانون للهيئة الوطنية دور هام فى الوقاية من جرائم الإعتداء على البيانات الشخصية حيث تتمثل مهام الهيئة الوطنية فى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها راجع فى ذلك المادة ١٤ من القانون ٤-٩ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها . وهى تلك التى تمس بأنظمة المعالجة الآلية للمعطيات المحددة فى قانون العقوبات ، وأى جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ، وتشكل اعتداء على البيانات الشخصية لاطراف المعاملة الإلكترونية نفس المرجع السابق المادة (٢). إن الحياة الخاصة لألف ا رد تحتاج فى الوقت الحاضر إلى حماية كبيرة خصوصاً بعد الانتهاكات التي تمس الخصوصية بسبب التعدي الحاصل عليها من قبل غيرهم من الافراد ، أو نتيجة تدخل السلطات العامة فيها، فإن أهداف القانونين بالتشريع فى المجتمع هو م ا رعاة الحقوق والحريات الفردية والجماعية، فهي تعد مقياساً حقيقياً لتقدم الأمم ورفقها لذلك اتجه الفقه الجزائرى المقارن فى غالبه على انه لا يوجد تناقض بين الحرية والقانون، لان الحفاظ على حرية الاف ا رد سيقابلها حتماً الحفاظ على الامن والنظام العام فى المجتمع وبالتالي سيتم الحفاظ على خصوصية الاف ا رد التي هي جزء من الحقوق والحريات إذ إن الاعتداء على حياة الانسان والتجسس عليها سيخلق شخصاً خائف أ لإصلاح لمجتمع الأحر ا ر الذي تتكلم عنه الفقرة الثانية من ديباجة الإعلان العالمي كمجتمع نموذجي لكفالة حقوق الانسان عجمالي، جمال عبد الناصر، الحماية الجنائية من اشكال المساس بحرمة الحياة الخاصة عبر المكالمات والصور، د ا رسة مقارنة ، . الجزائرى ، ص ٦

تابع التزامات المتحكم :-

(٢)- التأكد من صحة البيانات الشخية واتفاقها وكفايتها مع الغرض المحدد لجمعها . وفى هذا الإطار تقرر المادة ٢٥ بند ٢ من اللائحة الأوروبية التزاماً على عاتق المتحكم بتنفيذ التدابير الفنية والتنظيمية المناسبة لضمان أن البيانات الشخصية الضرورية فقط لكل غرض محدد للمعالجة تتم بشكل افتراضي ..

(٣)- وضع طريقة واسلوب ومعايير المعالجة طبقاً للغرض المحدد مالم يقرر تفويض المعالج فى ذلك ويتسق هذا الالتزام مع تعريف المتحكم، فى القانون المصري واللائحة الأوروبية، الذى يشير إلى أنه يكون له بحكم أو طبيعة عمله تحديد طريقة وأسلوب ومعايير الاحتفاظ بالبيانات أو معالجتها *the purposes and means of the processing of personal* أو التحكم فيها طبقاً للغرض المحدد أو نشاطه. و يمكن إعتبار هذه القاعدة هى أساس ترتيب مسؤولية المتحكم بصفته المسئول الأساسى عن حماية البيانات الشخصية. ولكن يجوز تفويض وضع طريقة وأسلوب ومعايير المعالجة طبقاً للغرض إلى المعالج بناء على تعاقد مكتوب، وهو ما قد ينبني عليه عدم وضوح الرؤية لدى تحديد المسئول الفعلي عن حماية البيانات. وأرى كباحث أن يتم ذلك التفويض وفق لمعايير تقنية واضحة .

(٤) التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها . ويهدف هذا الالتزام لضمان حيده المتحكم فى عملية جمع البيانات وضمان جمعها للأغراض المحددة للمعالجة.

(٥)- القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية ك بموجب تعاقد مكتوب . ويؤكد المشرع المصرى على

٦- اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظاً على سريتها وعدم اختراقها أو اتلافها أو تغييرها أو العبث بها قبل أى إجراء غير مشروع ونؤكد تأتي هذه الفقرة متنسقة مع الفقرة الأولى من المادة ٥ من اللائحة الأوروبية بند ٨١ حيث تنص أيضاً على مبدأ أمن البيانات، بيد أنها لم تتعرض لبيان المقصود بأمن البيانات أو وضع معايير معينة لتحديدها، بل اكتفت بتقرير أن اشتراط الأمن يجب أن يكون "مناسب *Appropriate Security*" ، وقد اتبع المشرع فى ذلك النهج القائم على قياس المخاطر " *Risk Based Approach* " وتحديد مناسبة الإجراءات الأمنية حسب حجم

المخاطر التى قد تتعرض لها البيانات ٨٢ . وعليه فمن الأفضل أن يتطرق المشرع المصري إلى وضع هذه المعايير فى اللائحة التنفيذية للقانون أو من خال اعتماد معايير عالمية أو اقتراح معايير مصرية تشرح ما هو الحد الأدنى من الأمن أو ماهو المقصود بالأمن بشكل عام.

٧- محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها ، أما فلى حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض ، فيجب الأتبقى فى صورة تسمح بتحديد الشخص المعنى ببيانات . يتماشى هذا الالتزام مع حق المحو الذي يقرره المشرع المصري للشخص المعنى للبيانات، وهو ما ورد أيضاً فى اللائحة الأوروبية، حيث أقرت حق الأفراد فى مسح ومحو البيانات الشخصية "الحق فى النسيان"

٨- تصحيح أى خطأ بالبيانات الشخصية فور ابلاغ أو علمه به . يجب أن يضطلع به المتحكم، حتى ولو لم ينص عليه القانون، نظراً لأن الخطأ فى البيانات قد يرتب ضرراً بالغاً للشخص المعنى بالبيانات، ويكون مؤثراً عليه.

٩- إمساك سجل للبيانات ، على أن يتضمن رصد فئات البيانات الشخصية لديه وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم ، وسنده والمدة الزمنية ، وقيودها ونطاقها وأليات محو البيانات الشخصية لديه أو تعديلها وأى بيانات أخرى متعلقة بنقل البيانات الشخصية ، عبر الحدود ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات . ويتسق مسلك المشرع المصري فى هذا الالتزام مع مسلك المشرع الأوروبي، حيث تنص المادة (٣٠) من اللائحة الأوروبية على أن: على كل متحكم، وعند الضرورة، ممثل المتحكم، الاحتفاظ بسجل لأنشطة المعالجة تحت مسؤوليته. ويجب أن يتضمن هذا السجل على جميع المعلومات التالية:

■ اسم وتفاصيل الاتصال الخاصة بالمتحكم، وعند الاقتضاء، المتحكم المشترك وممثل المتحكم ومسئول حماية البيانات؛ ■ أغراض المعالجة؛

■ وصف لفئات مواضيع البيانات وفئات البيانات الشخصية ؛

■ فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم أو سيتم الكشف عنها بما فى ذلك المستلمين فى دول ثالثة أو المنظمات الدولية؛

■ عند الاقتضاء، نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، بما فى ذلك تحديد ذلك البلد الثالث أو المنظمة الدولية، وفى حالة عمليات النقل المشار إليها فى الفقرة الفرعية الثانية من المادة (٤٩) ١(،) وثائق مناسبة الضمانات.

■ حيثما أمكن، الحدود الزمنية المتوخاة لمحو مختلف فئات البيانات ؛

■ حيثما أمكن، وصف عام للتدابير الأمنية التقنية والتنظيمية المشار إليها فى المادة ٣٢ / ١ .

■ يجب على كل معالج، وعند الاقتضاء ممثل المعالجالاحتفاظ بسجل لجميع فئات أنشطة المعالجة المنفذة نيابة عن المتحكم، يحتوى على اسم وتفاصيل الاتصال الخاصة بالمعالج أو المعالجين ولكل وحدة تحكم يعمل المعالج نيابة عنها، وحيثما أمكن، المتحكم أو ممثل المعالج ومسئول حماية البيانات؛ فئات المعالجة المنفذة نيابة عن كل وحدة تحكم؛ عند الاقتضاء، نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، بما فى ذلك تحديد ذلك البلد الثالث أو المنظمة الدولية، وفى حالة عمليات النقل المشار إليه فى الفقرة الفرعية الثانية من المادة ٤٩ / ١ اللائحة، وثائق مناسبة الضمانات"

١٠- الحصول على ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية . ينفرد القانون المصري بهذا الالتزام فا يوجد نظير له في اللائحة الأوروبية، فلم تشترط الأخيرة ضرورة الحصول على تصريح أو ترخيص مسبق بل اكتفت بوضع معايير وجزاءات لمخالفة هذه المعايير.

١١- يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له في خارج جمهورية مصر العربية ، وذلك على النحو الذى تبينه اللائحة التنفيذية وأرى كباحث أن استخدام ثورة المعلومات فى جمع ومعالجة البيانات الشخصية ، لأغراض متعددة كان كما ذهب رأى راجح ، نؤيده بفعل الكفاءة العالية لوسائل تقنية المعلومات الحديثة ، والقدرة الفائقة لها فى عملية تحليل واسترجاع المعلومات حيث اتجهت جميع الدول إلى إنشاء قواعد البيانات لتنظيم عملها

١٢- توفير الإمكانات اللازمة لإثبات التزامه بتطبيق أحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك ، وفى حالة وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصوص عليها فى هذا القانون . وللشخص المعنى ممارسة حقوقه تجاه كل متحكم على حدة ، وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير الفنية لتلك الالتزامات (١) . تتشابه هذه الفقرة مع مضمون المادة ٢٤ من اللائحة الأوروبية المشار إليها، حيث توضح أن الالتزام الأساسي للمتحكم هو وضع طريقة المعالجة وغرضها طبقاً للقانون ويكون هو المسؤول عن توفير الإمكانات اللازمة لذلك وعن إثبات هذا الالتزام. ولكن بخلاف اللائحة الأوروبية لم يتطرق القانون المصري إلى مبدأ التناسب (Proportionality) (٢)

تابع التزامات المتحكم فى قانون حماية البيانات الشخصية المصرى رقم ١٥١ لسنة ٢٠٢٠م - وتجدر الإشارة إلى أن اللجنة الأولى لتنظيم وحماية نظام المعلوماتية فى فرنسا كان قد صدر فى القانون رقم ٧٨ - ١٧ - الصادر فى ١٩٨٧/١/٦ فى شأن الحريات والمعلوماتية وقد عالج فيه المشرع مسألة تخزين البيانات فى الحاسب الألى ، وأنواع هذه البيانات ، ومدتها وتلك التى تخزن وتلك التى لايجوز تخزينها ، وكذلك الجهة المختصة بالرقابة والإشراف على أعمال ذلك القانون ، حيث أنشأت بمقتضاه "اللجنة القومية للمعلوماتية والحريات " وهى تختص بإجراء رقابة سابقة ورقابة نظم المعلومات - راجع فى ذلك د/ حسام الدين الأخوانى - الحاسب الألى والحياة الخاصة - ص ١٦٤ ، تنص الفقرة الأولى من المادة الخامسة بند (هـ) على أن : تتم معالجتها بطريقة تضمن الأمان المناسب للبيانات الشخصية، بما فى ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقد أو التلف أو التلغ العرضى ، باستخدام التدابير التقنية أو التنظيمية المناسبة ("النزاهة والسرية") . - يتفق ذلك أيضاً مع قانون خصوصية المستهلك فى كاليفورنيا، حيث ينص أيضاً على التزام الشركة بتوفير إجراءات أمنية مناسبة وذلك بدون تعريف ما هو مستوى الأمان المعقول " Reasonable Security " . ولكن قامت وزارة العدل بكاليفورنيا بإصدار يمكن إستخدامه لتحديد عناصر الحد الأدنى من الحماية التى يجب أن تتبعها جميع الشركات الخاضعة لنطاق القانون.. يمكن تصفح هذا التقرير الصادر بتاريخ فبراير ٢٠١٦ عبر الموقع التالى:

(١) <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

(٢) مبدأ التناسب هو مبدأ عام لللائحة الأوروبية يقيد الجهات فى ممارسة سلطاتها من خلال مطالبتهم بتحقيق التوازن بين الوسائل المستخدمة والهدف المقصود. وفى سياق الحق فى حماية البيانات الشخصية، يبدو التناسب هو التبرير لأى قيود على أى من حقوق أصحاب البيانات. لمزيد من المعلومات فضا أنظر الموقع الإلكتروني لمركز حماية البيانات الأوروبي الآتى:

(٣) https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

وفى البحرين ينص قانون حماية البيانات الشخصية رقم ٣٠ لسنة ٢٠١٨ على الاشتراطات الخاصة بمعالجة البيانات الشخصية الحساسة

تُحظر معالجة البيانات الشخصية الحساسة دون موافقة صاحبها، ويُستثنى من هذا

الحظر ما يأتي:

- ١ - المعالجة التي يقتضيها قيام مدير البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في مجال علاقة العمل التي تربطه بالعاملين لديه.
- ٢ - المعالجة الـ [] ضرورية لحماية أيّ إنسان إذا كان [] صاحب البيانات - أو الو [] صي أو الولي أو القِيم عليه - غير قادر قانوناً على إعطاء موافقته على ذلك، وبشرط الحصول على تصريح مسبق من الهيئة طبقاً للمادة (١٥) من هذا القانون.
- ٣ - معالجة البيانات التي أتاحتها صاحبها للجمهور.
- ٤ - المعالجة الضرورية لمباشرة أيّ من إجراءات المطالبة بالحقوق القانونية أو الدفاع عنها، بما في ذلك ما يقتضيه التجهيز لهذا الأمر والاستعداد له.
- ٥ - المعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الـ [] صحية من قِبَل مرخّص له بمزاولة أيّ من المهن الطبية، أو أيّ شخص ملزم بحكم القانون بالمحافظة على السريّة.
- ٦ - المعالجة التي تتم في سياق أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق ربح، وذلك بـ [] شرط الالتزام بما يأتى:
 - أ - أن تتم المعالجة في حدود ما هو ضروري للغرض الذي أن [] شئت الجمعية أو النقابة أو الجهة من أجله.
 - ب - أن ترد المعالجة على بيانات تخص أعضاء تلك الجمعية أو النقابة أو الجهة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها.
 - ج - ألا يتم الإفصاح عن البيانات لأيّ شخص آخر ما لم يوافق صاحب البيانات على ذلك.
 - ٧ - المعالجة التي تتم من قِبَل جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانوناً.

(١)- بمعالجة البيانات الشخصية الحساسة البحريني رقم ٣٠ لسنة ٢٠١٨م

تابع المادة ٥ من قانون ٣٠ لسنة ٢٠١٨م حماية البيانات الشخصية البحريني :

٨ - معالجة بيانات تتعلق بالأصل العرقي أو الإثني أو الديني إذا كانت ضرورية للوقوف على

مدى توافر المساواة في الفرص و المعاملة لأفراد المجتمع الذين ينحدرون من أصول

عرقية أو إثنية أو دينية مختلفة، وبشرط مراعاة الضمانات المناسبة لحقوق وحرمان

أصحاب البيانات المقررة قانوناً. وعلى مجلس الإدارة أن يُصدر قراراً بتحديد القواعد والإجراءات التي يتعين على مدراء

(١)- وتجدر الإشارة إلى أن المشرع المصري أكد على أهمية التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات ، حيث أكد " تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلدان الأجنبية ، في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها ، أو تطبيقاً لمبدأ المعاملة بالمثل ، بتبادل المعلومات ، بما من شأنه أن يكفل تقييد ارتكاب جرائم تقنية المعلومات ، والمساعدة على التحقيق فيها وتتبع مرتكبيها راجع في ذلك)- قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م - الجريد الرسمية - العدد (٣٢) مكرر في ١٤ أغسطس ٢٠١٨م - نماذج من أهم قضايا حماية البيانات الشخصية حول العالم قضية ماكس شريمز ضد مركز حماية البيانات الأيرلندي (Max Schrems v. Data Protection Commissioner) (٢٠١٥ قضية نُظرت أمام محكمة العدل الأوروبية بناءً على شكوى قدمها محامي يُدعى ماكس شريمز إلى مركز حماية البيانات بأيرلندا ضد فيسبوك حيث قامت الأخيرة بنقل بيانات الشاكي وبيانات مواطني الاتحاد الأوروبي بشكل عام من أوروبا إلى الولايات المتحدة الأمريكية. أدت هذه القضية إلى إلغاء محكمة العدل الأوروبية العمل باتفاقية " Safe Harbor المنظمة لنقل البيانات بين الاتحاد الأوروبي والولايات المتحدة الأمريكية.- شركة H&M ضد مركز حماية البيانات وحرية المعلومات بهامبورج H&M v. Data Protection Commissioner of Hamburg (2020) (لقد كلف عدم التزام شركة H&M) Hennes & Mauritz) بتابع الإجراءات القانونية اللازمة عند إجراء عمليات المعالجة وتحديداً التتبع والإيداع بمبالغ طائلة مؤخراً في أكتوبر من هذا العام) ٢٠٢٠ (، حيث فرض مفوض هامبورج لحماية البيانات الشخصية وحرية المعلومات غرامة قدرها ٣٥.٣ مليون يورو على الشركة بسبب انتهاكاتها للبيانات الشخصية لموظفيها؛ حيث جمعت الشركة واحتفظت بتسجيلات لموظفيها تحتوي بيانات على مستوى عالٍ من الخصوصية، ولفترات زمنية طويلة. كما تم استخدام تلك البيانات في تقييم أداء العاملين، وعمل ملفات تعريفية مفصلة لهم، تستخدم وتؤثر في اتخاذ قرارات تجاههم. والجدير بالذكر أن الموظفين لم تكن لديهم أدنى فكرة عن ذلك إلا حين حدث خطأ فني في أنظمة حواسيب الشركة مما جعل هذه البيانات متاحة لعدة ساعات في أكتوبر من العام الماضي. وارى كباحث أنه يجب بأن تكون علاقة المتحكم بالمعالج في القانون المصري بناءً على تعليمات تعاقدية واضحة، وأكدت على ضرورة أن تكون في صورة تعاقدية، على أن يفرض ذلك أيضاً على كل متحكم أو معالج من الباطن. ويجب أن تخضع أنشطة معالجة البيانات لعقد أو أي تصرف قانوني آخر مع المتحكم، على أن يحدد العقد موضوع ومدة وغرض المعالجة، وأنواع معالجة البيانات الشخصية والإجراءات الأمنية والتزامات وحقوق المعالج والمتحكم. وعند إنهاء العقد مع المتحكم، يجب على المعالج إعادة البيانات الشخصية أو حذفها، بالإضافة إلى ذلك، إذا أراد المعالج إشراك معالج آخر (معالج فرعي) يجب عليه الحصول على إذن كتابي من المتحكم كما يجب من جهة أخرى تحديد طبيعة علاقة الشخص المعنى بالبيانات مع الحائز أو المعالج أو المتحكم . وتحدد اللائحة الأوروبية موضوع المعالجة ومدتها، وطبيعة وغرض المعالجة، ونوع البيانات الشخصية وفئات أصحاب البيانات والتزامات وحقوق المتحكم ووفقاً للمادة ٢٨ فقرة ثالثة من اللائحة الأوروبية، يجب أن ينص هذا العقد أو أي تصرف قانوني آخر، على وجه الخصوص، على أن المعالج: (أ) يتولى معالجة البيانات الشخصية فقط بناءً على تعليمات موثقة من المتحكم، بما في ذلك ما يتعلق بنقل البيانات الشخصية إلى دولة ثالثة أو منظمة دولية، ما لم يكن ذلك مطلوباً بموجب قانون الاتحاد أو الدول الأعضاء الذي يخضع له المعالج ؛ وفي هذه الحالة ، يجب على المعالج إبلاغ المتحكم بهذا الشرط القانوني قبل المعالجة، ما لم يحظر هذا القانون هذه المعلومات لأسباب مهمة تتعلق بالمصلحة العامة؛ (ب) التأكد أن الأشخاص المرخص لهم بمعالجة البيانات الشخصية قد التزموا بالسرية أو خضوعهم لالتزام قانوني ملائم للسرية؛ (ج) يتخذ جميع التدابير المطلوبة عملاً بالمادة ٣٢ من اللائحة الخاصة بأمن المعالجة (د) يحترم الشروط المشار إليها في الفقرتين ٢ و ٤ لإشراك معالج فرعي؛ (هـ) مراعاة طبيعة المعالجة، ومساعدة المتحكم على اتخاذ التدابير الفنية والتنظيمية المناسبة، بقدر ما يكون ذلك ممكناً، للوفاء بالتزام المتحكم بالرد على طلبات ممارسة حقوق صاحب البيانات المنصوص عليها في الفصل الثالث؛ (و) يساعد المتحكم في ضمان الامتثال للالتزامات بموجب المواد من ٣٢ إلى ٣٦ مع مراعاة طبيعة المعالجة والمعلومات المتاحة للمعالج؛ (ز) عند اختيار المتحكم، يحذف أو يعيد جميع البيانات الشخصية إلى المتحكم بعد انتهاء تقديم الخدمات المتعلقة بالمعالجة، ويحذف النسخ الموجودة ما لم يشترط قانون الاتحاد أو الدول الأعضاء تخزين البيانات الشخصية؛ (ح) يتيح للمتحكم جميع المعلومات اللازمة لإثبات الامتثال للالتزامات المنصوص عليها في هذه المادة والسماح بعمليات التدقيق والمساهمة فيها، بما في ذلك عمليات التفتيش التي يجريها المتحكم أو أي مراجع أخ يفوضه المتحكم.

المطلب الثاني

التزامات المعالج

تمهيد :-

لقد اهتمت القوانين المقارنة بمعالجة مسألة حماية البيانات الشخصية في برامج المعلوماتية ، ووضعت قيوداً على الحكومات والأجهزة الإدارية للدولة والخاصة والأفراد عندما تفكر في إنشاء أنظمة معلوماتية تتضمن بيانات شخصية وهذا التخوف على الحريات بما فيها حق الإنسان في عدم الإغصاح عن البيانات الشخصية أو الرسمية له ، هو أمر يجب حمايته في مواجهة الحكومة وأجهزتها وكذلك في مواجهة النظم المعلوماتية (٣)

(١)- د/ عمرو احمد حسبو ص ٩٢ - مرجع سابق - لذلك نؤيد الرأي الفقهي القائل بضرورة التناسب بين المعلومات الشخصية المطلوب تسجيلها والهدف من ذلك التسجيل . فلا تخزن المعلومات الخاصة أو الشخصية إلا بالقدر الذي تكون فيه متبناة بالهدف من إقامة نظم المعلومات ، ولذلك يجب على الجهة الراغبة في إقامة نظم المعلومات ، أن تحدد الهدف من إقامته والمدة اللازمة للاحتفاظ بالمعلومات ، وعلى سبيل المثال ، وفيما يتعلق بالمعلومات المتصلة بالحياة الصحية ، فإنها تكون مفيدة في مجال التأمين الصحي والاجتماعي وبالتالي يجب أن تكون المعلومات المسجلة في حدود الغرض من هذا التسجيل راجعاً ذلك د/ عبد الفتاح بيومي حجازي - مكافحة جرائم الكمبيوتر في القانون العربي - دار الكتب القانية مصر - ٢٠٠٤م - ص ٦٢٠ - وأصدر المشرع الفرنسي القانون رقم ٢٧ (لسنة ٢٩٧٨ الخاص بالمعالجة الآلية للبيانات والحريات) ٤ ، إذ ذكر هذا القانون بشأن المعلوماتية والملفات والحريات ، على أن نظام الية المعلومات يجب أن يكون في خدمة كل مواطن ، وأن لا يكون من شأنه الاعتداء على الحياة الخاصة للإنسان ، كما ونص قانون العقوبات الفرنسي أيضاً على جريمة إطلاع الغير ممن له صفة في تلقي هذه البيانات ، دون إذن من صاحب الشأن ، إذا كان من شأنها المساس باعتبار صاحب الشأن أو المساس بحرمته الخاصة م (١١٦ ١ .) نهلا عبد القادر الجرائم المعلوماتية ، مرجع سابق ، ص ١٨٣ . هذا بالإضافة إلى الدور الرائد للقانون الفرنسي في التنبيه إلى أهمية الحياة الخاصة ، وحثه على ضرورة وضع تنظيم تشريعي لاستخدام الحاسبات الإلكترونية وجعلها بنوكاً للمعلومات ، وذلك بغية توفير ضمانات قانونية تحمي الحياة الخاصة وحريات الأفراد لاسيما بعد أن أتضح قصور التشريع الجنائي بنصوصه التقليدية عن حماية الحياة الخاصة وحريات الأفراد رد في مواجهة هذه الأخطار اللاهوني، حسام الدين، الحق في احتارم الحياة الخاصة، مرجع سابق، ص ٢ . فقد سن المشرع الفرنسي بعد ذلك عدة تشريعات لحل المشاكل القانونية التي نتجت عن استخدام المعالجة الإلكترونية للبيانات ومن أهم تلك التشريعات قانون سنة ٢٩٨٤ (المتعلق بالمعالجة الإلكترونية لصحيفة الحالة الجنائية، وقانون سنة ٢٩٨٤) الخاص بالإثبات في الأعمال القانونية، وقانون سنة ٢٩٨١ (المتعلق بالإلتزامات المحاسبية للتجارة والشركات الجبوري، سليم عبد الله،) ١٤٢٢ (، الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية ، لبنان ، ص ٣٧ - . وبما أن البيانات ذات الطابع الشخصي هي أحد أهم الحقوق للصيقة بالشخصية والمرتبطة بالحياة الخاصة للفرد، فإن المعالجة الآلية لهذه البيانات تتطلب أخذ الاحتياطات اللازمة، واحترام الإجراءات الخاصة الواجب إتباعها أثناء هذه العملية، ومنها احترام الغرض الذي من أجله تم السماح القانوني بمعالجة هذه البيانات ولا تتعداه إلى غيره من الأغراض، وقد جرم قانون العقوبات الفرنسي هذا الفعل وعاقب عليه - تنص المادة ٢٢٦/٢١ من قانون العقوبات الفرنسي بأنه: "يعاقب بالحبس خمس سنوات و غرامة ثلاثمائة ألف أورو كل من حاز بيانات إسمية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من أوجه المعالجة إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقاً للقانون أو للقرار الصادر في شأنها أو في الإخطار المسبق على القيام بالمعالج . عرفتها المادة السادسة من القانون التونسي المتعلق بحماية المعطيات الشخصية بانها: "العمليات المنجزة سواء بطريقة آلية أو يدوية من شخص طبيعي أو معنوي والتي تهدف خاصة إلى جمع معطيات شخصية أو تسجيلها أو حفظها أو تنظيمها أو تغييرها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو إتلافها أو الإطلاع عليها وكذلك جميع العمليات المتعلقة باستغلال قواعد البيانات أو الفهارس أو السجلات أو البطاقات أو بالربط البيني راجع إعداد: د/عبد القادر عمير -الحماية الجنائية للحق في الحياة الخاصة في البيئة الرقمية . وتجدر الإشارة في هذا الخصوص التأكيد على أن المعلومات التي والبيانات التي يحظر تخزينها ومعالجتها عن طريق الحاسب الآلي ، يجب أن تتعلق بالحياة الخاصة لصاحب الشأن ولما كانت فكرة الحياة الخاصة تنطوي على قدر من المرونة يدخل في تقديره دور إرادة الشخص ومسلكه ، فإن أمراً قد يدخل في الحياة الخاصة لشخص ولا يدخل في إطارها لشخص آخر مثل رقم التليفون ، ومتى كان الأمر يدخل في إطار الحياة الخاصة فلا يجوز تخزينه من حيث المبدأ راجع في ذلك أستاذنا الدكتور / حسام لطفى : الإطار القانوني للمعاملات الإلكترونية دار النهضة العربية القاهرة ٢٠٠٣ ، ص ١٨٢ . وقد تقتضى المصلحة العامة ضرورة تخزين البيانات متى استلزمت المصلحة العامة ذلك راجع في ذلك د/ حسام الدين كامل الاخواني : الحق في احترام الحياة الخاصة ص ٢٥٨ مرجع سابق

المعالج في مجال حماية البيانات، فتنص على جملة من الالتزامات تشبه في العديد منها الالتزامات التي وضعها المشرع الأوروبي في المادة ٢٨ من اللائحة الأوروبية لحماية البيانات GDPR. فتنص المادة ٥ من قانون حماية البيانات على أن: مع مراعاة أحكام المادة ١٢ من هذا القانون (المعنية بالبيانات الحساسة وحظر إجراء أي عملية عليها إلا بإذن مركز حماية البيانات)، يلتزم المعالج بما يأتي:

أ - إجراء المعالجة وتنفيذها طبقاً للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقاً للحالات المشروعة والقانونية وبناءً على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها، ونوع البيانات الشخصية، واتفاقها وكفايتها مع الغرض المحدد له.

ب - أن تكون أغراض المعالجة وممارستها مشروعة ولا تخالف النظام العام أو الآداب العامة. وهو شرط قانوني بديهي، يخضع له المتحكم أيضاً، وكافة أطراف عملية المعالجة، فالتصرفات عموماً لا بد من عدم مخالفتها للنظام العام والآداب.

ج - عدم تجاوز الغرض المحدد للمعالجة ومدتها، ويجب إخطار المتحكم أو الشخص المعنى بالبيانات أو كل ذي صفة، بحسب الأحوال، بالمدة اللازمة للمعالجة.

د- محو البيانات الشخصية بانقضاء مدة المعالجة أو تسليمها للمتحكم.

ه - القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانوناً.

و - عدم إجراء أية معالجة للبيانات الشخصية تتعارض مع غرض أو نشاط المتحكم فيها، إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة.

ز - حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك وما عليها من بيانات شخصية.

ح - عدم إلحاق أي ضرر بالشخص المعنى بالبيانات بشكل مباشر أو غير مباشر.

أشارت ورشة العمل إلى أن المشرع المصري اختار سلوك نهج اللائحة الأوروبية في تفصيل الالتزامات وتشديد شروط عمليات جمع ومعالجة البيانات، وهي مسائل تحتاج حقيقةً إلى إمكانات تقنية ومالية عالية للغاية، فكان يجدر عليه التعرض لمسألة تخفيف أو إعفاء بعض المتحكمين من هذه الشروط والالتزامات، بالنظر إلى أنها من الممكن أن تفوق في الكثير من الأحيان قدرات الشركات الصغيرة والمتوسطة مثلاً، الأمر الذي يحتاج إلى مراجعة وأؤكد كباحث عن أن القانون لم يُلقَ على عاتق الحائز للبيانات الشخصية أية التزامات تذكر، وأن الحائز قد يكون أحد مندوبي التسويق أو المبيعات أو الشركات التي تعمل في هذا المجال حيث يمكن تداول مثل هذه البيانات بين العاملين في هذا المجال. وفي هذا الصدد أوصى البعض، إما بوضع التزامات واضحة على كاهل الحائز أو الاستغناء عن تعريفه ضمن قائمة التعريفات التي أوردها القانون..

ط - إعداد سجل خاص بعمليات المعالجة لديه، على أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسئول حماية البيانات لديه، والمدد الزمنية للمعالجة وقيودها ونطاقها وآليات محو أو تعديل البيانات الشخصية لديه، ووصفًا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة.

ى - توفير الإمكانات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز من التفتيش والرقابة للتأكد من التزامه بذلك

ك - الحصول على ترخيص أو تصريح من المركز للتعامل على البيانات الشخصية.

ل - يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية. ومن ثم يتعين على اللائحة التنفيذية تحديد قواعد وضوابط تعيين ممثل المعالج الذي يقع خارج مصر، حتى يتم التعامل معه من قبل المركز أو الشخص المعنى بالبيانات لأغراض ضمان الامتثال لهذا القانون.

- طبيعة العلاقة بين المعالج والمتحكم: وفقاً للمادة ٢٨ / ١ من اللائحة الأوروبية، عند إجراء المعالجة نيابة عن المتحكم، يجب على الأخير اختيار المعالج الذي يوفر ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تجعل المعالجة تلبى متطلبات هذه اللائحة وتضمن حماية حقوق صاحب البيانات. ويمكن أن تتمثل هذه المعايير في المعرفة المتخصصة لدى المعالج (على سبيل المثال، الخبرة الفنية فيما يتعلق بالتدابير الأمنية وخرق البيانات)؛ موثوقية المعالج؛ موارد المعالج والتزام المعالج بقواعد السلوك المعتمدة أو آلية الاعتماد. كما تفرض الفقرة الثانية من هذه المادة على المعالج التزاماً بعدم الاستعانة بمعالج آخر دون إذن كتابي مسبق ومحدد من المتحكم، وفي حالة الحصول على إذن كتابي عام، يجب على المعالج إبلاغ المتحكم بأي تغييرات مقصودة تتعلق بإضافة أو استبدال معالين آخرين، مما يمنح المتحكم الفرصة للاعتراض على هذه التغييرات. كما تتطلب الفقرة الثالثة من هذه المادة إبرام عقد للمعالجة بين المتحكم والمعالج أو أي تصرف قانوني آخر بموجب قانون الاتحاد أو الدول الأعضاء أيضاً يتطلب قانون خصوصية المستهلك في كاليفورنيا أن يتم الكشف عن البيانات الشخصية للمعالج بموجب عقد مكتوب، ولكن يضع القانون المصري واللائحة الأوروبية التزامات مباشرة وتفصيلية على المعالج لا يرتبها القانون في كاليفورنيا على "مقدم الخدمة" بل على "الشركة" فقط. يحدد موضوع المعالجة ومدتها، وطبيعة وغرض المعالجة، ونوع البيانات الشخصية وفئات أصحاب البيانات والتزامات وحقوق المتحكم وفقاً للمادة ٢٨ فقرة ثالثة من اللائحة الأوروبية، يجب أن ينص هذا العقد أو أي تصرف قانوني آخر، على وجه الخصوص، على أن المعالج: أ- يتولى معالجة البيانات الشخصية فقط بناءً على تعليمات موثقة من المتحكم، بما في ذلك ما يتعلق بنقل البيانات الشخصية إلى دولة ثالثة أو منظمة دولية، ما لم يكن ذلك مطلوباً بموجب قانون الاتحاد أو الدول الأعضاء الذي يخضع له المعالج؛ وفي هذه الحالة، يجب على المعالج إبلاغ المتحكم بهذا الشرط القانوني قبل المعالجة، ما لم يحظر هذا القانون هذه المعلومات لأسباب مهمة تتعلق بالمصلحة العامة؛ ب) التأكد أن الأشخاص المرخص لهم بمعالجة البيانات الشخصية قد التزموا بالسرية أو خضوعهم للالتزام قانوني ملائم للسرية؛ ج- يتخذ جميع التدابير المطلوبة عملاً بالمادة ٣٢ من اللائحة (الخاصة بأمن المعالجة)؛ د- يحترم الشروط المشار إليها في الفقرتين ٢ و ٤ لإشراك معالج فرعي؛ هـ) مراعاة طبيعة المعالجة، ومساعدة المتحكم على اتخاذ التدابير الفنية والتنظيمية المناسبة، بقدر ما يكون ذلك ممكناً، للوفاء بالتزام المتحكم بالرد على طلبات ممارسة حقوق صاحب البيانات المنصوص عليها في الفصل الثالث؛ و) يساعد المتحكم في ضمان الامتثال للالتزامات بموجب المواد من ٣٢ إلى ٣٦ مع مراعاة طبيعة المعالجة والمعلومات المتاحة للمعالج؛ ز) عند اختيار المتحكم، يحذف أو يعيد جميع البيانات الشخصية إلى المتحكم بعد انتهاء تقديم الخدمات المتعلقة بالمعالجة، ويحذف النسخ الموجودة ما لم يشترط قانون الاتحاد أو الدول الأعضاء تخزين البيانات الشخصية؛ ح) يتيح للمتحكم جميع المعلومات اللازمة لإثبات الامتثال للالتزامات المنصوص عليها في هذه المادة والسماح بعمليات التدقيق والمساهمة فيها، بما في ذلك عمليات التفتيش التي يجريها المتحكم أو أي مراجع آخر يفوضه المتحكم ويجب أن يكون هذا العقد أو التصرف القانوني في صورة مكتوبة، بما في ذلك الكتابة في الشكل الإلكتروني (م ٢٨ فقرة ٩ من اللائحة). ومع ذلك، يجب ألا يكتفي عقد المعالجة بإعادة صياغة أحكام اللائحة الأوروبية لحماية البيانات؛ فيجب أن يتضمن معلومات أكثر تحديداً وملموسة حول كيفية تلبية المتطلبات ومستوى الأمان المطلوب لمعالجة البيانات الشخصية موضوع عقد المعالجة

وتشير الفقرة قبل الأخيرة من المادة ٤ من قانون حماية البيانات إلى أنه في حال وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعنى ممارسة حقوقه تجاه كل متحكم على حدة". وفي هذا الشأن يحيل القانون إلى اللائحة التنفيذية في شأن تحديد السياسات والإجراءات والضوابط والمعايير الفنية للالتزامات المعالج (المشار إليها في المادة ٥ من القانون .

وفي حالة قيام المعالج بإشراك معالج فرعي للقيام بأنشطة معالجة محددة نيابة عن المتحكم، يتم فرض نفس الالتزامات الخاصة بحماية البيانات المنصوص عليها في العقد أو أي تصرف قانوني آخر بين المتحكم والمعالج (على النحو المشار إليه في الفقرة ٣ من هذه المادة) على المعالج الفرعي بناء على عقد أو أي تصرف قانوني آخر بموجب قانون الاتحاد أو الدول الأعضاء، وبخاصة توفير ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تجعل المعالجة تلبى متطلبات هذه اللائحة. وفي حالة إخال المعالج الفرعي بالوفاء بالالتزامات حماية البيانات الخاصة به، يجب أن يظل المعالج الأصلي مسؤولاً بصورة كاملة تجاه المتحكم عن أداء التزامات المعالج الفرعي (م ٢٨ فقرة ٤ من اللائحة). وجدير بالذكر أن القانون المصري لم ينظم مسائل وأحكام المعالج الفرعي أو ما يطلق عليه المعالج من الباطن. وتتناول المادة ٢٨ فقرة ١٠ من اللائحة حالة مخالفة المعالج لأحكام هذه اللائحة وقيامه بتحديد أغراض ووسائل المعالجة، ففي هذه الحالة يجب اعتبار المعالج بمثابة متحكم فيما يتعلق بهذه المعالجة، وذلك مع عدم الإخلال بالمواد ٨٢ و ٨٣ و ٨٤ من هذه اللائحة. ومن جهة أخرى تتناول المادة ٢٩ من اللائحة الأوروبية حالة المعالجة تحت سلطة المتحكم والمعالج، فأشارت إلى أنه لا يجوز للمعالج وأي شخص يتصرف تحت سلطة المتحكم أو المعالج، وله حق الوصول إلى البيانات الشخصية، أن يقوم بمعالجة تلك البيانات إلا بناء على تعليمات من المتحكم، ما لم يكن مطلوباً بموجب قانون الاتحاد أو الدولة العضو أو رأى كباحث يجب أن تكون علاقة المتحكم بالمعالج في القانون المصري بناء على تعليمات تعاقدية واضحة، وأكدت على ضرورة أن تكون في صورة تعاقدية، على أن يفرض ذلك أيضاً على كل متحكم أو معالج من الباطن. ويجب أن تخضع أنشطة معالجة البيانات لعقد أو أي تصرف قانوني آخر مع المتحكم، على أن يحدد العقد موضوع ومدة وغرض المعالجة، وأنواع معالجة البيانات الشخصية والإجراءات الأمنية والتزامات وحقوق المعالج والمتحكم. وعند إنهاء العقد مع المتحكم، يجب على المعالج إعادة البيانات الشخصية أو حذفها، بالإضافة إلى ذلك، إذا أراد المعالج إشراك معالج آخر (معالج فرعي) وجب عليه الحصول على إذن كتابي من المتحكم وأرى كباحث أيضاً بأن المبالغة في فرض الالتزامات على جميع القائمين على معالجة البيانات قد يكون غير مناسب حالياً للمجتمع المصري. كما يجب من جهة أخرى تحديد طبيعة علاقة الشخص المعنى بالبيانات مع الحائز أو المعالج أو المتحكم. وفي قانون البيانات الشخصية الإماراتي رقم ٢٦ لسنة

ولذلك حماية البيانات الشخصية"، وهو الشخص الطبيعي الذي يعني بمباشرة مهام حماية البيانات الشخصية داخل المؤسسة أو الجهة. وقد تناول الفصل الرابع من القانون تنظيم تعيين مسئول حماية البيانات في المادة (٨) وبيان التزاماته في المادة (٩) منه. وعلى التسق نفسه، تعرضت اللائحة الأوروبية لمسئول حماية البيانات Data protection officer في المبحث الرابع من الفصل الرابع منها، بشئ من التفصيل، فأشارت لمسألة تعيينه Designation of the data protection officer في المادة ٣٧ ، ووضعه أو مركزه Position of the data protection officer في المادة ٣٨ ، ومهامه Tasks of the data protection officer في المادة ٣٩ من اللائحة. وباستقراء تلك المواد والمواد المتعلقة بالعقوبات يتضح لنا بسهولة أن مسئول حماية البيانات هو الجهة المسؤولة داخل كل مؤسسة عن تطبيق أحكام القانون، ويحمل بمعظم المسؤوليات في هذا الصدد، وهو ما لم يتوانى القانون عن ذكره.

- وتجدر الإشارة إلى أن تعريف المعالجة: عرف المشرع المصري 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". وفي شأن هذا التعريف، ربما كان من الأفضل لو ابتعد المشرع المصري عن إيراد لفظ "إلكترونية" واكتفى بالإشارة إلى أن المعالجة هي تلك العمليات "التقنية" وذلك لضبط دقة الصياغة كان قسم التشريع بمجلس الدولة قد أقر ذلك حين عُرض عليه مشروع القانون، غير أن قطاع التشريع بوزارة العدل رفض هذا الاقتراح معللاً ذلك بأن تعريف المعالجة يتضمنه مصطلح إلكترونية يعد تعريفاً متطابقاً مع تعريف المعالجة الإلكترونية الوارد بالقانون رقم (١٧٥) لعام ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الذي عرفها على أنها: "أي عملية إلكترونية أو تقنية تتم كلياً أو جزئياً لكتابة أو تجميع، أو تسجيل، أو حفظ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبال، أو تداول، أو نشر، أو محو، أو تغيير، أو تعديل، أو استرجاع، أو استنباط للبيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو مستحدثت من تقنيات أو وسائط أخرى". كما أضاف القطاع في رده أن توحيد التعريفات الفنية هو أساس لصياغة التشريعات. راجع: كتاب السيد المستشار/نائب رئيس مجلس الدولة ورئيس قسم التشريع رقم (٢٤) بتاريخ ١٦ يناير ٢٠٢٠ المشار إليه، ص ١٠٩ و ص ١٢٥ .

المطلب الثالث

حقوق صاحب البيانات المعالجة

تمهيد : مما لا شك فيه أن الشخص الذى تتم معالجة بياناته الشخصية هو المقصود بالحماية من قبل قانون حماية البيانات الشخصية ، حيث يهدف القانون إلى حماية الشخص من الاعتداء على بياناته الشخصية وقد أعطى المشرع الفرنسى والمصرى حقوق للخص على بياناته لمن يتم معالجة بياناته (١) وهى

١- العلم بالبيانات الشخصية الخاصة به الموجودة لدى أى حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها . ٢- العدول عن الموافقة المسبقة لى الاحتفاظ ببياناته الشخصية أو معالجتها ، ٣- التصحيح أو التعديل أو المحو أو الاضافة أو التحديث للبيانات الشخصية ، ٤- تخصيص المعالجة فى نطاق محدد ، ٥- العلم والمعرفة بأى خرق أو انتهاك لبياناته الشخصية ، ٦- الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الاساسية للشخص المعنى بالبيانات وبستثناء البند (٥) من الفقرة السابقة يودى الشخص المعنى بالبيانات مقابل تكلفة الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه ، ويتولى المركز إصدار قرارات تحديد هذا المقابل بما لايجاوز عشرين الف جنيه

(١)-د أمنية مصطفى صادق شبكات المعلومات الإلكترونية المفتوحة وأثارها على العمل مع تصور وطنى لأبعاد دورها فى خدمات المعلومات فى مصر ، عالم الكتب ، مج ١٨ ع ٢٤ مارس - ابريل ١٩٩٧ . تكمن نقطة الانطاق الأساسية فى بيان حقوق والتزامات هذا الشخص فى تعريفه على نحو يحدد ماهيته، ولهذا فقد عرفه القانون فى المادة الأولى منه بأنه: "أى شخص طبيعى تُنسب إليه بيانات شخصية معالجة إلكترونياً تدل عليه قانوناً أو فعاً، وتُمكن من تمييزه عن غيره". كما عرفت المادة ٤ من اللائحة الأوروبية "صاحب البيانات Data subject " بأنه "الشخص الطبيعى الذى يمكن التعرف عليه أو يمكن تحديده بشكل مباشر أو غير مباشر، وخاصة بالرجوع إلى رقم الهوية أو إلى عامل أو أكثر من العوامل المحددة لهويته البدنية أو الفسيولوجية أو العقلية أو الاقتصادية أو الاجتماعية" ويستفاد من هذه المادة، وعلى غرار نطاق تطبيق القانون، فقد حصر المشرع المصرى الشخص المعنى بالبيانات فى نطاق الشخص الطبيعى، منتهجاً طريق المشرع الأوروبى، ومن ثم يقتصر نطاق الحماية على الشخص الطبيعى فقط دون الشخص الاعتبارى. ويبدو من هذه التعريفات أن الشخص المعنى بالبيانات هو كل شخص طبيعى تكون بياناته الشخصية محاً للجمع والمعالجة بناء على رضاء سليم غير مشوب بأى عيب من عيوب الإرادة. كما يُعرفه المشرع الفرنسى فى قانون المعلوماتية والحريات المعدلاً بأنه "كل شخص طبيعى تكون بياناته الشخصية موضوعاً للمعالجة ٢ من القانون . وقد رسَّخ القانون حقوق الشخص المعنى بالبيانات فى المادة الثانية من القانون، التى يجرى نصها على ما يلى: "ويكون للشخص المعنى بالبيانات الحقوق الآتية:

١- العلم بالبيانات الشخصية الخاصة به الموجودة لدى أى حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها. ٢ العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها. ٣- التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية. ٤- تخصيص المعالجة فى نطاق محدد. ٥- العلم والمعرفة بأى خرق أو انتهاك لبياناته الشخصية. ٦- الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات. وباستثناء البند (٥) من الفقرة السابقة، يودى الشخص المعنى بالبيانات مقابل تكلفة الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه، ويتولى المركز إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه". ويتبين من هذه المادة أن المشرع عدّد حقوق الشخص المعنى بالبيانات، مما يثير التساؤل حول إيرادها على سبيل الحصر أو أنها جاءت على سبيل المثال، مما يتيح المجال أمام وجود حقوق أخرى للشخص. ولاشك أن ما ورد من حقوق فى القانون لا يخل بما للشخص من حقوق أخرى، وردت فى نصوص أخرى فى قانون حماية البيانات أو فى قوانين أخرى، مثل قانون حماية تقنية المعلومات أو قانون الأحوال المدنية وقد أوردت اللائحة الأوروبية GDPR حقوق صاحب البيانات Rights of the data subject فى الفصل الثالث منه المواد من ١٢ - ٢٣ وحقيقة يجب التسليم بأن الاعتراف للشخص المعنى بالبيانات ببعض الحقوق على بياناته هو غاية أساسية يسعى لها القانون، هادفاً توفير حماية قانونية فعالة له باعتباره المقصود أساساً من هذه الحماية.

١- العلم بالبيانات الشخصية الخاصة به الموجودة لدى أى حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها : منح المشرع المصري صاحب البيانات حقوق العلم بالبيانات الخاصة به لدى أى "حائز أو متحكم أو معالج" والاطلاع عليها والوصول إليها أو الحصول عليها، وقد أطلقت اللائحة الأوروبية عليه تسمية الحق فى الوصول للبيانات Right of access ، حيث نصت فى المادة ١٥ منها على أن يكون لصاحب البيانات الحصول على تأكيد من المتحكم حول ما إذا كانت البيانات الشخصية المتعلقة به قيد المعالجة أم لا، وفى حال حدوث ذلك، يحق له الوصول إلى البيانات الشخصية والمعلومات التالية: أغراض المعالجة - فئات البيانات الشخصية المعنية - المستفيدون أو فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم أو سيتم الكشف عنهم، وبخاصة المستفيدين فى بلدان أخرى أو منظمات دولية - الفترة التى سيتم خلالها تخزين البيانات الشخصية، أو إذا لم يكن ذلك ممكناً، المعايير المستخدمة لتحديد تلك الفترة - وجود الحق فى طلب تصحيح أو مسح البيانات الشخصية لدى المتحكم أو تقييد معالجة البيانات الشخصية المتعلقة بصاحب البيانات أو الاعتراض على هذه المعالجة

٢- حق العدول عن الموافقة على الاحتفاظ بالبيانات أو معالجتها: يشترط القانون، فى مادته الثانية، ضرورة صدور موافقة صريحة من الشخص المعنى بالبيانات على عمليات جمع البيانات أو معالجتها، إلا فى الأحوال المصرح بها قانوناً، ومن ثم فمن الطبيعي أن يكون للشخص العدول عن هذه الموافقة، أى سحب موافقته فى أى وقت، لتعلقها بحقوقه للصيقة بشخصيته، فقد تطرأ أمور خاصة لدى الشخص تستدعي عدم الاحتفاظ بالبيانات أو معالجتها. يشترط القانون، فى مادته الثانية، ضرورة صدور موافقة صريحة من الشخص المعنى بالبيانات على عمليات جمع البيانات أو معالجتها، إلا فى الأحوال المصرح بها قانوناً، ومن ثم فمن الطبيعي أن يكون للشخص العدول عن هذه الموافقة، أى سحب موافقته فى أى وقت، لتعلقها بحقوقه للصيقة بشخصيته، فقد تطرأ أمور خاصة لدى الشخص تستدعي عدم الاحتفاظ بالبيانات أو معالجتها. وارى كباحث أن تتضمن اللائحة التنفيذية شروط ومحددات ممارسة حق الشخص فى العدول عن الموافقة

وفى الواقع ينطوي نص الفقرة الأولى من المادة الثالثة من القانون المصري على عدة صور لحقوق الشخص المعنى بالبيانات، هى: أ- يكون للشخص الذى تم جمع ومعالجة بياناته الحق فى العلم ببياناته الموجودة لدى أى حائز أو متحكم أو معالج، ومن المسلم به أن العلم لغةً هو مصدر من الفعل عَلمَ، وهو إدراك الشيء على حقيقته، أى إدراكه على ما هو عليه إدراكاً جازماً، كما أنه المعرفة واليقين، وهو نقيض الجهل. بيد أن القانون لم يحدد صورة وآلية تحقق هذا العلم وعناصره، الذى يلبي هذا الاشتراط القانوني، فهل يكفى فيه مجرد الاطلاع أم يلزم الإخطار الكتابي؟ وتوحي صياغة النص "العلم بالبيانات.. الموجودة لدى المتحكم.." أن هذا الحق قاصر على مجرد تعرف الشخص على ما يوجد لدى المتحكم وغيره من بيانات شخصية خاصة به، دون غيرها من صور العلم، كأغراض المعالجة والجهات التى حصلت على البيانات وتحديد الفترة الزمنية التى سيتم خلالها تخزين البيانات الشخصية. ب- حق الشخص المعنى بالبيانات فى الاطلاع على بياناته والوصول إليها: ويقضى هذا الحق تمكين هذا الشخص أو ورثته أو من ينوب عنه قانوناً من الاطلاع على جميع بياناته موضوع المعالجة، ولا يجوز التنازل عن هذا الحق أو الحد منه إلا فى حدود القانون. وقد يثور التساؤل حو دقة الصياغة اللفظية فى هذا الصدد، حيث يشير النص لحق الاطلاع على البيانات وأيضاً حق الوصول للبيانات، رغم أن الأول يفيد الثانى فالاطلاع يأتى بطبيعة الحال لاحقاً للوصول للبيانات، فضلاً عن أن حق العلم بالبيانات، لفظ شامل، يتضمن بين طياته الاطلاع والوصول، إذ كيف يتسنى للشخص العلم بالشيء إلا من طريق الوصول إليه والاطلاع عليه. ويرتبط حق الوصول والاطلاع على البيانات بالحق فى الحصول عليها، كما عبر عن ذلك النص، ويقصد من ذلك حق الشخص فى الحصول على نسخة من بياناته بلغة واضحة ومطابقة لما هو موجود لدى المتحكم وغيره، بناء على طلبه، وفقاً للإجراءات المقررة، ودفع المقابل المالى لهذه الخدمة وكان يجب على المشرع المصضرى أن بأن تتضمن اللائحة التنفيذية ضوابط ممارسة هذا الحق، على غرار ما فعل المشرع الأوروبي

٣- الحق في تصحيح أو تعديل أو محو البيانات الشخصية: يتضمن هذا الحق صور متعددة، فيشمل التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية. وجدير بالملاحظة أن صياغة هذه الكلمات تنطوي على تكرار لا داعي له، فالتصحيح أو الإضافة أو التحديث هي مسائل في حد ذاته تندرج تحت وصف التعديل، فهناك تعديل بالإضافة أو الحذف أو التصحيح أو التحديث. أ- الحق في التصحيح: يكون للشخص المعنى بالبيانات، أو كل ذي صفة، الحق في طلب تصحيحها إذا ما شاب البيانات أخطاء أثناء جمعها ومعالجتها. كما يكون له التعديل على هذه البيانات سواء بالإضافة أو التحديث إلى هذه البيانات إذا كان يشوبها نقص أو تغييرها متى كانت غير دقيقة أو غير صحيحة أو مضللة أو غامضة. وقد نصت المادة ١٦ من اللائحة الأوروبية على الحق في التصحيح Right to rectification ، بقولها أنه يكون لصاحب البيانات الحق في الحصول من المتحكم دون تأخير غير مبرر على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به، ومع مراعاة أغراض المعالجة، يجب أن يكون له الحق في استكمال البيانات الشخصية الناقصة، بوسائل منها تقديم بيان إضافي. ب - الحق في المحو (الحق في النسيان): Right to be forgotten تتسم شبكة الانترنت، وما يرتبط بها من خوادم ضخمة تخضع لسيطرة شركات عملاقة، بشراستها لجمع وتخزين المعلومات، وذاكرتها المطلقة التي لا يمكن محو ما يختزن فيها بسهولة من قبل المستخدمين، وهو أمر جعل النسيان الطبيعي

أمراً صعب المنال في الوقت الحاضر، فهي تُحصى على مستخدميها أنشطتهم سواء كانت في شكل تعليقات أو أخبار خاصة أو صور أو معلومات شخصية، وتجمع وتسجل بياناتهم ومعلوماتهم وتخزينها وتحفظ بها لمدة غير محدودة، مع إتاحة هذه البيانات والمعلومات من أي مكان في العالم ولكل من يريد وفي الوقت الذي يحلو له، مع العلم أن هذه البيانات والمعلومات قد تكون قديمة أو مغلوبة أو غير صحيحة، ومع هذا تظل متاحة للجميع وعلى الدوام إلى ما لا نهاية. ومن شأن هذه المخاطر أن تسبب للشخص المعنى بالبيانات أضراراً بالغة الخطورة وتشكل تهديداً صريحاً للخصوصية، وحقهم في محو البيانات الخاصة بهم مع على الانترنت، وهو ما دعا الفكر القانوني إلى البحث عن حلول لهذه المشكلة لحماية خصوصية الأشخاص، ووجد ضالته في مفهوم "الحق في النسيان" في البيئة الرقمية، باعتباره أحد الحقوق المرتبطة بحرمة الحياة الخاصة للإنسان. ولهذا نص المشرع المصري (م ٢ من القانون) على حق الشخص المعنى بالبيانات في محو بياناته الشخصية، ويُطلق على الحق في المحو تسمية "الحق في النسيان" أو الحق في الدخول في طي النسيان، أو الحق في النسيان الرقمي

ويقصد بهذا الحق أن لكل شخص الحق في حذف البيانات الشخصية المحفوظة لدى المعالج أو المتحكم أو الحائز نهائياً عند إلغاء أو مغادرة الخدمة أو التطبيق، وعدم الاحتفاظ بنسخ منها لأي سبب كان، بما يتضمنه ذلك من إزالة الروابط التي تؤدي إلى معلومات عنه على الانترنت (محركات البحث، مواقع إلكترونية، مواقع التواصل الاجتماعي...)، كما يعنى أيضاً التزام المسئولون عن معالجة البيانات الشخصية أو حفظها بعدم حفظ تلك البيانات لمدة تتجاوز الغاية التي جمعت من أجلها. اللجنة الوطنية للمعلوماتية في فرنسا، الحق في النسيان الرقمي، بأنه الحق الذي يخول صاحبه مكنة السيطرة من حيث الزمان على بياناته الشخصية، بغية الحصول على حذفها أو محوها عندما يرغب في ذلك". Maxime BESÈME :Le droit à l'oubli numérique dans le droit de Consécration prétorienne et législative ,Mémoire UCL(Université catholique de l'Union européenne

/Louvain ,)2015-2016 .Disponible sur Internet :<https://dial.uclouvain.be/memoire/ucl>

en/object/thesis:7609/datastream/PDF_01/view

أوصى المشرع الأوروبي بضرورة وضع ضمانات لحماية هذا الحق، وقد استجاب المشرع لذلك حيث اعترف صراحة بهذا الحق في المادة ١٧ من اللائحة الأوروبية لحماية البيانات، حيث تنص في الفقرة الأولى على أن يكون لصاحب البيانات الحق في أن يحصل من المتحكم على محو البيانات الشخصية المتعلقة به دون تأخير لا مبرر له، ويجب على المتحكم أن يحذف البيانات الشخصية دون تأخير. وبناءً على ذلك تمكن المستخدم الأوروبي من مطالبة شركات الانترنت بحقه في محو بياناته الشخصية واحترام حقه في الدخول في طي النسيان الرقمي (١)

(١)- يُشار في هذا الصدد، إلى قيام شركة Google بتضمين سياستها لتقرير الشفافية إعاد المستخدمين لمحركها بتأثير قانون الخصوصية الأوروبي في نتائج بحث Google ، وبيان "طلبات حذف المحتوى بموجب قانون الخصوصية الأوروبي"، وطلبات إزالة عناوين URL من بحث Google للحفاظ على الخصوصية، وذلك على موقعها التالي:

أسباب تطبيق الحق في النسيان: <https://transparencyreport.google.com/eu-privacy/overview?hl=ar&hl=es>

لم يحدد المشرع المصري الحالات التي ينطبق فيها الحق في المحو Right to erasure أو ما يطلق عليه الحق في النسيان Right to be forgotten ، وهو ما تحوط له المشرع الأوروبي في اللائحة الأوروبية، حيث تضمنت المادة ١٧ منه أحكام واضحة لتنظيم هذا الحق، واشترطت لتطبيق الحق في النسيان ضرورة توافر أحد الأسباب التالية: - لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها من أجلها؛ - قيام صاحب البيانات بسحب الموافقة التي تستند إليها المعالجة وفقاً للفقرة الأولى من المادة ٦، أو الفقرة الأولى من المادة ٩، وحيث لا يوجد أساس قانوني آخر للمعالجة؛ - اعتراض صاحب البيانات على المعالجة وفقاً للمادة ٢١ / ١ ولا توجد أسباب مشروعة تبرر المعالجة، أو اعتراضه على المعالجة وفقاً للمادة ٢١ / ٢؛ - إذا جرى معالجة البيانات الشخصية بشكل غير قانوني - يجب محو البيانات الشخصية للوفاء بالتزام قانوني في قانون الاتحاد الأوروبي أو الدول الأعضاء يخضع له المتحكم - تم جمع البيانات الشخصية بخصوص عرض خدمات مجتمع المعلومات المشار إليها في المادة ٨ / ١. وفي حالة قيام المتحكم بإتاحة البيانات الشخصية للجمهور، وكان ملزماً بمحو البيانات الشخصية، يجب عليه، مع مراعاة التكنولوجيا المتاحة وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير التقنية، لإبلاغ المتحكمين في معالجة البيانات الشخصية بأن صاحب البيانات قد طلب محو أي روابط لديهم أو نسخ لهذه البيانات الشخصية (المادة ١٧ فقرة ثانية من اللائحة الأوروبية). لذلك أوصى كباحث وأرى بتعديل القانون للنص على تحديد مدة معينة يتعين تصحيح البيانات خلالها أو حذفها على غرار ما فعلت بعض التشريعات ولكن قد خلت اللائحة التنفيذية للقانون ١٥١ لسنة ٢٠٢٠م حماية البيانات الشخصية المصري من النص على ذلك وهذا قصور تشريعي. الحق في تخصيص المعالجة في نطاق محدد (تقييد المعالجة): يجيز القانون للشخص المعنى بالبيانات تحديد نطاق المعالجة (أي تقييدها) م٢، وقد نصت اللائحة الأوروبية على هذا الحق في المادة ١٨ منها. ولكن المشرع المصري لم يحدد ضوابط وشروط هذا التقييد، وهو ما راعته اللائحة الأوروبية، ونفذته فعلياً الشركات والكيانات التي تخضع لنطاق تطبيقها، حيث يجوز للشخص طلب تقييد معالجة بياناته الشخصية وفقاً للشروط التالية: - إذا اعترض على دقة معلوماته الشخصية لفترة من الزمن تمكن الشخص المسئول من التحقق من دقة المعلومات الشخصية؛ - إذا كانت المعالجة غير قانونية ورفض الشخص المعنى حذف البيانات الشخصية وطلب بدلاً من ذلك تقييد استخدام البيانات الشخصية؛ - إذا كان الشخص المسئول لم يعد بحاجة إلى بيانات شخصية لأغراض المعالجة، ولكن يحتاج الشخص المعنى بالبيانات إليها لتأكيد أو إقامة دعاوى قانونية، أو الدفاع فيها. - إذا اعترض الشخص على المعالجة وفقاً للمادة ٢١ الفقرة ١ من اللائحة الأوروبية، ولم يتم بعد تحديد ما إذا كانت الأسباب المشروعة للشخص المسئول تفوق أسباب الشخص المعنى بالبيانات. في حالة تقييد معالجة البيانات الشخصية المتعلقة بالشخص المعنى بالبيانات، لا يجوز استخدام هذه البيانات إلا بموافقة (باستثناء تخزين البيانات) لغرض تأكيد أو إقامة دعاوى قانونية، أو الدفاع فيها أو حماية حقوق شخص طبيعي أو اعتباري آخر أو لأسباب المصلحة العامة الهامة للاتحاد الأوروبي أو الدولة العضو. إذا تم تقييد المعالجة وفقاً للشروط المذكورة أعلاه، فسيقوم الشخص المسئول بإبلاغ الشخص المعنى قبل رفع هذا التقييد.

٤- الحق في تخصيص المعالجة في نطاق محدد (تقييد المعالجة): يجيز القانون للشخص المعنى بالبيانات تحديد نطاق المعالجة أي تقييدها م ٢(،) وقد نصت اللائحة الأوروبية على هذا الحق في المدة ١٨ منها. ولكن المشرع المصري لم يحدد ضوابط وشروط هذا التقييد، وهو ما راعته اللائحة الأوروبية، ونفذته فعلياً الشركات والكيانات التي تخضع لنطاق تطبيقها، حيث يجوز للشخص طلب تقييد معالجة بياناته الشخصية وفقاً للشروط التالية:

- إذا اعترض على دقة معلوماته الشخصية لفترة من الزمن تمكن الشخص المسئول من التحقق من دقة المعلومات الشخصية؛

- إذا كانت المعالجة غير قانونية ورفض الشخص المعنى حذف البيانات الشخصية وطلب بدلاً من ذلك تقييد استخدام البيانات الشخصية؛

- إذا كان الشخص المسئول لم يعد بحاجة إلى بيانات شخصية لأغراض المعالجة، ولكن يحتاج الشخص المعنى بالبيانات إليها لتأكيد أو إقامة دعاوى قانونية، أو الدفاع فيها.

- إذا اعترض الشخص على المعالجة وفقاً للمادة ٢١ الفقرة ١ من اللائحة الأوروبية، ولم يتم بعد تحديد ما إذا كانت الأسباب المشروعة للشخص المسئول تفوق أسباب الشخص المعنى بالبيانات. في حالة تقييد معالجة البيانات الشخصية المتعلقة بالشخص المعنى بالبيانات، لا يجوز استخدام هذه البيانات إلا بموافقتهم- الحق في تخصيص المعالجة في نطاق محدد (تقييد المعالجة): يجيز القانون للشخص المعنى بالبيانات تحديد نطاق المعالجة أي تقييدها م ٢(،) وقد نصت اللائحة الأوروبية على هذا الحق في المدة ١٨ منها. ولكن المشرع المصري لم يحدد ضوابط وشروط هذا التقييد، وهو ما راعته اللائحة الأوروبية، ونفذته فعلياً الشركات والكيانات التي تخضع لنطاق تطبيقها .

حيث يجوز للشخص طلب تقييد معالجة بياناته الشخصية وفقاً للشروط التالية:- إذا اعترض على دقة معلوماته الشخصية لفترة من الزمن تمكن الشخص المسئول من التحقق من دقة المعلومات الشخصية؛- إذا كانت المعالجة غير قانونية ورفض الشخص المعنى بالبيانات الشخصية وطلب بدلاً من ذلك تقييد استخدام البيانات الشخصية؛- إذا كان الشخص المسئول لم يعد بحاجة إلى بيانات شخصية لأغراض المعالجة، ولكن يحتاج الشخص المعنى بالبيانات إليها لتأكيد أو إقامة دعاوى قانونية، أو الدفاع فيها.- إذا اعترض الشخص على المعالجة وفقاً للمادة ٢١ الفقرة ١ من اللائحة الأوروبية، ولم يتم بعد تحديد ما إذا كانت الأسباب المشروعة للشخص المسئول تفوق أسباب الشخص المعنى بالبيانات. في حالة تقييد معالجة البيانات الشخصية المتعلقة بالشخص المعنى بالبيانات، لا يجوز استخدام هذه البيانات إلا بموافقتهم(باستثناء تخزين البيانات) لغرض تأكيد أو إقامة دعاوى قانونية، أو الدفاع فيها أو حماية حقوق شخص طبيعي أو اعتباري آخر أو لأسباب المصلحة العامة الهامة للاتحاد الأوروبي أو الدولة العضو. إذا تم تقييد المعالجة وفقاً للشروط المذكورة أعلاه، فسيقوم الشخص المسئول بإبلاغ الشخص المعنى قبل رفع هذا التقييد. لذلك أرى كباحث بأهمية أن تولى اللائحة التنفيذية في اعتبارها ضوابط ممارسة الحق في تقييد المعالجة، على غرار اللائحة الأوروبية. وهذا قصور من المشرع المصري فكان يجب ان تتضمن اللائحة التنفيذية للقانون مثل هذه الضوابط . وتجدر الإشارة إلى مجالات تطبيق الحق في النسيان: ينحصر مجال تطبيق الحق في النسيان في البيئة الرقمية فيما يتعلق بالآثار الإلكترونية أو الذكريات الرقمية، وهي كل البيانات والمعلومات المتعلقة بالشخص ونشاطه خال استخدامه لنشاط معلوماتي أو وسيلة إلكترونية أيأ كان نوعها (مواقع شبكات التواصل الاجتماعي - محركات بحث - مدونات - مواقع التجارة الإلكترونية.. وغيرها) يكون من شأنها أن تساهم في تحديد هويته الرقمية، كما يعتبر من الآثار الرقمية آراء الشخص ومساهماته على الإنترنت مهما كان نوعها. وحديثاً، قضت محكمة العدل الأوروبية، بتاريخ ٢٤ سبتمبر ٢٠١٩ ، بأنه إذا كان يتوجب على شركة " Google " سحب روابط بطلب من هيئة تنظيمية أو محكمة في دولة بالاتحاد الأوروبي من نسخ مواقعها الأوروبية، إلا أن "الحق في النسيان" عبر الإنترنت يتوقف عند هذا الحد، ومن ثم فهي غير مطابقة لتطبيق هذا الحق على محركات البحث التابعة لها خارج أوروبا وأرى كباحث ان يحدد القانون مدة تصحيح البيانات او حذفها كما فعلت بعض التشريعات حدد القانون المغربي بشأن حماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي، في المادة ٨ / ١ منه هذه المدة عشرة أيام

٤- الحق في معرفة أي خرق أو انتهاك للبيانات الشخصية: تشير المادة الثانية من القانون إلى حق الشخص في العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية. وهذا الحق يعد من البديهيات، فمن الطبيعي إلزام المتحكم أو المعالج بإخطار الشخص المعنى بما قد يطرأ على هذه البيانات، وما يحدث لها من اعتداءات، بأي شكل أو وسيلة كانت. ويفيد التعرف على الاعتداء على البيانات في تدبير الشخص المعنى بالبيانات لأمواره واتخاذ قراره الذي يحقق مصلحته، فقد يسحب موافقته أو يطلب تعديل أو تصحيح البيانات متى حدث لها أي تشويه أو يطلب حذف البيانات كلية

التزام المتحكم والمعالج بإخطار المركز بأي خرق أو انتهاك للبيانات: وفقاً للمادة ٧ من القانون يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ مركز حماية البيانات الشخصية خلال ٧٢ ساعة، وفي حال كان هذا الخرق أو الانتهاك متعلقاً باعتبارات حماية الأمن القومي فيكون الإبلاغ فوراً، وعلى المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فوراً، كما يلتزم بموافاة المركز خلال ٧٢ ساعة من تاريخ علمه بما يأتي: ١- وصف الخرق أو الانتهاك، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها ٢- بيانات مسؤل حماية البيانات الشخصية لديه. ٣- الآثار المحتملة لحدوث 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 لمواجهة. ٦- أي وثائق أو معلومات أو بيانات يطلبها المركز. وفي جميع الأحوال يجب على المتحكم أو المعالج، بحسب الأحوال، إخطار الشخص المعنى بالبيانات خلال ثلاثة أيام وأرى كباحث أنه كان يجب أن تتضمن اللائحة التنفيذية للقانون ضوابط ممارسة حق الشخص المعنى بالبيانات في معرفة أي خرق أو انتهاك للبيانات، على نسق المشرع الأوروبي. وتجدر الإشارة وفاء الشخص المعنى بالبيانات بمقابل تكلفة استفادته من الخدمات المتعلقة بممارسة حقوقه: في لفئة غير منطقية، وتتعارض مع الأصول القانونية المستقرة لممارسة الحق، ألزم المشرع، في الفقرة الثالثة من المادة الثانية، الشخص المعنى بالبيانات، بأداء مقابل مالي للمتحكم أو المعالج عند حصوله على خدمات تتعلق بممارسته للحقوق التي خولها له القانون. ويثير ذلك الدهشة، كيف يمنح القانون الحق للشخص الطبيعي من ناحية، وبكيله من ناحية أخرى بدفع مقابل مالي عند ممارسة كل حق على حدة؟ على الرغم من أن الخدمات التي يقدمها المتحكم في هذا المجال لا تخرج عن كونها خدمات إدارية لا تتكلف مبالغ تذكر، كما أنها تدخل في صميم عمل المتحكم أو المعالج. وتشمل الحقوق التي تخضع للوفاء بمقابل مالي للمتحكم أو المعالج كافة الحقوق المتقدم ذكرها (العلم بالبيانات - العدول عن الموافقة - التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات - تقييد المعالجة - الاعتراض على المعالجة). واستثنى المشرع فقط من دفع هذا المقابل حالة العلم والمعرفة بأي خرق أو اعتداء على البيانات الشخصية. ويتولى مركز حماية البيانات الشخصية إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه. ولا شك أن إلقاء هذا العبء المالي على عاتق الشخص الطبيعي قد يتعارض مع حقه الطبيعي في ممارسة الحقوق التي يخولها القانون، وخاصة في حالة إذا ما كان يرغب في ممارسة أكثر من حق، ومن ثم سيكون مضطراً للوفاء بمقابل مالي لكل خدمة على حدة. وعلى النقيض من ذلك راعت اللائحة الأوروبية مصالح الشخص المعنى بالبيانات وأتاحت له ممارسة جميع الحقوق ثانياً المذكورة مجاناً، با أي مقابل، وهو ما يعزز من فرص حماية البيانات الشخصية وقد ناقشت الورشة هذه المسألة وتفاوتت فيها آراء المشاركين، فاتجه البعض (رأي واحد) إلى أن هذه المقابل ضرورة حتى لا يحدث إفراط في ممارسة الحقوق وتضخم لطلبات على المعالج أو المتحكم. بينما اتجه الرأي الغالب إلى التوصية بتعديل القانون لإلغاء مقابل ممارسة الحقوق وأن يكون ذلك بصورة مجانية، كما فعلت بعض التشريعات. وتحوطاً، لحين تعديل القانون، يُراعى أن يكون هذا المقابل رمزياً حتى لا يرهق الشخص المعنى بالبيانات، وقد تحدد اللائحة التنفيذية ضوابط تحديد هذا المقابل ٢ - الالتزام بالإخطار في شأن تصحيح أو محو البيانات الشخصية أو تقييد المعالجة: لم يتضمن القانون أي التزام على المعالج والمتحكم بالإخطار في حالة تصحيح أو محو البيانات الشخصية أو تقييد المعالجة، واكتفى بالنص على الالتزام بالإخطار في حالة خرق أو انتهاك للبيانات الشخصية لديه، وفقاً للمادة ٧ من القانون، على نحو ما أشرنا. وفي المقابل نظمت المادة ١٩ من اللائحة الأوروبية الالتزام بالإخطار فيما يتعلق بتصحيح أو محو البيانات الشخصية أو تقييد المعالجة Notification obligation regarding rectification or erasure of personal data or restriction of processing ، التي تلزم المتحكم بإخطار كل متلق للبيانات تم الكشف عن البيانات الشخصية له، عن أي تصحيح أو محو للبيانات الشخصية أو تقييد المعالجة، ما لم يتبين أن ذلك مستحيل أو أنه يقتضى جهود لا تناسب قدراته. ويجب على المتحكم إخطار صاحب البيانات عن هواء المتلقين متى طلب ذلك. ٣ - تقديم الطلبات والشكاوى فما يتعلق بممارسة الحقوق (الطلبات): يجوز للشخص المعنى بالبيانات ولكل ذي صفة أن يتقدم إلى حائز أو متحكم أو معالج يطلب يتعلق بممارسة حقوقه المنصوص عليها في هذا القانون، مثل تعديل البيانات أو حذفها، وفي هذه الحالة يلتزم المقدم إليه الطلب بالرد عليه خلال ستة أيام عمل من تاريخ تقديمه إليه (م ٣٢ من القانون) - كما كان المشرع المغربي أكثر مراعاة لمصالح الشخص المعنى بالبيانات، فقد منحه ممارسة الحقوق بدون مقابل، ونص صراحة على أن يكون ذلك "دون عوض". ومثال ذلك ما نصت عليه المادة ٨ أ من القانون على أن: "ولتلتزم المسؤل عن المعالجة بالقيام بالتصحيحات اللازمة دون عوض لفائدة الطالب..". الشكاوى"

٥- الحق في الاعتراض على معالجة البيانات الشخصية: تشير المادة الثانية من القانون إلى حق الشخص المعنى بالبيانات في الاعتراض على معالجة البيانات أو نتائجها متى تعارضت مع حقوقه وحرياته الأساسية. ووفقاً للمادة ٢١ من اللائحة الأوروبية لحماية البيانات يحق للشخص في أي وقت الاعتراض على معالجة بياناته الشخصية Right to object وفقاً للفقرة الأولى من المادة (٦) (البند هـ) أو و) من اللائحة وذلك للأسباب التي تنشأ من وضعه الخاص؛ وهذا ينطبق أيضاً على إعداد الملفات الشخصية على أساس هذه الأحكام. ومن هنا لا يجوز للشخص المسئول بعد ذلك أن يقوم بمعالجة البيانات الشخصية المتعلقة بصاحب البيانات ما لم يتمكن من إثبات أسباب مشروعة مقنعة للمعالجة تفوق مصالحه وحقوقه وحرياته، أو أن المعالجة تهدف إلى فرض إقامة دعاوى قانونية أو الدفاع فيها. وإذا ما جرت معالجة البيانات الشخصية المتعلقة بصاحب البيانات لأغراض التسويق المباشر، فله الحق في الاعتراض في أي وقت على معالجة بياناته الشخصية لأغراض هذا الإعلان؛ وهذا ينطبق أيضاً على إعداد الملفات الشخصية طالما أنه مرتبط بهذا البريد المباشر. وإذا اعترض صاحب البيانات على المعالجة لأغراض التسويق المباشر، فإيجوز بعدها معالجة بياناته الشخصية لهذه الأغراض (م ٢١ / ٢، ٣ من اللائحة .

أورى كباحث أن هناك حق لصاحب البيانات وهو الحق في إمكانية نقل البيانات: أغفل المشرع المصري النص على حق الشخص المعنى بالبيانات في نقل البيانات الشخصية الخاصة به، رغم أنه من الحقوق المهمة. ولم يفت المشرع الأوروبي النص على هذا الحق في إمكانية نقل البيانات Right to data portability في اللائحة الأوروبية حيث تضمنها نص المادة ٢٠ منها، الذي جرى على أن يكون للشخص المعنى بالبيانات الحق في تلقي بياناته الشخصية التي قدمها إلى الشخص المسئول بتنسيق منظم ومعروف ويمكن قراءته آلياً. وبالإضافة إلى ذلك، لديك الحق في نقل هذه البيانات إلى شخص آخر مسؤول عنها دون عائق من قبل الشخص المسئول عن توفير البيانات الشخصية، شريطة أن: - تعتمد المعالجة على الموافقة على النحو الوارد في المادة ٦ الفقرة ١ (بند أ) من اللائحة أو المادة ٩ الفقرة ٢ (بند أ) من اللائحة أو بعقد وفقاً للمادة ٦ الفقرة ١ (بند ب) من

اللائحة. - تتم المعالجة بوسائل آلية. وبممارسة هذا الحق، يكون لصاحب البيانات أيضاً الحق في التحقق من إرسال بياناته الشخصية مباشرةً من شخص إلى آخر، طالما أن ذلك ممكن من الناحية التقنية. ولا يجوز أن تتأثر الحريات وحقوق الأشخاص الآخرين. ولا ينطبق الحق في نقل البيانات على معالجة البيانات الشخصية اللازمة لأداء مهمة لأغراض المصلحة العامة أو في ممارسة السلطة الرسمية المفوضة للشخص المسئول. لذلك أرى كباحث بتعديل القانون للنص على الحق في نقل البيانات (على غرار ما فعل المشرع الأوروبي)، باعتبار أن القانون هو الذي ينشأ الحق ويحميه، ولا يجوز لللائحة أن تضع من قبل السلطة التنفيذية (وزير الاتصالات) أن تنشئ الحقوق. لذلك أكد كباحث المشرع المصري اكتفى بمجرد تعداد وحصر حقوق الشخص المعنى بالبيانات دون الدخول في تفصيلاتها وابتعد عن تحديد ضوابط إنفاذ هذه الحقوق، رغم أن اللائحة الأوروبية تتضمن تفصيلات دقيقة لضوابط ومحددات هذه الحقوق، ولم تكن مجرد النص عليها. وأرى كباحث بأن تكون علاقة المتحكم بالمعالج في القانون المصري بناء على تعليمات تعاقدية واضحة، وأكدت على ضرورة أن تكون في صورة تعاقدية، على أن يفرض ذلك أيضاً على كل متحكم أو معالج من الباطن. ويجب أن تخضع أنشطة معالجة البيانات لعقد أو أي تصرف قانوني آخر مع المتحكم، على أن يحدد العقد موضوع ومدة وغرض المعالجة، وأنواع معالجة البيانات الشخصية والإجراءات الأمنية والتزامات وحقوق المعالج والمتحكم. وعند إنهاء العقد مع المتحكم، يجب على المعالج إعادة البيانات الشخصية أو حذفها، بالإضافة إلى ذلك، إذا أراد المعالج إشراك معالج آخر (معالج فرعي) وجب عليه الحصول على إذن كتابي من المتحكم. بأن المبالغة في فرض الالتزامات على جميع القائمين على معالجة البيانات قد يكون غير مناسب حالياً للمجتمع المصري. كما يجب من جهة أخرى تحديد طبيعة علاقة الشخص المعنى بالبيانات مع الحائز أو المعالج أو المتحكم.

الخاتمة

تناولنا فى هذا البحث الضوابط التشريعية لجمع ومعالجة البيانات الشخصية جمع ومعالجة البيانات بطريقة مشروعة وملائمة لأغراض تجميعها لم يكتف المشرع المصري بالنص على ضرورة جمع البيانات بطريقة مشروعة، وإنما اشترط أيضاً، فى المادة الثالثة (فقرة أولى، بند ٣) "أن تُعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها". ويعني هذا الشرط عدم جواز جمع أو تجهيز أو تسجيل أية بيانات شخصية أو معلومات بأساليب أو بطرق غير مشروعة أو بغير رضا الشخص المعنى أو من ينوب عنه لذلك يحظر على القائمين على معالجة البيانات القيام بجمعها أو تسجيلها بأساليب أو بطرق غير مشروعة مع بيان مدة الاحتفاظ بالبيانات الشخصية و أن تكون صحيحة وسليمة ومؤمنة مع بيان حقوق الشخص المعنى بالبيانات المعالجة إلكترونياً. وحظر المشرع المصري، فى المادة الثالثة من قانون حماية البيانات الشخصية، الفقرة الرابعة بند ٤، أن يتم الاحتفاظ بالبيانات التي يتم معالجتها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها. فالاحتفاظ بالبيانات لا يجوز أن يكون أبدياً بل يكون مؤقتاً ومحدداً لمدة معينة، ويعنى ذلك أنه يتعين على المعالج أن يقوم بحفظ البيانات التي تمت معالجتها لمدة زمنية معينة بحيث لا تتجاوز المدة المطلوبة للأغراض التي جمعت من أجلها ثم تطرقت لحقوق الشخص المعنى بالبيانات .

النتائج

- ١- أصدر المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠م وذلك لمواجهة تفاقم الاعتداءات على البيانات الشخصية بما استدعى تدخلاً من جانب المشرع وكذلك شمولها بالحماية الدستورية . حيث ان خصوصية جرائم الاعتداء على الحياة الخاصة او البيانات الشخصية أظهرت مشكلة المكافحة الاجرائية للجريمة المعلوماتية . الامر الذى دفع المشرع للسعى لمواكبة التطور الذى لحق بالجريمة المعلوماتية .
- ٢- نص القانون على التزامات تقع على عاتق المعالج والمتحكم والحائز وذلك حماية للبيانات الشخصية من الاختراق أو الاعتداء حتى من جانب القائمين على جمعها وتخزينها
- ٣- تأقيت احتفاظ الجهة الإدارية بالبيانات الشخصية وأن يكون الاحتفاظ لإغراض مشروعة
- ٤- حقوق صاحب البيانات المعالجة مما لاشك فيه أن الشخص الذى تتم معالجة بياناته الشخصية هو المقصود بالحماية من قبل قانون حماية البيانات الشخصية ، حيث يهدف القانون إلى حماية الشخص من الاعتداء على بياناته الشخصية وقد أعطى المشرع الفرنسى والمصرى حقوق للشخص على بياناته لمن يتم معالجة بياناته ومنها الحق فى تصحيح أو تعديل أو محو البيانات الشخصية وغيرها من الحقوق

التوصيات

- ١- أرى كباحث أن هناك حق لصاحب البيانات وهو الحق في إمكانية نقل البيانات حيث أغفل المشرع المصري النص على حق الشخص المعنى بالبيانات في نقل البيانات الشخصية الخاصة به، رغم أنه من الحقوق المهمة
- ٢- وأرى كباحث بأن تكون علاقة المتحكم بالمعالج في القانون المصري بناء على تعليمات تعاقدية واضحة، وأكدت على ضرورة أن تكون في صورة تعاقدية، على أن يفرض ذلك أيضاً على كل متحكم أو معالج من الباطن. ويجب أن تخضع أنشطة معالجة البيانات لعقد أو أي تصرف قانوني آخر مع المتحكم، على أن يحدد العقد موضوع ومدة وغرض المعالجة، وأنواع معالجة البيانات الشخصية والإجراءات الأمنية والتزامات وحقوق المعالج والمتحكم. وعند إنهاء العقد مع المتحكم، يجب على المعالج إعادة البيانات الشخصية أو حذفها، بالإضافة إلى ذلك، إذا أراد المعالج إشراك معالج آخر (معالج فرعي) وجب عليه الحصول على إذن كتابي من المتحكم. بأن المبالغة في فرض الالتزامات على جميع القائمين على معالجة البيانات قد يكون غير مناسب حالياً للمجتمع المصري. كما يجب من جهة أخرى تحديد طبيعة علاقة الشخص المعنى بالبيانات مع الحائز أو المعالج أو المتحكم.
- ٣- يجب توسعة نطاق مظلة حماية البيانات الشخصية لتشمل البيانات الشخصية لدى الجهات الاتية البيانات الشخصية لدى البنك المركزي، والبيانات المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية ولدى جهات الأمن القومي، حيث كان من الأولى وضعها تحت مظلة الحماية وفق ضوابط تراعى خصوصيتها، وليس استبعادها على إطلاقها.
- ٤- ويحظر تخزين البيانات الاسمية التي من شأنها أن تظهر مباشرة أو غير مباشرة الأصل العرقي أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماء النقابي للشخص أو تتعلق بصحته أو علاقاته الجنسية فلايجوز أن يتضمن الاسميين أى سؤال يتضمن هذه الامور ، كما لايجوز تخزينها في حالة الحصول عليها بطريق مشروع . ولايجوز أن يتضمن طلب الاستخدام أسئلة عن الإلتناء النقابي والاراء
- ٥- وكان يجب تحديد مدة الاحتفاظ بالبيانات ، وكذلك ان يفرض المشرع عقوبة وجزاء في حال الاحتفاظ بالبيانات لمدة أطول من المدة المحددة

المراجع

- أشرف محمد عبده - الحكومة الإلكترونية، وتطبيقاتها في البلدان العربية - دار الكتب والدراسات العربية
٢٠١٨ م - ص ٥٤ - أنشأ المعهد الفيدرالي للاتصالات (IFT) في عام ٢٠١٦
- أستاذنا الدكتور / أسامة عبد الله قايد الحماية الجنائية للحياة الخاصة وبنوك المعلومات - دار النهضة
العربية ٢٠٠٨
- أستاذنا الدكتور / احمد فتحي سرور - الحماية الدستورية للحقوق والحريات - دار الشروق - القاهرة
٢٠٠٠
- د/ سامح عبد الواحد التهامي - الحماية القانونية للبيانات الشخصية - دراسة القانون الفرنسي، القسم
الأول، مجلة الحقوق جامعة الكويت، المجلد ٣٥ ، العدد ١١ ، ٢٠١١ ،
- د. شريف يوسف خاطر: حق الاطاع على البيانات الشخصية في فرنسا، مجلة كلية القانون الكويتية
العالمية، السنة الثالثة، العدد التاسع، مارس ٢٠١٥ م، ص ٢٨١ ، ٢٨٢ - ٢٨٣ .
- د/ عبد الهادي فوزى العوضى : الحق في الدخول في طي النسيان على شبكة الإنترنت -
- د/ عثمان بكر عثمان المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي
- د/ محمد سامي عبد الصادق: شبكات التواصل الاجتماعي ومخاطر إنتهاك الحق في الخصوصية ، دار
النهضة العربية القاهرة ، ٢٠١٦
- د/ محمد عزت عبد العظيم ، الجرائم المعلوماتية الماسة بالحياة الخاصة ، دار النهضة العربية - القاهرة
٢٠١٨ م
- يونس عرب : المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي اتحاد المصارف
العربية الطبعة الأولى ٢٠٠٢ م ص ٩ .
- د/ محمد رشيد حامد - الحماية الجزائية للمعلومات الشخصية في مواجهة أخطار البنوك - رسالة ماجستير
- كلية الحقوق - جامعة آل البيت -
- د. سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية - دراسة القانون الفرنسي، القسم الأول،
مجلة الحقوق جامعة الكويت، المجلد ٣٥ ، العدد ١١ ، ٢٠١١
- د. وليد السيد سليم: ضمانات الخصوصية في الانترنت، دار الجامعة الجديدة، ٢٠١٢ ، ص ٥٨٨ وما
بعدها. ونشير إلى قرار رقم ١٣٠ الصادر عن مندى البيانات العالمي ٢٠١٨ م بدولة الامارات العربية المتحدة
- د/ سامي الشوا الغش المعلوماتي كظاهرة اجرامية مستحدثة ورقة عمل مقدمة للمؤتمر السادس للجمعية
المصرية للقانون الجنائي القاهرة من ٢٥ - ٢٨ اكتوبر ١٩٩٣ م
- د/ طارق عزت رجا قانون حقوق الانسان بين النظرية والتطبيق في الفكر الوضعي والتشريعية الاسلامية
كلية الحقوق جامعة المسيرة الكبرى طبرق الجماهيرية اللبية - دار النهضة العربية ٢٠٠٤ م ٢٠٠٥ م
- د/ عفيفي محمود التطورات الحديثة في تكنولوجيا المعلومات
- د/ سامي الشوا الغش المعلوماتي كظاهرة اجرامية مستحدثة ورقة عمل مقدمة للمؤتمر السادس للجمعية
المصرية للقانون الجنائي القاهرة من ٢٥ - ٢٨ اكتوبر ١٩٩٣ م

- د/ طارق عزت رجا قانون حقوق الانسان بين النظرية والتطبيق فى الفكر الوضعى والشريعة الاسلامية
كلية الحقوق جامعة المسيرة الكبرى طبرق الجماهيرية الليبية - دار النهضة العربية ٢٠٠٤م ٢٠٠٥م
- د/عفيى محمود التطورات الحديثة فى تكنولوجيا المعلومات مرجع سابق
- أستاذنا الدكتور محمد حسام محمود لطفى الحماية القانونية لبرامج الحاسب الإلكترونى - دار الثقافة
للطباعة والنشر - القاهرة ١٩٨٧
- د/ ناجح احمد عبد الوهاب - التطور الحديث للقانون الإدارى فى ظل نظام الحكومة الإلكترونية رسالة
دكتوراه كلية الحقوق - جامعة القاهرة ٢٠١١
- أستاذنا الدكتور / أسامة عبد الله قايد الحماية الجنائية للحياة الخاصة وبنوك المعلومات - دار النهضة
العربية ٢٠٠٨
- محمد سامى عبد الصادق، شبكات التواصل الاجتماعى ومخاطر انتهاك الحق فى الخصوصية، درا النهضة
العربية
- وسيم شفيق النظام القانونى لوسائل التواصل الاجتماعى دراسة مقارنة حول الحرية الشخصية
والاختصاص مرجع سابق
- د/ محمد رشيد حامد - الحماية الجزائية للمعلومات الشخصية فى مواجهة أخطار البنوك - رسالة
ماجستير - كلية الحقوق - جامعة أُل البيت
- د. بولين أنطونيوس الانسان عجالي، جمال عبد الناصر، الحماية الجنائية من اشكال المساس بحرمة الحياة
الخاصة عبر المكالمات والصور، دراسة مقارنة ، الجزائرى ، ص ٦ أيوب، المرجع السابق،
- د/ عبد الفتاح بيومى حجازى - مكافحة جرائم الكمبيوتر فى القانون العربى - دار الكتب القانية مصر -
٢٠٠٤م
- الجبورى، سليم عبد الله، (١٤٢٢)، الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الأولى، منشورات
الحلبى الحقوقية ، لبنان
- د/عبد القادر عمير -الحماية الجنائية للحق فى الحياة الخاصة فى البيئة الرقمية
- أستاذنا الدكتور / حسام لطفى : الإطار القانونى للمعاملات الإلكترونية دار النهضة العربية القاهرة ٢٠٠٣
- د أمنية مصطفى صادق شبكات المعلومات الإلكترونية المفتوحة وأثارها على العمل مع تصور وطنى لآبعاد
دورها فى خدمات المعلومات فى مصر ، عالم الكتب ، مج ١٨ ع ٢٤ مارس - ابريل ١٩٩٧ .
- د. وليد السيد سليم: ضمانات الخصوصية فى الانترنت، دار الجامعة الجديدة، ٢٠١٢ ، ص ٥٨٨ وما
بعدها. ونشير إلى قرار رقم ١٣٠ الصادر عن مندى البيانات العالمى ٢٠١٨م بدولة الامارات العربية المتحدة
- د/ محمد رشيد حامد - الحماية الجزائية للمعلومات الشخصية فى مواجهة أخطار البنوك - رسالة
ماجستير - كلية الحقوق - جامعة أُل البيت
- د/محمد سامى عبد الصادق: شبكات التواصل الاجتماعى ومخاطر إنتهاك الحق فى الخصوصية ، دار
النهضة العربية القاهرة ، ٢٠١٦
- د/ حسام الدين الأخوانى - الحاسب الألى والحياة الخاصة

- نهلا عبد القادر، الجرائم المعلوماتية ،

- أستاذنا الدكتور / حسام لطفى : الإطار القانونى للمعاملات الإلكترونية دار النهضة العربية القاهرة ٢٠٠٣

د/ حسام الدين كامل الاهوائى : الحق فى احترام الحياة الخاصة

- د. علاء عيد طه: الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية (٢٠١٦ الصادر عن البرلمان الأوربي، / وتداولها (دراسة في ضوء اللائحة التنظيمية رقم ٦٧٩ . ١٤٤١ / ٥ ٢٠٢٠ م،) مجلة جامعة الملك سعود ، الحقوق والعلوم السياسية، مج (٣٢)

- د. شريف يوسف خاطر: حق الاطلاع على البيانات الشخصية في فرنسا، مجلة كلية القانون الكويتية العالمية، السنة الثالثة، العدد التاسع، مارس ٢٠١٥ م،

- الإعان العالمى لحقوق الإنسان الصادر عام ١٩٤٨ :

المواقع :

<https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

<https://www.elwatannews.com/data/iframe/p>

<https://www.elwatannews.com/data/iframe/pdf/25021748.pdf/25021748.pdf>

<https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview>

<http://gate.ahram.org.eg/News/2224851.aspx>

<https://bit.ift.org.mx/BitWebApp/> :Banco de Información de Telecomunicaciones

<https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview>

<https://www.elwatannews.com/data/iframe/pdf/25021748.pdf>

<https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview>

<https://www.elwatannews.com/data/iframe/pdf/25021748.pdf>

<https://transparencyreport.google.com/eu-privacy/overview?hl=ar&hl=es>

القوانين :-

- قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ م
- اللا قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ م نحة التنفيذية قلنون حماية الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ م
- التوجيه الأوربي الاصدار عن البرلمان الأوربي في ٢٤ من أكتوبر ١٩٩٥ م
- القانون رقم ٣٠ لسنة ٢٠١٨ م قانون حماية البيانات الشخصية البحريني .
- القانون المغربي المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي القانون المغربي رقم ٨ لسنة ٢٠٠٩
- قانون البيانات الشخصية التونسي ٦٣ لسنة ٢٠٠٤

المراجع الاجنبية

European Union Agency for Fundamental Rights, and Council of Europe, -
Handbook on European data protection

law, Luxembourg: Publications Office of the European Union, 2014, pp 61-76-

[https://www.legifrance.gouv.fr/recguri gudi.reprise- true-fastreqid-15050935377page 3](https://www.legifrance.gouv.fr/recguri%20gudi.reprise-true-fastreqid-15050935377page%203)

Maxime BESÈME :Le droit à l'oubli numérique dans le droit de l'Union ." ."
européenne, Consécration prétorienne et législative ,Mémoire UCL(Université
catholique de

Louvain ,)2015-2016 .Disponible sur Internet
/:<https://dial.uclouvain.be/memoire/ucl>

الفهرس

رقم الصفحة	الموضوع
٢	اهمية البحث ومهج الدراسة
٤	المقدمة
	المبحث الاول :- ضوابط جمع ومعالجة البيانات الشخصية فى
٥	ظل الإدارة الإلكترونية .
	المطلب الأول : أن يتم جمع البيانات الشخصية لأغراض مشروعة ومحدد ومعلنة
٥	للشخص صاحب البيانات .
١١	المطلب الثانى : أن تكون صحيحة وسليمة ومؤمنة .
	المطلب الثالث : أن تعالج بطريقة مشروعة وملائمة للأغراض التى تم
١٣	تجميعها من أجلها .
	المطلب الرابع : الأيتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء
١٥	بالغرض المحدد لها .
١٧	المبحث الثانى : التزامات المتحكم والمعالج والحائز وحقوق صاحب البيانات .
١٨	المطلب الأول : إلتزامات المتحكم .
٢٥	المطلب الثانى التزمات المعالج .
٢٩	المطلب الثالث : حقوق صاحب البيانات المعالجة .
٣٦	الخاتمة
٣٦	النتائج
٣٧	التوصيات
٣٨	المراجع
٤٢	الفهرس
٤٣	الملخص

Summary

The law expresses the images of persons in the protection of their personal data, It criminalizes data collection illegally or without the consent of its owners, and criminalizing processing it in fraudulent ways or not in conformity with the purposes authorized by the data owner and regulating the transfer and processing of data across borders for the benefit of citizens and the national economy, thus contributing to the protection of investments and businesses. It also complies with international standards in the areas of personal data protection, through the rules, standards and requirements imposed by it, and supervised by .the Data Protection Center established for this purpose

Where the successive developments of information and communication technology, especially with the emergence of the technology of the Internet of Things, cloud computing, artificial intelligence and others, to the emergence of new challenges at the level of personal data protection, as the scope and volume of collection, exchange and processing of this data electronically increased in an unprecedented way, which allowed companies and private and public institutions to use the personal data of individuals on a large scale because electronic activities based on the collection, analysis, deduction and storage of such data help Businesses and organizations are increasingly getting economic and commercial benefit from that digital data. . In this research, we discussed the legislative controls for collecting and processing personal data, collecting and processing data in a lawful and appropriate manner for the purposes of its collection. The Egyptian legislator not only stipulated the need to collect data in a legitimate manner, but also stipulated, in Article Three (first paragraph, clause 3) “that it be treated in a legitimate and appropriate manner.” for the purposes for which it was collected.” This condition means that no personal data or information may be collected, processed, or recorded by illegal methods or methods or without the consent of the person concerned or his representative. In illegal ways, with an indication of the period of retention of personal data, and that it be true, sound and secure, with an indication of the rights of the person concerned with the

electronically processed data. And the Egyptian legislator prohibited, in Article 3 of the Personal Data Protection Law, fourth paragraph, clause 4, that the data being processed be kept for a period longer than the period necessary to fulfill the purpose specified for it. Retention of data may not be eternal, but rather be temporary and limited to a certain period, and this means that the processor must save the processed data for a certain period of time so that it does not exceed the period required for the purposes for which it was collected and then touched upon the rights of the person concerned with the data

-:Keywords

personal data collection - the rights of the data subject - the obligations of the custodian and processor - the legality and objectives of data collection

Title:- Controls for the collection and processing of personal data under electronic management - authored by Dr. Walid Ramadan Abdel Razeq Mahmoud, Doctor of Public Law