الحماية القانونية للبيانات الشخصية فى عصر التكنولوجيا الرقمية

د.هبه رمضان رجب
دكتوراه فى القانون المدنى

الحماية القانونية للبيانات الشخصية فى عصر التكنولوجيا الرقمية

الملخص

أصبح التعامل مع البيانات الشخصية للأفراد أمرا شبه يومى، فكثيرا ما تتطلب الهيئات (العامة – الخاصة) التى يتعامل معها الأفراد أن يقدم الشخص بياناته الشخصية للحصول على خدمة معينة، فتقوم تلك الهيئات بتجميع البيانات الشخصية المتاحة لديها، ثم تقوم بالإفصاح عنها لجهات أخرى للمتاجرة بتلك البيانات، وهو ما يعد انتهاكا لخصوصية البيانات الشخصية لهؤلاء الأفراد، وقد زادت هذه الإنتهاكات بشكل متسارع خصوصا مع التطور التكنولوجى ورقمنة حياة الأفراد، وإتاحة بياناتهم الشخصية فى البيئة الرقمية.

تهدف الدراسة إلى بيان مفهوم البيانات الشخصية واشتراطات جمعها ومعالجتها، وبيان المخاطر التى تهدد أمنها وسريتها، وبيان نطاق الحماية التى أضفاها القانون على البيانات الشخصية، مع بيان أوجه القصور الذى يعترى قانون حماية البيانات الشخصية، والذى يلزم معالجته فى اللائحة التنفيذية التى سوف يتم إصدارها، لضمان حماية فعالة لخصوصية البيانات الشخصية للأفراد.

واعتمدت الدراسة على المنهج التحليلى المقارن، بتحليل نصوص القانون المصرى ١٥١ لسنة ٢٠٢٠، فى ضوء اللائحة الأوروبية ٦٧٩/ ٢٠١٦ الذى استمد نصوصه منها، ومقارنته بها لبيان أوجه القصور الذى اعترى القانون المصرى.

وقد تم تقسيم الدراسة إلى ثلاثة مباحث: المبحث الأول: المقصود بالبيانات الشخصية محل الحماية، المبحث الثانى: الإطار القانونى لحماية البيانات الشخصية، المبحث الثالث: الإشكاليات القانونية التى تثيرها عملية المعالجة.

الكلمات المفتاحية: الحماية القانونية– البيانات الشخصية العادية– البيانات الشخصية الحساسة– التكنولوجيا الرقمية– حق النسيان الرقمى– أمن البيانات.

المقدمة

أدى إنتشار وتطور التقنيات التكنولوجية الحديثة إلى رقمنة حياة الأفراد، وتم التحول من المعالجة الورقية للبيانات إلى المعالجة الإلكترونية، فلم تعد البيانات الشخصية للأفراد حبيسة الأوراق والدفاتر، بل غدت

موضوعة فى بيئة رقمية متاحة للجميع يسهل الوصول إليها، مما يعرض تلك البيانات للعديد من الإنتهاكات[١].

فتم استخدام الحاسوب فى إنشاء قواعد للبيانات الشخصية للأفراد، وتكوين شبكات بين العديد من الجهات التى تنشئ تلك القواعد لتسهيل تبادل البيانات الشخصية فيما بينها، وظهر أيضا ما يسمى بالتسويق الإلكترونى الذى يستخدم البيانات الشخصية للعميل فى أساليب الدعاية والإعلان، وهو قد ينطوى على انتهاكا لخصوصية البيانات الشخصية للأفراد، ومساسا بحقوقهم وحرياتهم الأساسية، لاسيما أن خصوصية البيانات الشخصية تمس بحق دستورى ألا وهو الحق فى حرمة الحياة الخاصة[٢].

وقد تطور مفهوم الحق فى الخصوصية نتيجة لتطور تقنيات التكنولوجيا الرقمية، وأصبح يتسع ليشمل الحق فى حماية الخصوصية المعلوماتية للأفراد، وأصبح يضمن أيضا حماية سرية الإتصالات وحماية البيانات الشخصية لهم، أضف إلى ذلك أن هناك صلة وثيقة بين الحق فى الخصوصية والحق فى حماية البيانات الشخصية، تلك البيانات التى تعد أحد عناصر الحق فى الخصوصية، والتى تدخل فى صميم الحق فى حرمة الحياة الخاصة، وتعد أحد مقومات الحياة الخاصة بالأفراد، كما أن الإعتداء عليها يعد مظهر من مظاهر الإعتداء الصارخ على خصوصيتهم[٣].

وعليه فقد أصبح التدخل التشريعى أمر لازما وحتميا لحماية البيانات الشخصية فى عصر التكنولوجيا الرقمية، ذلك العصر الذى أصبح معه من السهل اليسير الحصول على البيانات الشخصية للأفراد وتجميعها وتخزينها، بل وإمكانية نقلها وتعديلها وحذفها فى ثوانى معدودة، وهو مايقتضى وضع ضوابط لحماية هذه البيانات الشخصية[٤].

الأمر الذى أثار حفيظة العديد من الدول الأوروبية منها والعربية، فأصدر البرلمان والمجلس الأوروبى اللائحة الأوروبية لحماية البيانات الشخصية ٦٧٩ لسنة ٢٠١٦[٥]، وصار على هديها المشرع المصرى فقام

---

[١] Ridha Hemici, Legal warranties for personal data protection within the numerical space, Special edition-inpac ,University of Kasdi Merbah Ouargla, Algeria, November 2019, p. 51.

[٢] المادة (٩٢) من الدستور المصرى ٢٠١٤.

[٣] طارق جمعه السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية فى العصر الرقمى، دراسة مقارنة، مجلة القانون والإقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع ٩٢، ص ١٠٩، ١١٠.

[٤] سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليا، دراسة مقارنة، مجلة العلوم القانونية والإقتصادية، كلية الحقوق جامعة عين شمس، مج ٦٢، ع ١، ٢٠٢٠، ص ٢.

[٥] لائحة الإتحاد الأوروبى ٢٠١٦/٦٧٩ الصادرة عن البرلمان الأوروبى والمجلس الأوروبى بتاريخ ٢٧ أبريل ٢٠١٦ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات؛ والذى ألغى التوجيه ٤٦/٩٥، انظر الرابط الآتى:
https://www.cnil.fr/en/official-texts.

بإصدار قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠[٦] إمعانا فى الحفاظ على خصوصية البيانات الشخصية للأفراد وحمايتها ضد أى إنتهاك.

أهمية الدراسة

يكتسب هذا الموضوع أهمية كبيرة كونه يتناول حماية البيانات الشخصية للأفراد خصوصا البيانات الشخصية الرقمية، التى باتت عرضة للعديد من الإنتهاكات فى عصر التكنولوجية الرقمية، فالبيانات الشخصية تعد أحد الحقوق اللصيقة بالإنسان ومن أهم خصوصياته.

أهداف الدراسة

تهدف الدراسة إلى بيان مفهوم البيانات الشخصية، واشتراطات جمعها وتداولها ومعالجتها إلكترونيا، وبيان المخاطر التى تهدد أمنها وسريتها، وإلى بيان أوجه الحماية التى قررها قانون حماية البيانات الشخصية، مع بيان أوجه القصور الذى يعتريه، والذى يلزم معالجته فى اللائحة التنفيذية التى سوف يتم إصدارها لاحقا، لضمان حماية فعالة لخصوصية البيانات الشخصية للأفراد.

منهج الدراسة

اعتمدت الدراسة على المنهج التحليلى المقارن، من خلال تحليل النصوص القانونية المتعلقة بحماية البيانات الشخصية فى ضوء كلا من القانون المصرى لحماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠، ونصوص اللائحة الأوروبية ٦٧٩ / ٢٠١٦، ومقارنتهم لبيان أوجه القصور الذى اعترى نصوص القانون المصرى.

إشكالية الدراسة

تثير الدراسة عدة إشكاليات أهمها:

- ما هى الحماية القانونية المقررة لحماية البيانات الشخصية فى العصر الرقمى؟
- هل يشمل قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠ حماية البيانات الشخصية التقليدية والرقمية؟
- ما هى الضوابط القانونية المقررة لحماية البيانات الشخصية؟
- ما هى الإجراءات التى يلزم اتخاذها لحماية أو وقف انتهاك خصوصية البيانات الشخصية؟

[٦] تم نشره فى الجريدة الرسمية – العدد ٢٨ مكرر (هـ) فى ١٥ يوليه سنة ٢٠٢٠.

- ما هى الإشكاليات القانونية التى تثيرها عملية المعالجة؟

خطة البحث

المبحث الأول: المقصود بالبيانات الشخصية محل الحماية.

المطلب الأول: ماهية البيانات الشخصية وأنواعها.

المطلب الثانى: المخاطر التى تهدد خصوصية البيانات الشخصية للأفراد.

المطلب الثالث: اشتراطات جمع ومعالجة وتخزين البيانات الشخصية فى العصر الرقمى.

المبحث الثانى: الإطار القانونى لحماية البيانات الشخصية

المطلب الأول: حقوق الشخص المعنى بالبيانات الشخصية.

المطلب الثانى: الإجراءات التى يلزم اتخاذها لحماية ووقف انتهاك خصوصية البيانات الشخصية.

المطلب الثالث: التزامات القائم بعملية المعالجة.

المبحث الثالث: الإشكاليات القانونية التى تثيرها عملية المعالجة

المطلب الأول: أمن البيانات الشخصية.

المطلب الثانى: الحق فى النسيان الرقمى.

المطلب الثالث: معالجة البيانات الشخصية الحساسة خصوصا تلك المتعلقة بالأطفال.

المطلب الرابع: البيانات الشخصية للأفراد محل تطبيقات الذكاء الإصطناعى.

المبحث الأول
المقصود بالبيانات الشخصية محل الحماية

المطلب الأول: ماهية البيانات الشخصية وأنواعها

يعد الفقيه (آلان ويستون) من أوائل الفقهاء الأمريكيين الذين عنوا بحماية البيانات الشخصية، وقام بتعريف خصوصية البيانات عام ١٩٦٧، فى مؤلفه الخصوصية والحرية، بأنها: "حق الفرد فى تحديد متى وكيف، وإلى أى مدى تصل البيانات الخاصة به إلى الآخرين".

بينما عرفها الفقيه (ميلر) فى مؤلفه عام ١٩٧١ بعنوان (الإعتداء على الخصوصية)، بأنها: "قدرة الفرد فى التحكم فى دورة المعلومات المتعلقة به"، أى حق الفرد فى منع الآخرين من الإطلاع أو التصرف فى المعلومات المتعلقة بحياته الخاصة[٧].

فيما عرف المشرع المصرى البيانات الشخصية فى المادة (١) من الفصل الأول من القانون الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، وعرفها بأنها: "أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده بشكل مباشر أو غير مباشر، عن طريق الربط بين هذه البيانات وأى بيانات أخرى، كالإسم أو الصوت أو الصورة، أو رقم تعريفى أو محدد للهوية عبر الإنترنت أو أى بيانات تحدد الهوية النفسية أو الصحية أو الإقتصادية أو الثقافية أو الإجتماعية" .

بينما عرفتها (١/٤) من اللائحة الأوروبية بشأن حماية البيانات ذات الطابع الشخصى، بأنها: "أى معلومات تتعلق بشخص طبيعى محدد أو يمكن تحديده بشكل مباشر أو غير مباشر، على وجه الخصوص عن طريق الرجوع إلى عنصر أو أكثر من العناصر المميزة له، مثل: الإسم أو الرقم التعريفى أو بيانات الموقع أو معرف الإتصال عبر الإنترنت، أو الخصائص الفسيولوجية أو أو الوراثية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعية".

ومما سبق ذكره من تعريفات يمكننا القول بأن: البيانات الشخصية أو البيانات ذات الطابع الشخصى هى: "تلك البيانات التى ترتبط بشخص طبيعى محدد أو قابل للتحديد بشكل مباشر أو حتى غير مباشر من خلال الربط بينها وبين أنماط البيانات الشخصية المحددة سلفا".

وقد أحسن المشرع صنعا بتحديد أنماط البيانات الشخصية الخاضعة للحماية القانونية من خلال ذكره لأمثلة للبيانات الشخصية، مما جعل مفهوم البيانات الشخصية أكثر دقة، وجعل التعريف الوارد أكثر مرونة بحيث يتسع لمختلف أنماط البيانات الشخصية.

كما يتضح لنا من النص السابق أن المشرع المصرى قد قصر حماية البيانات الشخصية على الأشخاص الطبيعيين فقط دون الإعتباريين، فالبيانات المتعلقة بالأشخاص الإعتبارية مستبعدون من نطاق الحماية القانونية، إلا إذا كانت تلك البيانات متعلقة بالأفراد الذين يمثلون الشخص الإعتبارى[٨].

---

[٧] شلواح ميرة، بشيرى كهينة، المسؤولية المدنية عن انتهاك حق الخصوصية فى المجال الرقمى، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة–بجاية، ٢٠١٩–٢٠٢٠، ص ١٠.

أضف إلى ما تقدم أن قانون حماية البيانات الشخصية قد إختص بحماية ومعالجة البيانات الشخصية الرقمية دون التقليدية، فلم يهتم المشرع بمعالجة البيانات الشخصية التقليدية ولم يشملها بالحماية لا فى القوانين العامة ولا فى قانون حماية البيانات الشخصية، وليس أدل على ذلك من تعريفة لعملية معالجة البيانات الشخصية، وذكره لفظ "الإلكترونية أو التقنية".

أما عن أنواع البيانات الشخصية:

فهناك نوعين من البيانات الشخصية:

النوع الأول: البيانات الشخصية العادية: تلك البيانات المتعلقة بالفرد، ولا يرى مانعا من إطلاع غيره عليها، ولا تشكل معرفتها تعديا على خصوصيته، مثل الأسم ورقم الهاتف وتاريخ[٩].

والثانى: البيانات الشخصية الحساسة: التى عرفها المشرع المصرى فى المادة (١) من الفصل الأول من قانون حماية البيانات الشخصية بأنها: "تلك البيانات التى تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية أو البيانات البيومترية[١٠] أو البيانات المالية أو الآراء السياسية أو الحالة الآمنية أو المعتقدات الدينية للشخص"، وحظر التعامل عليها إلا بترخيص من مركز حماية البيانات الشخصية، وبموافقة الشخص المعنى بالبيانات صراحة وبشكل كتابى.

فيما يرى البعض أن البيانات الحساسة: نوع من البيانات الشخصية ذات نطاق ضيق، ومرد حظر جمع تلك البيانات أو تداولها أو معالجتها هو ارتباطها المباشر والوثيق بحق الفرد فى حرمة الحياة الخاصة به، ذلك الحق الذى أقرته الدساتير الوطنية والمعاهدات والمواثيق الدولية[١١].

هذا وتعد البيانات الشخصية أحد أعمدة الإقتصاد فى العصر الحديث، فلا يمكن التنبؤ بسلوك الأفراد ومعرفة رغباتهم والتأثير عليهم إلا من خلالها، فشركات تحليل البيانات تقوم بعمل ملفات (سيكو جرافيك) لدراسة توجهات الشخص المعنى بالبيانات ومعرفة رغباته وتطلعاته، وإرسال رسائل موجهة له من أجل التأثير على

---

[٨] سامح عبدالواحد التهامى، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسى والقانون الكويتى، مجلة القانون الكويتية العالمية، ع ٩، س٣، مارس ٢٠١٥، ص ٤٠١.

[٩] محمد حماد مرهج الهيتى، البحث عن حماية جنائية للبيانات والمعلومات الشخصية (الأسمية) المخزنة فى الحاسب الآلى، مجلة كلية الشريعة والقانون، الإمارات، ع ٢٧، يوليو ٢٠١٦، ص ٤٠١.

[١٠] بيانات القياسات الحيوية (البيومترية): علم يستخدم الخصائص الفيزيائية أو البيولوجية للأشخاص لتحديد هويتهم، مثل بصمات الأصابع، فلا يوجد شخصان لهما نفس البصمات ولو كانا توأم.

https://www.interpol.int/How-we-work/Forensics/Fingerprints.

[١١] المادة (٩٢) من الدستور المصرى ٢٠١٤ ؛ المادة (١٢) من الإعلان العالمى لحقوق الإنسان، والمادة (١٧) من العهد الدولى الخاص بالحقوق المدنية والسياسية.

Ridha Hemici, Op.Cit, p. 56.

قناعاته، كما أن البيانات الشخصية هى حجز الأساس للدعاية والإعلان من خلال استخدام الشركات لتلك البيانات للترويج لمنتجاتها وخدماتها مثل: شركات الطيران والسياحة وشركات التأمين[١٢].

فعلى سبيل المثال: يرى بعض الفقه أن الإدلاء بالبيانات الشخصية يعد إجراء أولى ووجوبى، يتعين على كل من يرغب فى الإنضمام إلى مواقع التواصل الإجتماعى أن يدلى بها، كتدوين اسمه ولقبه وجنسه وتاريخ ميلاده وبريده الإلكترونى وغير ذلك من البيانات التى قد تتفاوت من موقع لآخر[١٣].

فنجد أن جميع مواقع التواصل الإجتماعى (Facebook– twitter–LinkedIn) تتطلب إدخال المستخدم لبعض بياناته الشخصية لإتمام عملية التسجيل، وعليه تحتفظ تلك المواقع بالبيانات الشخصية التى يلتزم المستخدم بإدخالها عند رغبته فى الإنضمام لأى منها، كما تحتفظ بالبيانات الخاصة بالإتصال بالإنترنت أى ما يعرف بالعنوان الإلكترونى (IP)، كما تصل إلى بيانات التصفح الخاصة بالمستخدم، وكذلك كافة التطبيقات التى يستخدمها وتكشف عن هوياته وميوله واهتماماته، وهو ما يمثل خطورة كبرى على خصوصية البيانات الخاصة بذلك المستخدم[١٤].

تجدر الإشارة أيضا فى هذا الصدد أن البيانات الشخصية للأفراد هي جزء لا يتجزأ من البيانات التي يتم بها تغذية تطبيقات الذكاء الاصطناعي بإختلاف أنواعها ومجالاتها، فالبيانات الشخصية المستند إليها فى المعالجة تعد وقودا لتلك التقنيات والتطبيقات، ومن ثم فإن اللجوء إلى جمع تلك البيانات ومعالجتها للتنبؤ بوقوع جريمة ما على سبيل المثال، قد ينطوى على مساس بالحماية المقررة فى قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠، فالبيانات الشخصية للأفراد هى محل تطبيقات الذكاء الإصطناعى[١٥].

وثم فقد اكتسبت العديد من مواقع الشبكات الاجتماعية أعمال الذكاء الاصطناعي، باستخدامها للذكاء الاصطناعي فى تحديد الخصائص الديموغرافية الجديدة، حيث تعتمد تقنيات الذكاء الاصطناعى على

---

[١٢] علاء عيد طه، الحماية القانونية للأشخاص الطبيعين فيما يتعلق بمعالجة البيانات الشخصية وتداولها، دراسة فى ضوء اللائحة التنظيمية رقم ٦٧٩/ ٢٠١٦الصادرة عن البرلمان والمجلس الأوروبى، مجلة كلية الحقوق للبحوث القانونية والإقتصادية، ع ٢، ٢٠١٩، ص ٢٤.

[١٣] محمد سامى عبد الصادق، شبكات التواصل الإجتماعى ومخاطر انتهاك الحق فى الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦، ص ٣٧ ومايليها.

[١٤] علاء الدين عبدالله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية فى نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، مج ٨، ع ٢، ٢٠١١، ص ٥ وما يليها.

[١٥] محمود سلامة عبدالمنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الإصطناعى ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعى، مج ٣، ٢٠٢١، ص ٣٥١.

الخوارزميات، التى تمكن من تجميع البيانات عن نشاط كافة المستخدمين المعروفين في شبكة اجتماعية معينة، وذلك لتقييم أو تحديد نشاط معين[١٦].

ومن خلال جمع تلك البيانات، تتم عملية التجهيز كمرحلة لازمة لإجراء عملية المعالجة، وتعرف تلك العملية وفقا للمادة (٤) من اللائحة الأوروبية بأنها: "عملية أو مجموعة من العمليات التى يقوم بها القائم بعملية المعالجة على مجموعة من البيانات الشخصية، بالقيام بالجمع والتنظيم والتسجيل والهيكلة والتخزين والتعديل والتكييف والإسترجاع، والكشف عن طريق النشر أو البث أو أى شكل آخر للإتاحة أو المحو أو التدمير"، هذا ولم يعرف المشرع المصرى فى مواده عملية التجهيز رغم أهميتها فى معالجة البيانات؛ ومن ثم يقوم المعالج[١٧] بعملية المعالجة.

فالقائم بعملية المعالجة هو الذى يحدد طريقة المعالجة، وتعرف عملية المعالجة وفقا للمادة (١) من الفصل الأول من قانون حماية البيانات الشخصية بأنها: " أى عملية إلكترونية أو تقنية، لكتابة البيانات الشخصية أو تجميعها أو تسجيلها أو حفظها أو تخزينها أو ....، وذلك باستخدام أى وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية، سواء تم ذلك جزئيا أو كليا"، بينما عرفتها اللائحة الأوروبية فى (٢/٤) منها بأنها: "عملية أو مجموعة من العمليات التى تجرى على البيانات الشخصية أو مجموعة منها، بأى وسيلة كانت تقليدية أو إلكترونية، مثل الجمع أو أو التسجيل أو التنظيم...".

ويلاحظ على ماتقدم أن المشرع المصرى اقتصر عملية معالجة البيانات الشخصية على المعالجة الإلكترونية فقط[١٨]، بينما المشرع الأوروبى أورد نوعين من عمليات المعالجة: المعالجة التقليدية إلى جانب المعالجة الإلكترونية، وإن كانت البيانات الشخصية التقليدية لا تختلف عن البيانات الشخصية الإلكترونية إلا فى أن الأخيرة لا تستخدم إلا عند التعامل مع الوسائط الإلكترونية، فكلتاهما تعبر عن البيانات الشخصية للإنسان، كالاسم واللقب والسن ورقم الهاتف وغيرها[١٩]، إلا أنه من الأحرى بالمشرع المصرى مسايرة المشرع الأوروبى

---

[١٦] عمار ياسر محمد زهير البابلى، توظيف تقنيات الذكاء الإصطناعى فى العمل الأمنى، دراسة تطبيقية، مجلة الأمن والقانون، مج ٢٨، ع ١، ٢٠٢٠، ص ٥٥.

[١٧] المعالج هو "ذلك الشخص الطبيعى أو الإعتبارى المختص بطبيعة عمله بمعالجة البيانات الشخصية، لصالحه أو لصالح المتحكم، بالإتفاق معه ووفقا لتعليماته"، التعريف الوارد بالمادة (١) من قانون حماية البيانات الشخصية ؛ ذات التعريف الوارد فى (٨/٤) من اللائحة الأوروبية .

[١٨] عرف المشرع المصرى المعالجة الإلكترونية فى المادة (١) من قانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨ بأنها: " أى عملية إلكترونية أو تقنية تتم كليا أو جزئيا، لكتابة أو تجميع أو ،.. إلخ، وذلك بإستخدام أى وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى، الإلكترونية أو المغناطيسية أو الضوئية، أو ما يستحدث من تقنيات أو وسائط أخرى".

[١٩] طارق جمعه السيد راشد، مرجع سابق، ص ١٩٢.

فى إدراجه للمعالجة التقليدية للبيانات إلى جانب الإلكترونية، إمعانا فى حماية أكبر للبيانات الشخصية للأفراد.

ونذكر فى هذا الصدد أن هناك عدة بيانات شخصية تخرج عن نطاق الحماية القانونية المنصوص عليها فى قانون حماية البيانات الشخصية، فقد نص القانون على عدم سريان أحكامه على البيانات الآتية[٢٠]:

- البيانات التى يحتفظ بها الشخص الطبيعى للغير، ويقوم بمعالجتها للاستخدام الشخصى.
- البيانات التى يتم معالجتها تطبيقا لنص قانونى أو بغرض الحصول على البيانات الإحصائية الرسمية.
- تلك المتعلقة بمحاضر الضبط القضائى، والتحقيقات والدعاوى القضائية.
- البيانات التى تتم معالجتها حصرا لأغراض إعلامية، يحيث تكون دقيقة وصحيحة، ولا يتم استخدامها لأى أغراض أخرى، ودون الإخلال بالتشريعات المنظمة للصحافة والإعلام.
- البيانات الشخصية لدى جهات الأمن القومى، وما تقدره لإعتبارات أخرى.

المطلب الثانى: المخاطر التى تهدد خصوصية البيانات الشخصية للأفراد

تتفاوت تلك المخاطر بحسب المراحل التى تمر بها البيانات الشخصية من تجميع ومعالجة وإتاحة عبر الإنترنت، وأى إجراء ينطوى على أى مساس بخصوصية البيانات الشخصية ويهدد حقوق وحريات الأفراد.

أولا: المخاطر المتعلقة بتجميع البيانات الشخصية

تعرف عملية التجميع بأنها: أى عمل من أعمال جمع وترتيب عناصر البيانات الشخصية لشخص ما، وإدراجها فى بطاقة معلومات ورقية كانت أو إلكترونية[٢١]، فعملية جمع البيانات أمر حتمى لاجراء عمليات المعالجة التى لاتخلو من مخاطر الإعتداء على خصوصية تلك البيانات المجمعة، فكثيرا ما تقوم الجهات الحكومية أو الهيئات الخاصة بتجميع بيانات مفصلة خاصة بالمتعاملين معها، وهو ما قد يؤدى لإساءة استخدام تلك البيانات المحفوظة، خاصة وأن تلك الجهات تقوم بربط الأجهزة المشتركة عبر شبكات عامة لتسهيل عملية تبادل البيانات الشخصية فيما بينها[٢٢].

---

[٢٠] المادة الثالثة من قانون حماية البيانات الشخصية.

[٢١] Cynthia chassigneux, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas , Paris II , ٢٠٠٣, nº ٢٧٨, p. ١٥٤.

[٢٢] محمود عبدالرحمن، التطورات الحديثة لمفهوم الحق فى الخصوصية –الحق فى الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، ع ٩، س ٣، مارس ٢٠١٥، ص ١٠٩

كما قد يتم تجميع البيانات الشخصية للأفراد بدون علمهم بفضل التقنيات التكنولوجية الحديثة المستخدمة عبر شبكة الإنترنت كرسائل الكوكيز[٢٣] التى تستخدمها الشركات التجارية فى أغراض الدعاية لخدماتها ومنتجاتها، ورغم فوائدها العديدة إلا أنها تعد من أنجح الوسائل المستخدمة لملاحقة خصوصية الأفراد وكشف بياناتهم الشخصية، وهو ما قد يساء استخدامه فى أغراض غير مشروعة، أما الوسيلة الأخطر من ذلك فهى أنظمة جمع المعلومات أو ما يعرف ببرمجيات التتبع والإلتقاط، فهى وسيلة تتبع تمكن مستخدمها من تجميع أكبر قدر ممكن من المعلومات السرية ومعالجتها بسرعة فائقة.

ومن جهة أخرى تقوم أغلب وسائل التواصل الإجتماعى بتجميع بيانات المستخدمين، وتقوم باستخدامها فى عمليات التسويق المباشر، فضلا عن تعرضها لعمليات القرصنة، وانتحال الأفراد بها لشخصيات أخرى مغايرة، وقيامهم بنشاطات غير مشروعة[٢٤]، وهو ما عبر عنه (جورج راى) المسئول عن الأمن المعلوماتى بشركة الأستثمارات الأمريكية (كوفمان– روسن/ كو) خلال منتدى الأمن المعلوماتى الذى نظمته غرفة التجارة فى بنما بقوله: "يتعرض يوميا نحو مليون ونصف مليون شخص لعمليات القرصنة المعلوماتية، التى يستهدف منها هؤلاء الحصول على معلومات شخصية أو الإضرار ببعض المؤسسات، حيث تم تسجيل نحو ٥٥٦ مليون هجوم معلوماتى خلال سنة واحدة على مواقع التواصل الإجتماعى والبريد الإلكترونى، واستطرد قائلا أنه: من السهل الحصول على معلومات شخصية من مواقع التواصل الإجتماعى، فضلا عن قيام الأفراد بانتحال الشخصيات والقيام بالأنشطة غير المشروعة"[٢٥].

ثانيا: المخاطر المتعلقة باستخدام ومعالجة البيانات الشخصية

تنطوى هذه المرحلة على مخاطر عديدة، منها:

- المخاطر المتعلقة باستخدام البيانات خلال عملية المعالجة ونتائجها: فهذه المرحلة اعتبرتها اللجنة الوطنية للمعلوماتية والحريات بفرنسا من البيانات الشخصية الحساسة، خصوصا مايتعلق منها بالهوس والفصام الذهنى، وبالتالى فإن معالجة البيانات الشخصية لأغراض البحث العلمى خصوصا تلك المتعلقة بالأبحاث الجينية أو للأغراض الإحصائية كإجراء البحوث على مجموعة من المراهقين

---

[٢٣] الكوكيز عبارة عن ملفات نصية تضعها معظم مواقع الويب عند زيارة موقعها، بغرض جمع معلومات عن المستخدمين، بحيث تمكن الموقع من الرجوع إليها عند الحاجه. للمزيد انظر الرابط التالى:
Joan E. Rigdon, Internet Users Say They'd Rather Not Share Their Cookies, Wall Street Journal, ١٤.Feb,١٩٩٦, p.٢٥.

[٢٤] محمد أحمد المعداوى، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع الواصل الإجتماعى، دراسة مقارنة، مجلة كلية الشريعة والقانون، جامعة طنطا، مج ٣٣، ع ٤، ديسمبر ٢٠١٨، ص ١٩٥٠ ومايليها.

[٢٥] محمود عبدالرحمن، مرجع سابق، ١٠٩–١١٠.

ذوى الأصول الإجرامية، قد تعرض الأفراد لإنتهاك خصوصيتهم والكشف عن حالتهم الصحية أو التنبؤ بسلوكهم الإجرامى، الأمر الذى من شأنه انتهاك حرمة الحياة الخاصة بهم.

- المخاطر المتعلقة بالهدف من عملية المعالجة: قد يتم استخدام تلك البيانات المستخدمة فى عملية المعالجة لتحقيق أهداف غير مشروعة، أضف إلى ذلك غموض الأهداف أو اتساعها أو تحديد أكثر من هدف من قبل المسئول، الأمر الذى يعطى مجالا كبيرا للإنتهاكات المتعددة لخصوصية تلك البيانات[٢٦].

وقد عبرت المحكمة الدستورية فى كارلسروه (ألمانيا الإتحادية) عن ذلك بقولها: "أن التقنيات الحديثة لجمع البيانات الشخصية واستخدامها والإحتفاظ بها، من المرجح أنها سوف تقوض الحق فى الحياة الخاصة بالأفراد، من خلال التخزين غير المحدود للبيانات، واستخدامها فى أى وقت، وفى غير الأغراض التى جمعت من أجلها؛ وبدون أى سيطرة عليها[٢٧]؛ فعملية جمع البيانات الشخصية الرقمية لأغراض المعالجة يجب أن تتم فى حدود الأهداف المحددة.

ثالثا: المخاطر الناجمة عن حوسبة البيانات الشخصية

حوسبة البيانات الشخصية: تعرف بتقنية تكنولوجيا التعلم، فغالبا ماتتميز تطبيقاتها بخاصية تكييف عملياتها مع البيانات التى تم الحصول عليها، ففى حالة المتجر متعدد الأقسام سيأخذ النظام فى الإعتبار المشتريات السابقة من أجل الدعايا لمنتجاتهم، وتعريفنا بالمنتجات الأخرى الأنسب لنا[٢٨].

فشيوع عملية النقل الرقمى للبيانات خلق مشكلات أمنية، إذ سهل عمليات التجسس الإلكترونى والقرصنة، وأصبحت شبكات الاتصال غير قادرة على توفير الأمان المطلق أو السرية الكاملة لما ينقل عبرها من بيانات[٢٩]

رابعا: المخاطر المتعلقة بتدفق البيانات عبر الإنترنت

---

[٢٦] سليم محمد سليم حسين، مرجع سابق، ص ٥١.

[٢٧] Cour constitutionnelle de Karlsruhe, ١٥ décembre ١٩٨٣. Pour un commentaire de cette décision, M. Fromont, République fédérale d'Allemagne, la jurisprudence constitutionnelle en ١٩٨٢ et ١٩٨٣, Revue du droit public et de la science politique, ١٩٨٤, pp. ١٥٦٢-١٥٦٨

[٢٨] Yves Poullet, La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et démocraties? , LEGICOM, n°٤٢ –٢٠٠٩/١, pp. ٤٧-٦٩.

[٢٩] منى تركى الموسوى، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الإقتصادية ، عدد خاص بمؤتمر الكلية، جامعة بغداد، ٢٠١٣، ص٣١٢.

صاحب تطور التكنولوجيا الرقمية تدفق البيانات الشخصية للأفراد عبر الحدود، فأتاحت لهم فرصة إعطاء بياناتهم ومعلوماتهم الشخصية لجهات داخلية أو خارجية، وهو ما يعرض تلك البيانات للعديد من الإنتهاكات؛ خصوصا فى الدول التى لاتتوافر فيها درجات عالية من مستويات الحماية، الأمر الذى دعا المشرع المصرى إلى حظر تداول البيانات الشخصية عبر الحدود[٣٠]؛ ولكن الأمر قد لا يكون فعالا فى ظل غياب التنسيق وضمان أن تكون عملية نقل البيانات فى إطار محكوم بإتفاقات دولية تكفل مستوى مماثل أو أعلى من الحماية[٣١].

وفى هذا الصدد قضت المحكمة العليا للإتحاد الأوروبى بتاريخ ٦ أكتوبر ٢٠١٥، ببطلان اتفاق الملاذ الآمن، ذلك الإتفاق الذى سمح للفيسبوك وبعض الشركات الأخرى مثل أمازون وجوجل بنقل بيانات المستخدمين بأعداد كبيرة وضخمة إلى أجهزتها فى الولايات المتحدة الأمريكية، وتبين فيما بعد أن أكثر من ٤ آلاف شركة، كانت قد استغلت هذا الإتفاق[٣٢].

خامسا: المخاطر المتعلقة باستخدام البيانات فى التسويق المباشر

أصبح للبيانات الشخصية قيمة مادية فى وقتنا المعاصر، ففيما يبدو أن البيانات المسجلة لدى العديد من الجهات مثل المصارف وشركات الهواتف المحمولة أصبحت تجارة رائجة تتداولها شركات التسويق فى السوق المصرى، ضاربة عرض الحائط بمبادئ حماية خصوصية البيانات التى تنص عليها القوانين ويحميها حق دستورى[٣٣].

المطلب الثالث: اشتراطات جمع ومعالجة وتخزين البيانات الشخصية فى العصر الرقمى

اشترط المشرع المصرى وكذلك الأوروبى لقيام عملية المعالجة ضرورة موافقة الشخص المعنى بالبيانات الشخصية بشكل صريح وواضح على قيام المعالج بجمع بياناته أو معالجتها أو الإفصاح عنها بأى وسيلة من الوسائل؛ وكذلك فى الأحوال المصرح بها قانونا[٣٤].

وشدد المشرع المصرى على ضرورة توافر عدة شروط يلزم توافرها للسماح بجمع البيانات الشخصية ومعالجتها، وذلك لتعدد صور الإنتهاكات التى تلحق بالبيانات الشخصية الخاصة للأفراد، تلك الإعتداءات

---

[٣٠] المادة (١٤) من الفصل السابع من قانون حماية البيانات الشخصية .

[٣١] سليم محمد سليم حسين، مرجع سابق، ص ٥٤.

[٣٢] ECLI, available at: http://curia.europa.eu/juris/document/document.jsf?docid=١٦٩١٩٥&doclang=EN.

[٣٣] محمود عبد العظيم، بيزنس البيانات الشخصية يغزو السوق المصرية، جريدة الإتحاد الإمارتية، بتاريخ ٨ يناير ٢٠٠٦، انظر: http://www.alittihad.ae/details.php?id=٤٤٥٩٢&y=٢٠٠٦.

[٣٤] المادة (٢) من الفصل الثانى من قانون حماية البيانات الشخصية؛ المادة (٧) من اللائحة الأوروبية.

التى تزيد يوما بعد يوم ليس فقط من الناحية الكمية بل ومن الناحية التقنية، خصوصا أنه يوجد صعوبة فى السيطرة على تلك الإعتداءات فى ظل التطورات التكنولوجية الرقمية، والقدرة الهائلة على تخزين كم هائل من البيانات الشخصية لمستخدمى الشبكات العنكبوتية ومواقع التواصل الإجتماعى.

حيث يلزم لجمع أو معالجة أو الإحتفاظ بالبيانات الشخصية توافر الشروط الآتية[٣٥]:

١- جمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة ومعروفة للشخص المعنى.

٢- أن تكون تلك البيانات صحيحة وسليمة ومؤمنة.

٣- يتم معالجة تلك البيانات بطريقة مشروعة وملائمة للغرض الذى جمعت من أجله.

٤- عدم الإحتفاظ بها لمدة أطول من المدة المحددة للوفاء بالغرض المحددة لها.

وتحدد اللائحة التنفيذية للقانون السياسات والإجراءات والضوابط والمعايير القياسية لعملية الجمع والمعالجة والتأمين لهذه البيانات، ورغم النص فى القانون على ضرورة قيام الوزير المعنى بشئون الإتصالات وتكنولوجيا المعلومات بإصدار اللائحة التنفيذية للقانون خلال ستة أشهر من تاريخ العمل بالقانون، إلا أنه لم يتم صدورها إلى الآن.

وهى ذات الشروط التى أوردها المشرع الأوروبى فى المادة (٥) من اللائحة الأوروبية، فقد حرص كلا من المشرعين على تحقيق المشروعية والإنصاف فى معالجة البيانات الشخصية، بإعتبار أن كافة هذه العمليات لا يجب أن تتم إلا بالموافقة الصريحة من قبل الشخص المعنى بالبيانات، ولأغراض مشروعة ومحددة ومعلنة لذلك الشخص، مع ضمان أمن وسلامة البيانات، وأن تكون تلك البيانات صحيحة وسليمة، وتعالج بطريقة مشروعة، فلايجوز استعمال الطرق الإحتيالية فى جمعها أو معالجتها، فيقوم الشخص بالإدلاء ببياناته بناء على هذه الوسائل الإحتيالية.

كما عدد المشرع المصرى عدة شروط أخرى يلزم توافرها عند القيام بعملية المعالجة، كى تكون قانونية ومشروعة، على الوجه الآتى[٣٦]:

١- أخذ موافقة الشخص المعنى بالبيانات على إجراء المعالجة.

٢- أن تتم عملية المعالجة تنفيذا لإلتزام تعاقدى أو تصرف قانونى، أو لإبرام عقد لصالح الشخص المعنى بالبيانات؛ أو لمباشرة أى من إجراءات المطالبة بالحقوق القانونية له أو للدفاع عنها.

٣- تنفيذا لإلتزام ينظمه القانون أو بناء على حكم قضائى أو أمر من جهات التحقيق المختصة.

---

[٣٥] المادة (٣) من الفصل الثانى من قانون حماية البيانات الشخصية.

[٣٦] المادة (٦) من قانون حماية البيانات الشخصية؛ المادة (٦) من اللائحة الأوروبية.

٤- تمكين المتحكم من تنفيذ التزامه أو أى شخص ذى صفة من ممارسة حقوقه المشروعة، مالم يتعارض ذلك مع حقوق وحريات الشخص المعنى بالبيانات.

وللتأكد من توافر تلك الشروط وإمعانا من الدولة المصرية فى حماية حقوق وحريات الأفراد، حرص المشرع المصرى على ضرورة إنشاء هيئة عامة إقتصادية يطلق عليها "مركز حماية البيانات الشخصية" تُمنح لها الشخصية الإعتبارية، وتتولى وضع وتطوير السياسات والخطط الإستراتيجية والبرامج اللازمة لحماية البيانات الشخصية والقيام على تنفيذها، وكذلك الرقابة والتفتيش على المخاطبين بأحكام هذا القانون، والخ[٣٧].

المبحث الثانى

الإطار القانونى لحماية البيانات الشخصية

تجدر الإشارة بداية إلى أن خصوصية البيانات الشخصية الرقمية المعنية بقانون حماية البيانات الشخصية تعنى: "حق الفرد فى سرية بياناته الشخصية خلال مراحل معالجتها إلكترونيا، وذلك من خلال ضبط عملية جمع البيانات وتخزينها ومعالجتها وتأمينها أثناء عمليات تداولها ونقلها"، ويهدف ذلك الحق إلى حماية سرية البيانات الشخصية، سواء كانت تتعلق بحياة الفرد الخاصة أو بمعاملاته أو بحساباته، وغيرها من البيانات المتاحة فى الفضاء الإلكترونى[٣٨].

المطلب الأول: حقوق الشخص المعنى بالبيانات الشخصية

حرص المشرع المصرى فى قانون حماية البيانات الشخصية على حماية خصوصية البيانات الشخصية الرقمية للأشخاص الطبيعيين[٣٩]، وألزم القائم بعملية المعالجة بضرورة منح العديد من الحقوق للشخص المعنى بالبيانات، وقد ذكر فى ذات القانون تعريفا للشخص المعنى بالبيانات وعرفه بأنه: "أى شخص طبيعى تنسب إليه بيانات شخصية معالجة إلكترونيا، تدل عليه قانونا أو فعلا؛ وتمكن من تمييزه عن غيره، وبذات المعنى عرفته اللائحة الأوروبية.

وأعطى له عدة حقوق، نذكرها على الوجه الآتى[٤٠]:

أولا: الحق فى الوصول للبيانات محل المعالجة والإطلاع عليها.

---

[٣٧] المادة (١٩) من الفصل التاسع من قانون حماية البيانات الشخصية.

[٣٨] عزت عبد المحسن إبراهيم، الحق فى الخصوصية الرقمية وتحديات عصر التقنية، مجلة العلوم القانونية والإقتصادية، كلية الحقوق، جامعة عين شمس، مج ٦٢، ع ١، ٢٠٢٠، ص ٨،٩.

[٣٩] محمد حماد مرهج الهيتى، مرجع سابق، ص ٤٠٠.

[٤٠] المادة (٢) من الفصل الثانى من قانون حماية البيانات الشخصية .

نص المشرع المصرى على ضرورة علم الشخص المعنى بالبيانات بوجود بياناته الشخصية لدى أى حائز أو متحكم أو معالج، كما نص على إمكانية الوصول إليها والإطلاع عليها، وكذلك الحصول على تلك البيانات إن أراد.

فيما تناولت (٦/٤) من اللائحة الأوروبية حق الشخص المعنى بالبيانات فى الوصول لبياناته الشخصية من خلال الوصول للمجموعات المنظمة التى أدرجها المشرع الأوروبى تحت ما يعرف "بنظام الإيداع"[٤١]، مثال ذلك: حق الأشخاص الخاضعة بياناتهم الشخصية للمعالجة فى الحصول على البيانات الخاصة بصحتهم، كالسجل الطبى الخاص بهم[٤٢].

ثانيا: الحق فى تعديل أو تصحيح أو محو البيانات الشخصية محل المعالجة.

ينبغى أن يكون للشخص المعنى بالبيانات الحق فى تعديل بياناته الشخصية محل المعالجة بالمحو أو الإضافة أو بالتصحيح أو بالتحديث لتلك البيانات، ويقع إلتزاما على عاتق القائم بعملية المعالجة بتبصير الشخص المعنى بالبيانات بالإجراءات التى يجب عليه إتباعها لإجراء التعديل أو المحو لبياناته الشخصية[٤٣].

وقد نص المشرع الأوروبى على حق الشخص المعنى فى تصحيح بياناته فى المادة (١٦) من اللائحة الأوروبية، كما يحق له استكمال بياناته الناقصة بأى طريقة، كما اعترف فى المادة (١٧) من ذات اللائحة على حق الشخص فى النسيان الرقمى، فلابد من الإعتراف بحقه فى النسيان الرقمى إذا كان الإحتفاظ بتلك البيانات يشكل إنتهاكا أو إخلالا بخصوصيته.

ثالثا: الحق فى الإعتراض على معالجة البيانات الشخصية أو نتائجها.

للشخص المعنى بالبيانات وفقا لقانون حماية البيانات الشخصية الحق فى الإعتراض على معالجة البيانات الشخصية أو نتائجها فى حالة واحدة فقط، أوردها المشرع على سبيل الحصر، وهى متى كانت عملية المعالجة تمس أو تتعارض مع الحقوق والحريات الأساسية للشخص المعنى.

---

[٤١] عرفت المادة (٤) الرابعة من اللائحة الأوروبية نظام الإيداع بأنه: أى مجموعة منظمة من البيانات الشخصية، يمكن الوصول إليها وفقا لمعايير محددة، مركزية كانت أو لا مركزية، موزعة على أساس جغرافى أو وظيفى.

[٤٢] علاء عيد طه، مرجع سابق، ص ٩٥.

[٤٣] المادة الخامسة من إلتزامات المعالج من قانون حماية البيانات الشخصية.

فيما عدد المشرع الأوروبى الحالات التى يحق فيها للشخص المعنى بالبيانات الإعتراض على عملية المعالجة كالآتى[٤٤]:

١- للشخص المعنى الحق فى الإعتراض فى أى وقت لأسباب تتعلق بوضعه الخاص، مالم يثبت المعالج أن هناك أسبابا مقنعة للمعالجة كالتسويق المباشر، والتحقق ما إذا كانت هذه الأسباب تتجاوز تلك الواردة فى طلب المعالجة من عدمه.

٢- عند معالجة البيانات الشخصية لأغراض البحث العلمى أو التاريخى أو لأغراض إحصائية وفقا للمادة (٨٩)، يحق للشخص المعنى الإعتراض لأسباب خاصة به، مالم تكن المعالجة ضرورية لإعتبارات تتعلق بالصالح العام.

٣- الحق فى إبداء الإعتراض على دقة البيانات الشخصية محل المعالجة.

٤- ابداء الإعتراض على عمليات المعالجة غير المشروعة التى تتم بالمخالفة للقانون.

رابعا: الحق فى إخطاره بأى خرق أو انتهاك لبياناته الشخصية.

تنص المادة (٧) من الفصل الثالث من القانون المصرى على ضرورة قيام المتحكم أو المعالج بإخطار الشخص المعنى بالبيانات بأى خرق أو إنتهاك لخصوصية بياناته خلال ثلاثة أيام عمل من تاريخ إبلاغهم بهذا الإنتهاك لمركز حماية البيانات الشخصية.

خامسا: الحق فى العدول عن الموافقة المسبقة على تخزين أو معالجة بياناته الشخصية.

يحق للشخص المعنى بالبيانات العدول عن الموافقة المسبقة التى أبداها عند البدء فى عملية جمع البيانات الشخصية ومعالجتها، ولكن يؤخذ على المشرع المصرى إشتراطه لمقابل مادى نظير الخدمة المقدمة إلى الشخص المعنى من المتحكم أو المعالج نظير ممارسته لحقوقه، فيما عدا الحق المتعلق بإخطاره بأى خرق أو انتهاك لخصوصية بياناته الشخصية، قام مركز حماية البيانات الشخصية بتحديده بما لايجاوز عشرين ألف جنية، وهى تكلفة مرتفعة وباهظة قد تعوق الشخص المعنى عن ممارسة حقوقه التى كفلها له القانون والدستور بصدد حماية بياناته الشخصية؛ لذا يجب على المركز عند تحديد أسعار الخدمات، مراعاة وضع رسوم تتناسب وطبيعة البيانات الشخصية محل الحماية.

المطلب الثانى: الإجراءات التى يلزم اتخاذها لحماية ووقف انتهاك خصوصية البيانات الشخصية

يلتزم مسئول حماية البيانات الشخصية وفقا للمادة (٩-١) من قانون حماية البيانات الشخصية بإجراء تقييم وفحص دورى لنظم حماية البيانات الشخصية لمنع إختراقها، وكذلك توثيق نتائج التقييم، وإصدار التوصيات

[٤٤] المادة (٢١) من اللائحة الأوروبية .

اللازمة لحمايتها، كما يلتزم أيضا بإبلاغ مركز حماية البيانات الشخصية بأى خرق أو انتهاك للبيانات الشخصية الموجودة لديه.

فيما يلتزم المتحكم فى عملية المعالجة وفقا للمادة (٤-٦) من ذات القانون بضرورة إتخاذ كافة الإجراءات التقنية والتنظيمية لحماية البيانات الشخصية وحفظ سريتها وتأمينها وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها فى أى إجراء غير مشروع.

أما عن المعالج فوفقا للمادة (٥-٧) يلتزم بحماية وتأمين عملية المعالجة، وتأمين الوسائط والأجهزة الإلكترونية وما عليها من بيانات شخصية؛ كما أعطى المشرع المصرى للشخص المعنى بالبيانات بعض الحقوق[٤٥] التى تمكنه من المطالبة بتصحيح أو تعديل أو محو البيانات الشخصية محل المعالجة، ومكنه من الإعتراض على المعالجة أو نتائجها، إذا ما تعارضت مع الحقوق والحريات الأساسية الخاصة به.

كما تجدر الإشارة إلى أن لكل هيئة أو منشأة طريقتها الخاصة فى توفير أمن البيانات، فأقل حماية ممكن أن يقوم بها الشخص هى عمل كلمة سر للحاسوب للولوج إلى النظام ذاته أو إلى الملفات الهامة به؛ فى حين أنه إذا كانت البيانات أكثر أهمية ومصنفه على أنها سرية، يجب حينئذ على المتحكم أو المعالج لحماية تلك البيانات الشخصية الهامة، أن يقوم بوضع برنامج أو أكثر لمقاومة الفيروسات الإلكترونية الضارة؛ وكذلك القيام بإضافة جدران نارية تحد من دخول الأشخاص من الخارج؛ وتمنع أى إعتداءات منظمة قد يتعرض لها الجهاز؛ كما يمكن أن يقوموا باستخدام تقنيات التشفير لحماية البيانات المتبادلة[٤٦].

فيما ألقت اللائحة الأوروبية إلتزاما على عاتق المواقع الإلكترونية بضرورة حماية بيانات المستخدمين متى وافق المستخدم على جمع المعالج لبياناته؛ حيث تنتقل الحماية للمعالج بحيث يمكنه استخدام أى وسيلة من شأنها حماية بيانات المستخدمين، كتشفيرها لحمايتها من الإختراق أو من حصول الغير عليها بالطرق غير المشروعة[٤٧].

ويعد التشفير من أهم وسائل تأمين البيانات الإلكترونية السرية؛ فبهذه الطريقة يتم الحفاظ على سلامة البيانات وعلى سريتها وعدم تعرضها للسرقة أو التزوير أو الإختراق[٤٨].

وما أن تتعرض البيانات الشخصية الرقمية[٤٩] لخرق أو انتهاك[٥٠] يلتزم كلا من المتحكم والمعالج وفقا للمادة (٧) بإبلاغ مركز حماية البيانات الشخصية خلال اثنين وسبعين ساعة من حدوث الواقعة؛ وإذا ما تعلق

---

[٤٥] المادة الثانية من ذات القانون.

[٤٦] منى تركى الموسوى؛ جان سيريل فضل الله، مرجع سابق، ص ٣٢٩.

[٤٧] إيمان أحمد على طه ريان، مرجع سابق، ٢٥٣.

[٤٨] شلواح ميرة، بشيرى كهينة، مرجع سابق، ص ٣٢.

الأمر بإعتبارات الأمن القومى يكون الإبلاغ فوريا لجهات الأمن القومى بالواقعة فورا ، كما يلتزم كلا منهم بموافاة المركز خلال اثنين وسبعين ساعة من تاريخ علمه بالخرق أو الإنتهاك بالبيانات الواردة بالمادة (٧) من القانون.

وفى جميع الأحوال يتم إخطار الشخص المعنى بالبيانات بذلك الخرق خلال ثلاثة أيام عمل من تاريخ الإبلاغ، وإخطاره كذلك بما تم إتخاذه من إجراءات؛ وفى هذا الصدد يؤخذ على المشرع المصرى عدم نصه على إلتزام المتحكم أو المعالج بإخطار الشخص المعنى بالبيانات بالشخص المسئول عن الخرق، وكذلك بيان هوية المتحكم أو المعالج أو المسئول الذى أخل بإلتزامه، كى يتمكن من إتخاذ الإجراءات القانونية حياله؛ كما يجب عليه إيضاح ما يجب على الشخص المعنى بالبيانات فعله من إجراءات عند علمه بحدوث واقعة الإنتهاك أو الإختراق، كونه الأولى بالحماية لتعلق تلك البيانات الشخصية به.

فيما نصت المادة (٣٣) من اللائحة الأوروبية على ضرورة إخطار السلطة المختصة فى حالة حدوث خرق للبيانات الشخصية، وبينت البيانات التى يلزم توافرها فى الإخطار الموجه: من بيان لطبيعة خرق البيانات الشخصية والفئات والعدد التقريبى للبيانات المخترقة، واسم وبيانات الاتصال بمسئول حماية البيانات، ووصف للعواقب المحتملة المترتبة على الخرق، والتدابير التى يقترح اتخاذها لمعالجة الخرق، وألزمت المتحكم بموجب المادة (٣٤) منها بضرورة إخطار الشخص المعنى فى أقرب وقت ممكن بخرق بياناته الشخصية، إذا كان هناك إحتمال أن يؤدى خرق البيانات الشخصية على مخاطر كبيرة على حقوق وحريات ذلك الشخص.

المطلب الثالث: التزامات القائم بعملية المعالجة

فرض المشرع المصرى على المعالج عدة التزامات ينبغى عليه أن يراعيها عند قيامه بعملية المعالجة، وشدد على أن تتم عملية المعالجة طبقا للقواعد المنظمة لهذا القانون ووفقا للائحته التنفيذية، كما ذكر أنه إذا ما تعدد القائمين على عملية المعالجة يلتزم كل منهم بالإلتزامات المنصوص عليها فى القانون فى حالة عدم وجود عقد يحدد بوضوح إلتزامات ومسئوليات كل منهم، وعلى ذلك نذكر الإلتزامات الملقاه على عاتق المعالج على الوجه الآتى[٥١]:

---

[٤٩] انظر: باسل فايز حمد القطاطشة، ممدوح حسن العدوان، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية، دراسة مقارنة، رسالة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان، ٢٠٢٢، ص ٢١.

[٥٠] عرفت المادة (١) من قانون حماية البيانات الشخصية خرق وانتهاك البيانات الشخصية بأنها:"كل دخول غير مرخص به إلى بيانات شخصية، أو وصول غير مشروع لها، ....، يهدف إلى الكشف أو الإفصاح عن البيانات الشخصية، أو إتلافها أو تعديلها، أثناء تخزينها أو نقلها أو معالجتها".

[٥١] نص المادة (٥) من الفصل الثالث (التزامات المتحكم والمعالج) من قانون حماية البيانات الشخصية.

أولا: أن تكون أغراض وممارسة المعالجة فى إطار مشروع: فالمشروعية هى أحد أهم الضمانات التى تتم فى إطارها معالجة البيانات الشخصية، فلايتم جمع البيانات الشخصية ومعالجتها إلا بطريقة مشروعة، ولأغراض مشروعة ومحددة، لصالح الشخص المعنى بالبيانات أو لصالح القائم بعملية المعالجة؛ بحيث لا تخالف النظام العام أو الآداب العامة[٥٢].

ثانيا: عدم تجاوز مدة المعالجة والغرض المحدد لها: يلتزم المعالج فى عملية المعالجة باستخدام البيانات لمدة محددة لا تتجاوز المدة المحددة لتحقيق أهداف عملية المعالجة، فهذه الضمانة تجسد حق هام من حقوق الفرد الرقمية تعرف" بالحق فى النسيان الرقمى"، ويلتزم المعالج أيضا بعدم الإحتفاظ بالبيانات الشخصية إلى أجل غير مسمى، بل يتم تحديد فترة الإحتفاظ وفقا للغرض من عملية جمع البيانات[٥٣]، ويقوم بإخطار كل ذى صفة (متحكم – الشخص المعنى..) بتلك المدة، وبإنقضائها يلتزم بمحو البيانات الشخصية أو بتسليمها للمتحكم.

ثالثا: حماية وتأمين عملية المعالجة: يلتزم المعالج بإتخاذ كافة الإجراءات التقنية والتنظيمية المناسبة لحماية البيانات الشخصية، وكذلك تأمين الأجهزة الإلكترونية والوسائط المستخدمة فيها، فيما حظر المشرع المصرى عمليات نقل أو تخزين أو مشاركة البيانات الشخصية إلى دولة أجنبية لا تضمن مستوى ملائم من الحماية، وحدد مستوى الحماية بأنه يجب ألا يقل عن المنصوص عليه فى قانون حماية البيانات الشخصية[٥٤].

رابعا: يلتزم المعالج بالقيام بعمل أو الإمتناع عن القيام بعمل: يكون من شأنه إتاحة البيانات الشخصية للأفراد، أو إتاحة نتائج معالجتها؛ ويستثنى من ذلك الأحوال المصرح بها قانونا.

خامسا: كما يلتزم أيضا بعدم إجراء أى معالجة تتعارض مع غرض المتحكم فيها أو نشاطه: واستثناء من ذلك يتم إجراء المعالجة لأغراض إحصائية أو تعليمية؛ ولكن بشرط عدم استهداف الربح؛ ودون الإخلال بحرمة الحياة الخاصة للمتحكم.

سادسا: كذلك يلتزم بإعداد سجل خاص بعمليات المعالجة: يبين فيه فئات المعالجة وبيانات المتحكم ووسائل الإتصال به وبيان مسئول حماية البيانات لديه؛ وقيود عملية المعالجة ونطاقها، وكذلك وصف الإجراءات التقنية والتنظيمية الخاصة بعمليات المعالجة وأمن البيانات.

سابعا: إثبات التزامه بأحكام القانون عند طالب المتحكم: وبتمكين مركز حماية البيانات الشخصية من الرقابة والتفتيش عليه.

---

[٥٢] Ridha Hemici, Op.Cit, p.٦١.

[٥٣] CNIL, Les durées de conservation des données, ٢٨ juillet ٢٠٢٠.

[٥٤] المادة (١٤) من الفصل السابع من ذات القانون.

المبحث الثالث

الإشكاليات القانونية التى تثيرها عملية المعالجة

تتعدد الإشكاليات القانونية التى تثيرها عملية معالجة البيانات الشخصية بتعدد المراحل التى تمر بها البيانات الشخصية.

المطلب الأول: أمن البيانات الشخصية

من أبرز الإشكاليات القانونية التى تثيرها عملية المعالجة هى أمن البيانات الشخصية، حيث تمر هذه العملية بعدة مراحل يجب أن تتوافر فيها الحماية، حتى لا يتم إفشاء سرية هذه البيانات، لكن الأمر يزاد تعقيدا يوما بعد يوما خصوصا فى ظل تزايد ظاهر قرصنة المعلومات، وهو ما يزيد من صعوبة مواجهة هذه التحديات فى ظل تطور تقنيات التكنولوجيا الرقمية.

وبالرجوع إلى قانون حماية البيانات الشخصية نجد المشرع المصرى ألقى إلتزاما على عاتق المتحكم والمعالج بإتخاذ جميع الإجراءات التقنية والتنظيمية لحماية البيانات الشخصية وتأمينها حفاظا على سريتها، وإمساك سجل خاص بالبيانات به وصف للإجراءات التنظيمية والتقنية المتعلقة بأمن البيانات[٥٥].

بينما عالجت اللائحة الأوروبية هذه الإشكالية فى ثلاثة مواد (٣٢-٣٣-٣٤)، فى محاولة لمواكبة التطور المتسارع فى تكنولوجيا المعلومات، وأولت إهتماما كبيرا بأمن وسرية البيانات، فنصت فى المادة (٣٢) على أنه: "يقوم المتحكم والمراقب والمتعاقد من الباطن من أجل حقوق وحريات الأشخاص الطبيعين بتنفيذ الإجراءات التقنية والتنظيمية المناسبة لضمان مستوى معين من الأمان المناسب لتلك المخاطر"، من بين هذه الأمور، مايلى:

- استخدام الأسماء المستعارة وتشفير البيانات الشخصية.
- وسائل ضمان السلامة والسرية والمرونة لأنظمة وخدمات المعالجة.
- وسائل إستعادة البيانات الشخصية والوصول إليها فى غضون فترة زمنية مناسبة فى حالة وقوع حادث مادى أو تقنى.
- إجراء اختبار لفاعلية التدابير التقنية والتنظيمية وتحليلها وتقييمها بإنتظام، لضمان أمن المعالجة.

وقد حرص المشرع الأوروبى فى (٢/٣٢) على سرية وسلامة البيانات الشخصية وأمن المعالجة عند تقييم المستوى المناسب للأمن، ونص على أنه يجب أن يؤخذ فى الإعتبار المخاطر التى تمثلها المعالجة والتى تنتج عن إتلاف أو فقدان أو تغيير أو الكشف غير المصرح به عن البيانات إلى شخص أو نقلها أو تخزينها أو معالجتها بأى طريقة أخرى، أو الوصول غير المصرح به إلى هذه البيانات عن طريق الخطأ او بطريقة

[٥٥] المادة (٤،٥) من الفصل الثالث من قانون حماية البيانات الشخصية.

غير مشروعة، هذا وتخضع عمليات التشفير والأسماء المستعارة وفقا (٣/٣٢) لما يسمى بمدونة السلوك التى تعد بمثابة عنصر إثبات للإمتثال للإلتزامات الملقاة على عاتق ذى الصفه (متحكم- معالج).

يتضح لنا مما تقدم أن المشرع الأوروبى سعى لإيجاد نظام متكامل لحماية أمن وسرية البيانات الشخصية من خلال تشريعه لبناء قانونى ملائم، وتوفيره للأدوات التقنية، وتنظيمة للإجراءات التنظيمية لضمان أمن البيانات.

المطلب الثانى: الحق فى النسيان الرقمى

يعد تطور تقنيات التكنولوجيا الرقمية مفيدا لحرية المعلومات لكنه يحمل تهديدات بانتهاك خصوصية البيانات، فالتسهيلات الخاصة بالحفظ والتخزين واستخدام البيانات المقدمة من محركات البحث، أدت إلى المطالبة بحق الفرد فى النسيان بحصوله على النسخة الأصلية للبيانات الخاصة به، والمطالبة بإزالتها من المحفوظات، وبين ذاك وتلك يجب تحقيق توازن دقيق بين الحقوق والمصالح التى تبدو متضاربة أى حماية البيانات الشخصية واحترام حرمة الحياة الخاصة وحق الفرد فى النسيان من جهة وحرية المعلومات والإبداع الفنى والأدبى والتاريخى من جهة أخرى[٥٦].

وعبر (Christian Charriere) عن ذلك الحق بقوله أنه: "تم استبدال الذاكرة المؤقتة للورق بذاكرة عالمية غير قابلة للتغيير ولا تترك أى فرصة للنسيان[٥٧]".

ويرى جانب من الفقه المصرى أنه: على الرغم من الإرتباط الوثيق بين كلا من الحق فى النسيان الرقمى والخصوصية، إلا أن ذلك لايعنى حتمية التلازم بينهم، فالحق فى النسيان يعد حق مستقل عن الحق فى الخصوصية[٥٨]، فقد يتم الإحتفاظ بالبيانات لإعتبارات المصلحة العامة ومن ثم يتم حماية تلك البيانات بموجب الحق فى النسيان لإمتداده لفترة أطول من المدة المحددة لأغراض المعالجة أى خرجت عن الحماية المقررة بموجب الحق فى الخصوصية، وهو مايعنى امكانية استقلالهما عن بعضهما.

الحالات التى يحق فيه للشخص المعنى بالبيانات استخدام الحق فى النسيان الرقمى:

[٥٦] Derieux Emmanuel, Vie privée et données personnelles- droit à la protection et droit à l'oubli, face à liberté d'expession, Nouveaux cahiers du conseil constituyionnel, N°٤٨ (Dossier: Vie Privée), Juin ٢٠١٥, p.٢١.

[٥٧] Christian Charriere Bournazel, Propos autour d'Internet : l'histoire et l'oubli, Gazette du Palais, ٢١ avril ٢٠١١, n°١١١, p.٦.

[٥٨] أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الإجتماعى، دار النهضة العربية، القاهرة، ٢٠١٣ ، ص ٦٦.

وفقا للمادة (٧) من اللائحة الأوروبية يتقرر الحق فى النسيان بإعطاء الشخص المعنى الحق فى محو البيانات الشخصية، وإلزام المتحكم بمحوها فى أقرب وقت ممكن، عند إنطباق أحد الأسباب الآتية:

١- لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التى تم جمعها من أجلها، أو تمت معالجتها بطريقة أخرى.

٢- سحب الشخص المعنى الموافقة المسبقة التى تمت المعالجة بموجبها، ولايوجد أساس قانونى آخر للمعالجة.

٣- لا توجد أسباب مشروعة للمعالجة، أو فى حالة معالجة البيانات الشخصية بشكل غير قانونى.

٤- يجب محو البيانات الشخصية للإمتثال لإلتزام قانونى منصوص عليه فى قانون الإتحاد أو بموجب قانون الدولة العضو الذى يخضع لها المتحكم.

٥- محو البيانات الشخصية كمتطلب للحصول على خدمات مجتمع المعلومات، إذا تم ذلك بشكل غير قانونى.

الإستثناءات الواردة على حق الشخص المعنى بالبيانات فى محو بياناته وفقا للائحة الأوروبية:

١- المعالجة ضرورية امتثالا لإلتزام قانونى يتطلب المعالجة فى مجال العمل والضمان الإجتماعى وقانون الحماية الإجتماعية أو لإتفاقية جماعية.

٢- لأسباب تتعلق بالمصالح الحيوية للمعنى بالبيانات أو لشخص طبيعى آخر، حيث يكون المعنى بالبيانات غير قادر على إبداء الموافقة.

٣- لإنشاء الدعاوى القانونية أو ممارستها أو الدفاع عنها أو عندما تتصرف المحاكم بصفتها القضائية.

٤- لأسباب تتعلق بالمصلحة العامة الجوهرية لقانون الاتحاد أو الدولة العضو.

٥- لأغراض الطب الوقائى أو المهنى أو لإدارة أنظمة وخدمات الرعاية الصحية والإجتماعية.

٦- تتم المعالجة فى إطار مشروع مع توافر ضمانات مناسبة من قبل مؤسسة أو هيئة غير هادفة للربح، وبشرط أن تتعلق المعالجة بالأعضاء فى الهيئة أو الأشخاص الذين على صلة منتظمة بها، وبشرط ألا يتم الكشف عن البيانات خارج الهيئة بدون موافقة الأشخاص المعنية بالبيانات

٧- لأسباب تتعلق بالمصلحة العامة فى مجال الصحة العامة مثل الحماية من الأمراض الخطيرة أو ضمان معايير عالية لجودة الرعاية الصحية والمنتجات الطبية، على أساس قانون الإتحاد أو الدول الأعضاء الذى ينص على تدابير مناسبة لحماية وحقوق وحريات الشخص المعنى لاسيما السرية المهنية.

٨- المعالجة لأغراض الأرشفة للمصلحة العامة، أو لأغراض البحث العلمى أو التاريخى أو للأغراض الإحصائية وفقا للمادة (١/٨٩).

فيما أعطى المشرع المصرى فى قانون حماية البيانات الشخصية للشخص المعنى الحق فى العدول عن الموافقة المسبقة على الإحتفاظ ببياناته أو معالجتها، وفى محو تلك البيانات إذا ما رأى أن استمرار وجود تلك البيانات سوف يضر بمصالحه أو يتسبب فى انتهاكا لخصوصيته، ويلتزم المتحكم أو المعالج وفقا لأحكام هذا القانون بمحو البيانات الشخصية الموجودة لديه فور إنقضاء الغرض المحدد منها، وإذا ما تم الإحتفاظ بها لفترة أطول من ذلك، فيجب أن يكون لأسباب مشروعة وبصورة لا تسمح بتحديد شخص المعنى بالبيانات الشخصية، كما يحدد المتحكم آليات المحو لديه فى السجل الذى يعده[٥٩].

المطلب الثالث: معالجة البيانات الشخصية الحساسة خصوصا تلك المتعلقة بالأطفال

تنص المادة (١٢) من الفصل السادس من قانون حماية البيانات الشخصية، على مثال البيانات المتعلقة بالأطفال كمثال للبيانات الحساسة التى يحظر التعامل عليها، واستلزم ضرورة أخذ موافقة ولى الأمر فيما يخص بيانات الأطفال، وألا تكون مشاركة الطفل فى لعبة أو مسابقة أو أى نشاط آخر مشروط بتقديم بيانات شخصية للطفل أزيد مما هو ضرورى للمشاركة.

فيما نصت اللائحة الأوروبية فى المادة (٨) على ضرورة موافقة ولى الأمر أو الولى أو الوصى على معالجة البيانات الشخصية للأطفال دون السادسة عشر من عمرهم، وأعطت اللائحة الأوروبية للدول الإعضاء فى الإتحاد الأوروبى الحق فى النص على سن أقل من المنصوص عليه فى المادة السابق ذكرها، بحث لايقل عمر الطفل عن ثلاثة عشر عاما[٦٠].

ونصت فى المادة (١٠) منها على حظر تجهيز البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية والبيانات الأمنية المتعلقة بالأفراد بإعتبارها من البيانات الحساسة إلا تحت رقابة السلطة المختصة أو فى الحالات التى يسمح بها قانون الإتحاد أو الدولة العضو، وبشرط توفير الضمانات المناسبة لحقوق وحريات الأشخاص المعنية.

المطلب الرابع: البيانات الشخصية للأفراد محل تطبيقات الذكاء الإصطناعى

[٥٩] المادة (٤،٥) من الفصل الثالث من قانون حماية البيانات الشخصية.

[٦٠] محمد سامى عبد الصادق، مرجع سابق، ص ٦٨.

البيانات الشخصية للأفراد هى الوقود لتطبيقات الذكاء الإصطناعى، حيث يتم تغذيتها بها، وفى هذا الصدد ذكرت المفوضية السامية لحقوق الإنسان فى تقرير لها كيف تعتمد أنظمة الذكاء الإصطناعى على كم هائل من البيانات، وتتضمن معلومات حول الأفراد، يتم جمعها وتحليلها ومعالجتها بشتى الطرق، إلا أن هذه البيانات المستخدمة قد تكون تمييزية أو قديمة أو معيبة، وقد يتولد عن تخزينها لمدة طويلة مخاطر معينة، كأن يتم استغلالها بطرق غير معروفة[٦١].

ويقر التقرير أيضا بأن: "التطورات التقنية تنطوى على مخاطر كبيرة، بالنسبة إلى الكرامة الإنسانية، والإستقلالية، والخصوصية، وممارسة حقوق الإنسان عموما، إذا لم تتم إدارتها بعناية فائقة"، كما أشار مجلس حقوق الإنسان كذلك إلى أن: الذكاء الإصطناعى يتطلب معالجة كميات كبيرة من البيانات، التى غالبا ما تتعلق بالبيانات الشخصية بما فى ذلك سلوك الفرد، وعلاقاته الإجتماعية، وتفضيلاته الخاصة، وهويته، ويمكن أن يشكل ذلك مخاطر جسيمة على الحق فى الخصوصية، خاصة إذا تم توظيفه فى تحديد الهوية أو التنميط أو التتبع أو التنبؤ السلوكى، أو التعرف على الوجه[٦٢].

وقد صدر قرار الجمعية العامة للأمم المتحدة رقم ١٦٧/٦٨، فى كانون الأول/ ديسمبر ٢٠١٣، بشأن الحق فى الخصوصية فى العصر الرقمى، حيث أكد هذا القرار على أن حقوق الأشخاص خارج الفضاء الإلكترونى يجب أن تحظى بذات الحماية داخله، كما ألزمت الدول المشاركة بضرورة احترام الحق فى الخصوصية فى الإتصالات الرقمية، وفى جمع المعطيات الشخصية، وحثت الدول على أن تعيد النظر في إجراءاتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها، والمتعلقة كذلك بجمع المعطيات الشخصية، وذلك بهدف تأكيد الحق في الخصوصية[٦٣].

وكما ذكرنا أن المشرع المصرى قد عنى بحماية البيانات الشخصية فى قانونه رقم ١٥١ لسنة ٢٠٢٠، ونص كذلك فى القانون الخاص بجرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨[٦٤]على العقوبات المتعلقة بجرائم الإعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع، وعليه فقد أصبحت كافة الخدمات الرقمية

---

[٦١]باشيليت، مخاطر الذكاءالإصطناعى التى تهدد الخصوصية تتطلب اعتماد إجراءات عاجلة، بتاريخ ١٥ سبتمبر ٢٠٢١، على الرابط الآتى:
https://www.ohchr.org/ar/press-releases/٢٠٢١/٠٩/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

[٦٢] عمرو وجدى، الذكاء الإصطناعى والحق فى الخصوصية، بتاريخ ٥ مارس ٢٠٢٣، على الرابط الآتى:
https://www.shorouknews.com/mobile/columns/view.aspx?cdate=٠٥٠٣٢٠٢٣&id=efb٩ca٣c-٧e٥a-٤٢٦٠-٨a٦٨-e٦af١٠٣f٧٠b١.

[٦٣]بوكر رشيدة، تحديات العصر الرقمى فى مواجهة خطط حماية الحق فى الخصوصية، مجلة حقوق الإنسان والحريات العامة، مج ٠٧، ع ٠٢، ٢٠٢٢، ٨١-٨٢.

[٦٤]الفصل الثالث من قانون جرائم تقنية المعلومات، المنشور فى الجريدة الرسمية، العدد ٣٢ مكرر (ج) فى ١٤ أغسطس ٢٠١٨.

والتكنولوجية تفرض على المستخدم ضرورة الموافقة على السماح أو الترخيص بجمع وتحليل بياناته الشخصية، بواسطة خوارزميات الذكاء الإصطناعى[٦٥].

إلا أن المشرع المصرى قد أورد بعض الإستثناءات على القانون الخاص بحماية البيانات الشخصية حيث استثنى البيانات الشخصية المتعلقة بمحاضر الضبط القضائى والتحقيقات والدعاوى القضائية، والبيانات الشخصية لدى جهات الأمن القومى، وما تقدره لإعتبارات أخرى، وغيرها من البيانات الواردة على سبيل الحصر فى قانونه، من نطاق الحماية القانونية المقررة بموجب ذلك القانون[٦٦].

والعلة من استثناء هذه الجهات من نطاق القانون ١٥١ لسنة ٢٠٢٠ تتجلى في حماية الأمن القومي الذي يضطلع بمهمة حفظ الأمن والإستقرار فى البلاد والتنبؤ بالجرائم ومنع وقوعها، وعليه فإن ذلك الإستثناء يعزز موقف الأجهزة الأمنية من جمع ومعالجة البيانات الشخصية الخاصة بالأفراد، واستخدامها فى تغذية تطبيقات الذكاء الإصطناعى، وبهذا الإستثناء يتضح لنا موقف القانون المصرى من استخدام البيانات الشخصية كوقود للذكاء الإصطناعى، فقد أصبحت هناك أرض خصبة لإستخدام تقنيات الذكاء الاصطناعي في حفظ الأمن، إلا أن تنامى استخدام تقنيات الذكاء الإصطناعى بدون ضوابط قانونية، قد ينطوى على مساس لحق الإنسان فى خصوصية بياناته الشخصية[٦٧].

ففى عام ٢٠١٨ تعرضت مصر وفق التقرير الصادر من شركة تريند مايكرو عام ٢٠٢١، للعديد من الهجمات والتهديدات الإلكترونية، ففى الربع الأخير من عام ٢٠١٧ زادت عدد البرمجيات الخبيثة بشكل كبير بنسبة وصلت ل ٢٥٪، بحيث تأتى مصر فى المرتبة الثالثة على مستوى القارة الأفريقية من حيث تعرضها للبرمجيات الخبيثة والهجمات الإلكترونية[٦٨] بهدف سرقة البيانات الخاصة بالمؤسسات والشركات بالقاهرة والعاصمة الإدارية الجديدة، وفى عام ٢٠٢٠ تعرضت المؤسسات الحكومية المصرية لنحو ٤٢ مليون هجمة إلكترونية، إلا أن المؤسسة الأمنية قد استطاعت التصدى لتلك التهديدات من خلال استخدام الخوارزميات الذكية فى منع التهديدات المحتملة[٦٩].

---

[٦٥] يحيى دهشان، المسئولية الجنائية عن جرائم الذكاء الإصطناعى، مجلة الشريعة والقانون، الإمارات، مج ٣٤، ع ٨٢، أبريل ٢٠٢٠، ص ١٤٤.

[٦٦] المادة الثالثة من قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠.

[٦٧] محمود سلامة عبدالمنعم الشريف، مرجع سابق، ص ٣٥٢.

[٦٨] رانيا سليمان أبو المعاطى محمود، ونهى محمد إبراهيم الدسوقى، وفاتن فايز حميدة الصفتى، سياسة مكافحة الإرهاب الإلكترونى، مصر والسعودية أنموذجا، المركز العربى للبحوث والدراسات، آفاق سياسية، ع ٥٣، ٢٠٢٠، ص ٥٢، ٥٣.

[٦٩] مجدى الداغر، اتجاهات النخبة نحو توظيف الإعلام الأمنى لتطبيقات الذكاء الإصطناعى فى مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى فى مصر، المجلة العربية لبحوث الإعلام والإتصال، ع ٣٣، أبريل/يونيو ٢٠٢١، ص ٨.

والجدير بالذكر أن القدرة على الوصول إلى بيانات الأفراد وجمعها وتخزينها، التى أحدثتها عصر المعلوماتية، تمثل تغييرا فى العلاقة بين الدولة والمواطنين، ومع تزايد انتشار استخدام تقنيات الذكاء الاصطناعي، ازدادت أهمية فرض ضمانات أخلاقية، وقد اتُّخذت عدة مبادرات طوعية، للتقليل من مخاطر انتهاك الحقوق الأساسية للإنسان، والتخفيف من غموض المسئولية القانونية بالإستخدام الأخلاقي للذكاء الاصطناعي، وضمان عدم إساءة استخدامها من قبل السلطة، من خلال الإشراف القضائي على الإستخدام، مع مراعاة مبادئ الشرعية والضرورة والتناسب، وقد قامت المفوضية الأوروبية لكفاءة العدالة التابعة لمجلس أوروبا "CEPEJ" بالإعلان عن الميثاق الأخلاقي الأوروبي بشأن استخدام الذكاء الاصطناعي في النظم القضائية، وقد نص الميثاق على عدة مبادئ للميثاق الأخلاقى وهي: مبدأ احترام الحقوق الأساسية للإنسان، مبدأ الجودة والأمان، مبدأ عدم التمييز، مبدأ الشفافية والنزاهة والحياد[٧٠].

وقد اقترحت فرنسا عدة ضمانات بموجب نص المادة (٢/٢٢) من اللائحة الأوروبية ٦٧٩/ ٢٠١٦، منها: الحق في معرفة آليات عمل الخوارزميات؛ حيث يحق للشخص المعنى بالبيانات الإطلاع على آلية عمل الخوارزميات التى تضطلع بمعالجة بياناته الشخصية.

الخاتمة

توصلت الدراسة إلى مجموعة من النتائج والتوصيات، نسرد أهمها كالآتى:

النتائج

- أحسن المشرع المصرى صنعا بتحديد أنماط البيانات الشخصية الخاضعة للحماية القانونية من خلال ذكره لأمثلة للبيانات الشخصية فى التعريف الوارد بقانون حماية البيانات الشخصية.
- قصر المشرع المصرى حماية البيانات الشخصية على الأشخاص الطبيعيين فقط دون الأشخاص الإعتبارية.
- اقتصر المشرع المصرى عملية معالجة البيانات الشخصية على المعالجة الإلكترونية فقط ، بينما أورد المشرع الأوروبى المعالجة التقليدية للبيانات إلى جانب المعالجة الإلكترونية.
- لم يعرف المشرع المصرى فى مواده عملية التجهيز رغم أهميتها فى معالجة البيانات.

[٧٠] http://julkaisut.valtioneuvosto.f/bitstream/hadle/١٠٠٢٤/١٦٠٣٩١/TEMrap_٤٧_٢٠١٧_verkkojulkaisu.pdf?sequence=١&isAllowed=y.

- اشترط المشرع المصرى والأوروبى لقيام عملية المعالجة ضرورة موافقة الشخص المعنى بالبيانات الشخصية بشكل صريح وواضح على قيام المعالج بجمع بياناته أو معالجتها.
- أعطى المشرع المصرى للشخص المعنى الحق فى الإعتراض على معالجة البيانات الشخصية أو نتائجها فى حالة واحدة فقط أوردها المشرع على سبيل الحصر، فيما عدد المشرع الأوروبى الحالات التى يحق فيها للشخص المعنى بالبيانات الإعتراض على عملية المعالجة.
- يؤخذ على المشرع المصرى عدم نصه على إلتزام المتحكم أو المعالج بإخطار الشخص المعنى بالبيانات بالشخص المسئول عن الخرق، وبيان هويته، كى يتمكن من إتخاذ الإجراءات القانونية حيالهم؛ كما يجب عليه إيضاح ما يجب على الشخص المعنى بالبيانات فعله من إجراءات عند علمه بحدوث واقعة الإنتهاك أو الإختراق.

التوصيات

- يجب على المشرع المصرى أن يولى اهتماما أكثر بالشخص المعنى بالبيانات، وضرورة إلزام المتحكم أو المعالج أو المسئول بإبلاغه بالشخص المسئول عن الخرق أو الإنتهاك، وبإيضاح الإجراءات التى يلزم عليه اتخاذها حال علمه بحدوث خرق أو انتهاك لبياناته الشخصية الرقمية.
- يجب على مركز حماية البيانات الشخصية عند تحديد أسعار الخدمات المقدمة من المتحكم أو المعالج نظير ممارسة الشخص المعنى بالبيانات لحقوقه، ضرورة وضع رسوم تمكنه من ممارسة حقوقه، وتتناسب مع طبيعة البيانات محل الحماية.
- تكثيف الجهود من أجل محو الأمية الرقمية، وتشكيل وعى مجتمعى حول شروط وسياسات الخصوصية، التى تعزز من خصوصية الأفراد عند إستخدمهم مواقع الإنترنت، خصوصا مواقع التواصل الإجتماعى.
- سن القوانين التى تحد من الإستخدامات السيئة للبيانات من قبل الشركات والمؤسسات، ووضع إلتزامات قانونية على عاتقهم تحظر الإستخدام غير المشروع للبيانات الشخصية للأفراد ووضع جزاءات فى حالة المخالفة.
- ضرورة اشتمال مفهوم المعالجة على المعالجة التقليدية إلى جانب المعالجة الإلكترونية، وشمول تلك البيانات الشخصية المعالجة تقليديا بالحماية، لإنطواء أغلب التعاملات اليومية على الإفصاح عن كثير من البيانات الشخصية غير المعالجة إلكترونيا والتى تطالها العديد من الإنتهاكات ولا توجد تشريعات أخرى تحميها.

- ضرورة الإسرع فى إصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠، نظرا لإحالة العديد من الإجراءات المتعلقة بتفعيل القانون إلى تلك اللائحة التنفيذية.
- ضرورة تفعيل قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠، والمضى قدما فى إنجاز الهيئة القائمة على تفعيله "مركز حماية البيانات الشخصية".
- تنظيم حق الإنسان فى محو بياناته (الحق فى النسيان الرقمى)، وخلق نوع من التوازن بين ذلك الحق والحق فى الأرشفة لأغراض المصلحة العامة.
- ضرورة وجود ضمانات كافية (أخلاقية– فنية– تنظيمية) لاستخدام البيانات الشخصية للأفراد من قبل الحكومات فى تقنيات الذكاء الإصطناعى، مع مراعاة خصوصية الأفراد، والإمتثال للقواعد المتعلقة بحقوق الإنسان وحق الفرد فى خصوصية بياناته الشخصية.
- يجب أن تتم عمليات تحليل البيانات بشكل آلى، مع ضرورة إتخاذ بعض التدابير الفنية لمنع سوء استخدام البيانات الشخصية للأفراد، مع إحكام الرقابة على عملية المعالجة، بحيث يكون استمرار الوصول إلى البيانات لأغراض محددة ومشروطة بالقدرة على استخلاص نتائج معينة من البيانات المحددة، مما يعنى تناسب إمكانية الوصول للبيانات وارتباطه مباشرة بتحقيق أهداف مشروعة.

المراجع

المراجع العربية:

- أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الإجتماعى، دار النهضة العربية، القاهرة، ٢٠١٣.
- باسل فايز حمد القطاطشة، ممدوح حسن العدوان، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية، دراسة مقارنة، رسالة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان، ٢٠٢٢.
- بوكر رشيدة، تحديات العصر الرقمى فى مواجهة خطط حماية الحق فى الخصوصية، مجلة حقوق الإنسان والحريات العامة، مج ٠٧، ع ٠٢، ٢٠٢٢.
- رانيا سليمان أبو المعاطى محمود، ونهى محمد إبراهيم الدسوقى، وفاتن فايز حميدة الصفتى، سياسة مكافحة الإرهاب الإلكترونى، مصر والسعودية أنموذجا، المركز العربى للبحوث والدراسات، آفاق سياسية، ع ٥٣، ٢٠٢٠.
- سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليا، دراسة مقارنة، مجلة العلوم القانونية والإقتصادية، كلية الحقوق جامعة عين شمس، مج ٦٢، ع ١، ٢٠٢٠.

- شلواح ميرة، بشيرى كهينة، المسؤولية المدنية عن انتهاك حق الخصوصية فى المجال الرقمى، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة-بجاية، ٢٠١٩-٢٠٢٠.
- طارق جمعه السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية فى العصر الرقمى، دراسة مقارنة، مجلة القانون والإقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع ٩٢، بدون سنة.
- عزت عبد المحسن إبراهيم، الحق فى الخصوصية الرقمية وتحديات عصر التقنية، مجلة العلوم القانونية والإقتصادية، كلية الحقوق، جامعة عين شمس، مج ٦٢، ع ١، ٢٠٢٠.
- علاء الدين عبدالله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية فى نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، مج ٨، ع ٢، ٢٠١١.
- علاء عيد طه، الحماية القانونية للأشخاص الطبيعين فيما يتعلق بمعالجة البيانات الشخصية وتداولها، دراسة فى ضوء اللائحة التنظيمية رقم ٢٠١٦/٦٧٩ الصادرة عن البرلمان والمجلس الأوروبى، مجلة كلية الحقوق للبحوث القانونية والإقتصادية، ع ٢، ٢٠١٩.
- عمار ياسر محمد زهير البابلى، توظيف تقنيات الذكاء الإصطناعى فى العمل الأمنى، دراسة تطبيقية، مجلة الأمن والقانون، مج ٢٨، ع ١، ٢٠٢٠.
- مجدى الداغر، اتجاهات النخبة نحو توظيف الإعلام الأمنى لتطبيقات الذكاء الإصطناعى فى مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى فى مصر، المجلة العربية لبحوث الإعلام والإتصال، ع ٣٣، أبريل/يونيو ٢٠٢١.
- محمد أحمد المعداوى، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع الواصل الإجتماعى، دراسة مقارنة، مجلة كلية الشريعة والقانون، جامعة طنطا، مج ٣٣، ع ٤، ديسمبر ٢٠١٨.
- محمد حماد مرهج الهيتى، البحث عن حماية جنائية للبيانات والمعلومات الشخصية (الأسمية) المخزنة فى الحاسب الآلى، مجلة كلية الشريعة والقانون، الإمارات، ع ٢٧، يوليو ٢٠١٦.
- محمد سامى عبد الصادق، شبكات التواصل الإجتماعى ومخاطر انتهاك الحق فى الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦.
- محمود سلامة عبدالمنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الإصطناعى ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعى، مج ٣، ٢٠٢١.
- محمود عبد العظيم، بيزنس البيانات الشخصية يغزو السوق المصرية، جريدة الإتحاد الإمارتية، بتاريخ ٨ يناير، ٢٠٠٦.

- محمود عبدالرحمن، التطورات الحديثة لمفهوم الحق فى الخصوصية –الحق فى الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، ع ٩، س ٣، مارس ٢٠١٥.
- منى تركى الموسوى، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الإقتصادية – عدد خاص بمؤتمر الكلية، جامعة بغداد، ٢٠١٣.
- يحيى دهشان، المسئولية الجنائية عن جرائم الذكاء الإصطناعى، مجلة الشريعة والقانون، الإمارات، مج٣٤، ع ٨٢، أبريل ٢٠٢٠.

المراجع الأجنبية

- Christian Charriere -Bournazel, Propos autour d′Internet : l′histoire et l′oubli, Gazette du Palais, ٢١ avril ٢٠١١, n°١١١.
- Cour constitutionnelle de Karlsruhe, ١٥ décembre ١٩٨٣. Pour un commentaire de cette décision, M. Fromont, République fédérale d'Allemagne, la jurisprudence constitutionnelle en ١٩٨٢ et ١٩٨٣, Revue du droit public et de la science politique, ١٩٨٤.
- Cynthia chassigneux, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas , Paris II , ٢٠٠٣.
- Derieux Emmanuel, Vie privée et données personnelles- droit à la protection et droit à l′oubli, face à liberté d′expession, Nouveaux cahiers du conseil constituyionnel, N°٤٨ (Dossier: Vie Privée), Juin ٢٠١٥.
- Joan E. Rigdon, Internet Users Say They'd Rather Not Share Their Cookies, Wall Street Journal, ١٤.Feb,١٩٩٦.
- Ridha Hemici, Legal warranties for personal data protection within the numerical space, Special edition- inpac ,University of Kasdi Merbah Ouargla, Algeria, November ٢٠١٩.
- Yves Poullet, La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et démocraties? , LEGICOM, n°٤٢ –٢٠٠٩/١.

المواقع الإلكترونية

- باشيليت، مخاطر الذكاءالإصطناعى التى تهدد الخصوصية تتطلب اعتماد إجراءات عاجلة، بتاريخ ١٥ سبتمبر ٢٠٢١، على الرابط الآتى:

https://www.ohchr.org/ar/press-releases/٢٠٢١/٠٩/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

- عمرو وجدى، الذكاء الإصطناعى والحق فى الخصوصية، بتاريخ ٥ مارس ٢٠٢٣، على الرابط الآتى:
https://www.shorouknews.com/mobile/columns/view.aspx?cdate=٠٥٠٣٢٠٢٣&id=efb٩ca٣c-٧e٥a-٤٢٦٠-٨a٦٨-e٦af١٠٣f٧٠b١.
- http://julkaisut.valtioneuvosto.f/bitstream/hadle/١٠٠٢٤/١٦٠٣٩١/TEMrap_٤٧_٢٠١٧_verkkojulkaisu.pdf?sequence=١&isAllowed=y.