الخطأ المدني الناشئ عن الإخلال بالحماية القانونية للبيانات الشخصية

" دراسة مقارنة "

دكتـــور

أحمـد علـي حسـن عثمـان

مدرس القانون المدني

كلية الحقوق – جامعة الزقازيق

مقدمة

تعد مسألة توفير الحماية القانونية اللازمة للبيانات الشخصية، من أهم الأمور التي تحتاج إلى البحث والدراسة فيما يخص هذه البيانات. ولن تتأتى الحماية القانونية المجدية لهذه البيانات، إلا بوضع إطار قانوني للمسؤولية المدنية في حالة صدور أي فعل يشكل تهديداً أو اختراقاً لهذه البيانات؛ وذلك لكي تكون هذه الحماية مجدية وعملية ومرضية للأفراد.

وما يستدعي ضرورة وضع نظام قانوني للمسؤولية المدنية في حالة حدوث اعتداء على البيانات الشخصية أياً كان نوع هذا الاعتداء، هو أن لهذه البيانات أهمية لا تُنكر لصاحبها أياً كان شأنه أو وضعه. فإن كان من الأفراد العاديين من أفراد المجتمع، فإن انتهاك هذه البيانات أو التعدي عليها يمثل اعتداءً صارخاً وحقيقياً على خصوصيته.

وإن كان من الأفراد المميزين، سواء بحكم منصبه أو طبيعة عمله أو مركزه المالي، فإن مسألة حماية البيانات الشخصية تبلغ من الأهمية ذروتها؛ حيث إن البيانات في هذه الحالة تكون محلاً للاستغلال المالي والمتاجرة بها، والدليل على ذلك أن هناك الكثيرين على استعداد تام لدفع الملايين في سبيل معرفتها، وهو ما يحدث بالفعل. لذلك كانت هذه البيانات جديرة بوضع نظام قانوني حمائي لها.

ولا شك أن البيانات الشخصية تعد أحد أبرز وأهم صور الحق في الخصوصية. فهي لا تقل أهمية عن حرمة المسكن، وسرية المحادثات

الشخصية، وحرمة الحياة العاطفية والزوجية والأسرية، وحرمة حالته الصحية، وحرمة مراسلاته وآرائه السياسية وذمته المالية ومعتقداته الدينية، وكذلك حرمة جسده، وحقه في الدخول في طي النسيان.

بل إن البيانات الشخصية تتميز بخصوصية تختلف عن تلك الثابتة لكافة صور الحق في الخصوصية، تتمثل في أن هذه الأخيرة نالت حقها من الدراسة بالقدر الملائم والكافي. أما بالنسبة لحماية البيانات الشخصية على وجه العموم والخطأ المدني في الإخلال بهذه الحماية على وجه الخصوص، فهو أمر حديث نسبياً، وبلغ من الأهمية بمكان في هذه الفترات وخصوصاً في ظل التطور التكنولوجي والانفتاح المعلوماتي الذي نعيشه، والذي يلقي بظلاله على هذه الحماية وذاك الخطأ.

وما يؤكد خصوصية البيانات الشخصية في هذا الصدد، هو أن تجميع هذه البيانات غالباً ما يتم عن طريق تعامل الشخص مع الجهات الحكومية وغير الحكومية. حيث إن هذا التعامل يفرض على الشخص أن يفصح عن بعض البيانات الخاصة به، والتي تمثل صوراً لما يندرج تحت مصطلح البيانات الشخصية.

ومما يحتم علينا ضرورة بيان حالات الخطأ المدني في هذا الخصوص، هو أن الجهات السابقة قد تسيء استعمال البيانات الشخصية لأغراض معينة، سواء كانت هذه الأغرض مشروعة أو غير مشروعة. فمن أمثلة الاستعمال المشروع لهذه البيانات، أن يتم تجميعها من قبل الجهات الإدارية والحكومية التابعة للدولة؛ لأن تجميعها يكون في الغالب متطلباً ضرورياً لتحقيق أمر مشروع كشغل الوظائف الحكومية مثلاً أو من أجل تزويد الفرد بالخدمات التي يريدها.

ولكن يلزم لكي تُضفى صفة المشروعية في هذه الحالة، ضرورة أن يقتصر تجميع هذه البيانات على تحقيق الهدف المشروع فقط وألا يتعداه، وإذا حدث مثل هذا التعدي أو التجاوز في الغرض من التجميع، فيمكن أن تُثار مشكلة الخطأ المدني في هذه الحالة.

وكثيراً ما يتم تجميع البيانات الشخصية من قبل جهات خاصة لتحقيق أهداف غير مشروعة، عن طريق اختراق هذه البيانات وتجميع أكبر قدر منها من أجل تقديمها إلى جهات معينة أو أفراد معينون بقصد المتاجرة بها. بل وأكثر من ذلك، أن هذا الأمر أصبح مهنة لفئة معينة؛ نظراً لما يدره من أموال طائلة، لا سيما في ظل الانفتاح المعلوماتي والشبكي الذي نعيشه. وهذا الأمر يوَجب علينا ضرورة وضع إطار قانوني لحالات الخطأ المدني في حالة حدوث مثل هذه الاختراقات والتي تحدث بصورة يومية لا محالة [١].

ومن صور الاستخدام أو التجميع غير المشروع للبيانات الشخصية والتي أصبحت ذات تكرار منتشر ومستمر في هذه الآونة، الحالة التي يقدم فيها الشخص على شراء سلعة من منشأة معينة ويقدم لهذه المنشأة معلومات معينة في إطار الحصول على هذه السلعة، فتقوم هذه المنشأة باستكمال هذه البيانات بتلك التي قد سبق وأن أدلى بها الشخص نفسه لمنشأة أخرى في سبيل الحصول على سلعة أخرى من هذه المنشأة الأخيرة، على نحو تكون محصلته في الأخير

[١] – فعلي سبيل المثال وعلى المستوى الشخصي، يتعرض حسابي الخاص بي على موقع فيس بوك لمحاولات الاختراق المتكرر. ناهيك عن أرقام الهواتف المحمولة الشخصية وبعض البيانات الشخصية الأخرى، التي أصبحت متناولاً يسيراً لشركات الدعاية والإعلان وشركات الإنتاج السلعي والخدمي.

تكوين رصيد كافٍ من البيانات الشخصية عن هذا الشخص بما يسمح بالمتاجرة بها [١].

وجدير بالذكر أن حماية حق الشخص بالنسبة لبياناته الشخصية، يتميز بالصورة النسبية، بمعنى أن نطاق هذه الحماية والخطأ المدني الذي يمثل إنتهاكاً لها، يختلف باختلاف المجتمعات والبيئات. فعلى سبيل المثال، لا يحظى هذا الحق بالاهتمام الكافي في أغلب مجتمعاتنا العربية، سواء من الناحية التشريعية أو الناحية العملية، ويُعامل بقدر من التهميش وخصوصاً في ظل ما أُطلق عليه ثورات الربيع العربي.

فقد فقد هذا الحق قدراً كبيراً من وجوده بالصورة الصحيحة والتي يتطلع إليها كل شخص، وأصبح انتهاك هذا الحق منتشراً دون مراعاة للضوابط القانونية التي تجيز الاطلاع على هذه البيانات في بعض الحالات ولاعتبارات معينة، وذلك في بعض الدول العربية التي وضعت تنظيماً تشريعياً لحماية هذه البيانات.

وعلى عكس ما تقدم، نجد أن حق الشخص في خصوصية بياناته الشخصية، يزداد احتراماً وتقديراً وفعالية في أغلب المجتمعات الغربية، والتي تتمتع فيها هذه البيانات بسياج كبير من الحماية القانونية على نحو لا يجوز فيه بأي حال من الأحوال الاطلاع على هذه البيانات إلا في أضيق الحدود وباتباع إجراءات صارمة وحازمة.

ويرجع هذا التباين والاختلاف في نطاق الحماية القانونية للبيانات الشخصية، لسببين أحدهما تشريعي والآخر عملي:

---

[١] – د/ سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – دراسة في القانون الفرنسي، بحث منشور في مجلة الحقوق الكويتية، العدد الثالث، سنة ٢٠١١، ص ٤٠٢.

١- التباين في الحماية القانونية من منظور السبب التشريعي:

وفي هذا السبب نجد أن أغلب تشريعات الدول الغربية أفردت قوانين خاصة ومستقلة لحماية البيانات الشخصية، سابقةً في ذلك التشريعات العربية، إمعاناً من هذه الدول بأهمية هذه البيانات وخطورتها لتعلقها الشديد بالجانب المعنوي لحياة الشخص وهو الحق في الخصوصية.

ومن أبرز هذه التشريعات، قانون حماية البيانات الشخصية الفرنسي رقم ١٧ لسنة ١٩٧٨ والذي تم تعديله بالقانون رقم ٨٠١ لسنة ٢٠٠٤. وقانون حماية البيانات الأمريكي لسنة ١٩٩٧. وقانون حماية البيانات البريطاني لسنة ١٩٩٨. وقانون حماية المعلومات الروسي لسنة ١٩٩٥. وقانون حماية البيانات الايطالي لسنة ١٩٩٦. وقانون حماية البيانات الألماني لسنة ٢٠٠٠ [١].

أما تشريعاتنا العربية، فنجد أن بعض هذه التشريعات بدأت تشعر بأهمية هذه البيانات وخطورتها وبادرت إلى إصدار قوانين لحماية هذه البيانات. ومن أبرزها، المشرع التونسي بالقانون رقم ٦٣ لسنة ٢٠٠٤، والمشرع الإماراتي بالقانون رقم ٢٦ لسنة ٢٠١٥ بشأن تنظيم نشر وتبادل البيانات في إمارة دبي، والمشرع القطري بالقانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية. وكذلك المشرع المغربي بقانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، وأيضاً المشرع العماني عندما وضع النصوص الخاصة بحماية البيانات الشخصية ضمن قانون المعاملات الإلكترونية الصادر سنة ٢٠٠٨.

---

[١]- وجدير بالذكر أن سرد هذه التشريعات إنما هو على سبيل المثال وليس الحصر. حيث توجد العديد من التشريعات أقرت مثل هذه الحماية القانونية بتشريعات مستقلة، كالمشرع السويدي، والمشرع الاسترالي، والمشرع الأسباني، وغيرها من التشريعات الغربية المختلفة.

وعلى الرغم من تأخر المشرع المصري رائد التشريعات العربية وسابقها قاطبة في شتى التشريعات والمجالات في سن قانون خاص لتنظيم حماية البيانات الشخصية، **إلا أنه تدارك هذا الأمر بإصدار القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية** [١]. وإن كان قد تدارك – أي المشرع المصري – هذا الأمر جزئياً بصدور القانون رقم ١٧٥ لسنة ٢٠١٨، بشأن مكافحة جرائم تقنية المعلومات، وذلك قبل أن يصدر التنظيم المتكامل لحماية هذه البيانات بالقانون رقم ١٥١ لسنة ٢٠٢٠ والمذكور آنفا.

٢– التباين في الحماية القانونية من منظور السبب العملي:

يتمثل هذا السبب في أن التطبيق العملي والمحكم لقوانين حماية البيانات الشخصية، يتم بـصورة أفضل في المجتمعات الغربية عنه في مجتمعاتنا العربية. ففي المجتمعات الغربية لا يجوز الاطلاع على البيانات الشخصية إلا للضرورة القصوى. ومن التطبيقات العملية الحديثة التي تؤكد ذلك، ما يلي:

أ– النزاع الذي حدث بين مكتب التحقيق الفيدرالي الأمريكي وشركة آبل: وتتلخص أحداث هذا النزاع في حدوث هجوم ارهابي في مدينة " سان برناردينو " في ولاية كاليفورنيا، والذي راح ضحيته أربعة عشر شخصاً، وتم العثور على هاتف ماركة " آيفون " كان يخص أحد منفذي هذا الهجوم؛ ونظراً لأن مكتب التحقيق الفيدرالي قد واجه مشكلة في فتح الهاتف، فقد حصل على قرار من المحكمة بإلزام الشركة بوضع برامج جديدة يكون الغرض منها تعطيل نظام التشفير الذي يحمي أجهزة الهواتف من الماركة المذكورة والتي تصنعها شركة

[١] – منشور بالجريدة الرسمية، العدد (٢٨) مكرر (هـ)، الصادر في ٢٤ ذي القعدة سنة ١٤٤١ هـ الموافق ١٥ يولية سنة ٢٠٢٠ م، السنة الثالثة والستون.

آبل، بما يسهل عملية الولوج إلى الهاتف المضبوط من أجل تسهيل مهمة اكتشاف من قام بهذا التفجير.

غير أن شركة آبل رفضت طلب مكتب التحقيق الفيدرالي، مبررة رفضها بأن حماية بيانات المستخدمين وخصوصيتهم هو ما جعلها تحظى بثقة مستخدمي أجهزتها، وأنه في حال قبولها طلب مكتب التحقيق الفيدرالي فإنها ستطيح بسمعتها إلى الأبد. وقال المدير التنفيذي لشركة آبل أن ما طلبته الحكومة الأمريكية شيء غير مسبوق ويهدد خصوصية المستخدمين في المدى البعيد الذي يتجاوز القضية المطروحة الآن وهو ما لا يمكن القيام به [١].

فعلى الرغم من تعلق الأمر في هذه الواقعة بالأمن القومي الأمريكي من ناحية، وصدور أمر من المحكمة الفيدرالية من ناحية أخرى بإلزام شركة آبل بتعطيل نظام التشفير للهاتف المذكور، على نحو يمكن القول معه بأنه توجد غاية مشروعة تجيز الاطلاع على البيانات الشخصية بالهاتف واختراق سريتها، إلا أن شركة آبل رفضت ذلك تقديراً منها لأهمية هذه البيانات وخصوصية عملائها.

بالإضافة إلى أنها لو فعلت عكس ذلك، لفقدت ثقة عملائها فيها، فضلاً عن ارتكابها لخطأٍ مدني يثير مسؤوليتها المدنية والتي غالباً ما تكبدها تعويضات بالغة في حالة ثبوت إخلالها بالحماية القانونية المطلوبة لبيانات العملاء الشخصية.

ب- واقعة اختراق البيانات الشخصية لمساعدة الرئيس الأمريكي " دونالد ترامب " في حملته الإنتخابية: وتتلخص أحداث هذه الواقعة، فيما صرح به

---

[١] – يُنظر في تفاصيل ذلك على الموقع الآتي:

- www. Al-Hayat. Com.

المدير التنفيذي لشركة " فيس بوك " من أن هذه الأخيرة قامت بدور مساعد في الحملة الإنتخابية للرئيس الأمريكي، عن طريق قيام هذه الشركة بتسريب البيانات الشخصية لنحو خمسين ألف مواطن أمريكي. الأمر الذي كبد شركة فيس بوك خسائر مالية قدرت ب ٦٠ مليون دولار في يومين فقط بسبب انخفاض القيمة السوقية لأسهم الشركة بنحو ١٠ %.

فضلاً عن ذلك، فإن إحدى المتخصصات في المجتمع الأمريكي، قالت بأن شركة فيس بوك، ستلتزم بتعويض كل مواطن تم اختراق حسابه بنحو ٤٠ ألف دولارٍ، أي بما يعادل تريليوني دولار لـ ٥٠ ألف مواطن الذين اُخترقت حساباتهم الشخصية.

وعلى الرغم من تعدد أركان المسؤولية المدنية التي يمكن أن تنشأ عن الإخلال بالحماية القانونية للبيانات الشخصية ما بين ركن الخطأ وركن الضرر وعلاقة السببية بينهما، إلا أننا فضلنا التعرض لركن الخطأ فقط ؛ لكونه الركن الذي يثير الكثير من الإشكاليات القانونية في هذا الصدد.

- مشكلة البحث:

لاشك أن التعامل في البيانات الشخصية يحدث بصورة مستمرة وشبه يومية أياً كان الغرض من هذا التعامل، على نحو أصبح فيه لدى الشركات والمنشآت التجارية الخاصة، رصيد كافٍ وكبير من البيانات الشخصية عن كثير من الأفراد، سواء عن اسمائهم أو عناوينهم أو هواياتهم أو ميولهم سواء كانت اقتصادية أو سياسية أو اجتماعية أو رياضية، وخصوصاً في ظل تعدد وسائل تجميع هذه البيانات بسبب هذا التعامل، كالتسويق المباشر، والتسويق الإلكتروني، والتسويق عن طريق استخدام أسلوب الكوكيز.

الأمر الذي بات يمثل تهديداً خطيراً لأصحاب هذه البيانات في الوقت الذي زادت فيه بصورة ملحوظة محاولات اختراق هذه البيانات والمساومات المالية عليها. أو استخدامها بطريق الاكراه المعنوي كوسيلة ضغط على أصحابها من أجل الرضوخ لطلبات مخترقي هذه البيانات.

وتتعـدد الـصـور التي تشكل إخلالاً بالحماية القانونية للبيانات الشخصية. فأحياناً يكون الخطأ المدني ناشئاً عن تخلف شروط معالجة هذه البيانات، أو تخلف إلتزام من الإلتزامات الملقاة على عاتق القائم بعملية المعالجة، أو تخلف الضمانات المقررة لأصحاب هذه البيانات في مواجهة القائمين بعملية المعالجة.

وأحياناً يكون منشأ الخطأ المدني الذي يعتبر وجوده إخلالاً بحماية البيانات الشخصية، هو اختراق هذه البيانات، سواء كان هذا الاختراق بسبب التعامل اليومي والمتكرر بين الأفراد بالصورة الآنف ذكرها، أو بسبب القرصنة المعلوماتية والاعتداء على هذه البيانات من قبل القراصنة المعلوماتيين الذين يمتهنون القيام بمثل هذه الاعتداءات.

وكثيراً ما يحدث الخطأ المدني بسبب سرقة البيانات الشخصية أو فقدها أو سرقة الجهاز الذي توجد عليه هذه البيانات أياً كان نوع هذا الجهاز، سواء كان جهاز كمبيوتر عادي أو لاب توب أو هاتف محمول أو أي أداة الكترونية أخرى تسجل عليها أي بيانات شخصية.

وتعد من أهم مشكلات البحث، أن جميع التشريعات التي تعرضت لفرض جزاءات قانونية حال انتهاك الضوابط المقررة لحماية البيانات الشخصية، تعرضت صراحة للجزاء الجنائي فقط ، أما الجزاء المدني فلم تتعرض له تلك القوانين تاركة أمره للقواعد العامة. ولعل ما يثير المشكلات القانونية في تحديد

الجزاء المدني، هو بيان الحالات التي تشكل خطأً مدنياً يستوجب تطبيق قواعد المسؤولية المدنية على المخالف أو المسؤول عن ذلك، وهو ما سنحاول بيانه في هذا البحث بمشيئة الله تعالى.

والخطأ المدني إما أن يكون عقدياً أو تقصيرياً. فالخطأ يكون عقدياً في حالة وجود رابطة عقدية بين المسؤول عن عملية معالجة البيانات الشخصية وبين صاحب هذه البيانات. ويكون الخطأ تقصيرياً في كل حالة تنتفي فيها هذه الرابطة العقدية، وذلك على النحو المعلوم في القواعد العامة بالنسبة لأنواع الخطأ.

وما يزيد مشكلة البحث تعقيداً وصعوبةً، هو ندرة الأحكام القضائية في القضاء المصري التي تعرضت لمسألة الحماية القانونية للبيانات الشخصية على وجه العموم – إن لم تكن منعدمة –، والتي تتمثل في أغلبها في حماية الحق في الخصوصية، وذلك على عكس الوضع في القضاء الفرنسي، والذي تعرض في أحكام كثيرة ومتنوعة لهذه الحماية، حتى قبل صدور قانون المعلوماتية والحريات الفرنسي عام ١٩٧٦م.

وذات الصعوبة – بالنسبة للوضع في مصر – على المستوى الفقهي والتشريعي، إلى أن صدر القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية، ومن قبله قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م، واللذان خففا من حدة هذا الأمر إلى حدٍ بعيد.

- أهمية البحث:

توجد لهذا البحث أكثر من أهمية. فهناك الأهمية القانونية، وكذلك الأهمية العملية. وذلك على التوضيح الآتي:

١- **الأهمية القانونية للبحث:** تتمثل هذه الأهمية في محاولة وضع الإطار القانوني لحالات الخطأ المدني الذي يتضمن إخلالاً بالحماية القانونية للبيانات الشخصية؛ نظراً لخطورتها وأهميتها البالغة، لاسيما بعد أن أصبح استخدام التقنيات الرقمية في عملية حفظ البيانات الشخصية ضرورة ملحة وواقعية، وذلك في صورة قواعد بيانات وربط هذه الأخيرة بشبكة الإنترنت، الأمر الذي ترتب عليه أن أصبحت هذه البيانات عرضة للاختراق أو السرقة أو الاطلاع عليها في غير الحالات المسموح فيها بهذا الاطلاع.

٢- **الأهمية العملية للبحث:** وتتمثل هذه الأهمية في محاولة التصدي لظاهرة خطيرة ذات انتشار واسع في هذه الفترات، ألا وهي الاعتداء على البيانات الشخصية، الأمر الذي يـمس بلا شـك حـق الشخص في الخصوصية. وما يؤكد ذلك أن الإحصائيات الحسابية تشير إلى إزدياد حالات الاختراق بشكل كبير، وخصوصاً مع التوسع والانفتاح التكنولوجي الذي سهل عملية الوصول إلى هذه البيانات، ومن ثم تسهيل عملية اختراقها.

فعلى الرغم من تعدد النظم الحمائية لهذه البيانات، إلا أنها لا تفي بالغرض المطلوب. لذلك فإن محاولة وضع إطار قانوني لحالات الخطأ المدني في هذا الصدد، سيساعد بلاشك على تقليل عمليات الاعتداء على البيانات الشخصية.

كما أن نجاح محاولة وضع إطار قانوني للخطأ المدني في الإخلال بالحماية القانونية للبيانات الشخصية، سيكون له بالغ الأثر على الأفراد من الناحية النفسية أو المعنوية؛ لأن من يحاول اختراق هذه البيانات أو الاعتداء عليها بأي صورة، سيخضع للمسؤولية المدنية والتي ربما تكبده تعويضات بالغة، الأمر الذي يمكن القول معه أن تقرير المسؤولية في هذا الصدد، يكون من ضمن السبل الفعالة والمجدية لحماية هذه البيانات من الناحية القانونية.

فمن يريد شراء سلعة معينة، سيفصح عن بياناته دون خوف أو قلق أو تردد، مما يترتب عليه زيادة القوة الشرائية للسلع التي تتطلب افصاحاً عن البيانات الشخصية، وخصوصاً أن الكثير من الأفراد يحجمون عن شراء سلع معينة خشية الإفصاح عن بياناتهم الشخصية وحفاظاً على سريتها.

- منهج البحث:

سنحاول التعرض لمسألة الخطأ المدني في الإخلال بالحماية القانونية للبيانات الشخصية من خلال اتباع المنهج التحليلي التأصيلي المقارن. وذلك بتحليل هذه المسألة وتأصيلها في كل من التشريع الفرنسي والمصري والأوربي. مع مقارنة حالات الخطأ المدني في هذا الصدد في القانون الفرنسي والقانون المصري والقانون الأوربي الخاص بحماية البيانات الشخصية، بقصد الوصول في الأخير إلى إطار قانوني محكم لحالات الخطأ المدني في هذا الصدد.

- خطة البحث:

ستكون خطة البحث بمشيئة الله تعالى، مقسمة إلى فصلين، يعقبهما خاتمة تتضمن نتائج البحث وتوصياته، على النحو التالي:

الفصل الأول: الخطأ المدني الناشيء عن تخلف ضوابط معالجة البيانات الشخصية.

الفصل الثاني: الخطأ المدني الناشيء عن مخالفة الضوابط الإجرائية والتأمينية لعملية معالجة البيانات الشخصية.

الفصل الأول

الخطأ المدني الناشيء عن تخلف ضوابط معالجة البيانات الشخصية

– تمهيد وتقسيم:

لقد وضع كل من المشرع الفرنسي والمشرع المصري وكذلك التشريعات التي نظمت موضوع حماية البيانات الشخصية تنظيماً مستقلاً، مجموعة من الضوابط القانونية اللازمة لصحة القيام بعملية معالجة البيانات الشخصية. كضرورة أن يتم تجميع البيانات بصورة مشروعة وواضحة، وأن تتم المعالجة بطريقة مشروعة ومتوافقة مع الهدف منها، وكذلك ضرورة دقة البيانات ذاتها للحفظ والمعالجة، وضرورة توافر رضا صاحب البيانات بالمعالجة، وكذلك وجوب مراعاة الضوابط الخاصة بمعالجة البيانات ذات الطابع الحساس. ويترتب على عدم مراعاة أي من الضوابط السابقة، نشوء خطأ مدني في حق القائم بعملية المعالجة، وهذا ما سنوضحه في هذا الفصل.

وترتيباً على ذلك، سنقسم الدراسة في هذا الفصل إلى ثلاثة مباحث هي:

المبحث الأول: الخطأ المدني الناشئ عن تجميع وحفظ البيانات الشخصية بصورة غير مشروعة.

المبحث الثاني: الخطأ المدني الناشئ عن عدم مشروعية معالجة البيانات الشخصية.

المبحث الثالث: الخطأ المدني الناشئ مخالفة ضوابط معالجة البيانات الشخصية ذات الطابع الخاص شخصياً وأمنياً.

المبحث الأول

الخطأ المدني الناشئ عن تجميع وحفظ البيانات الشخصية بصورة غير مشروعة

– تقسيم:

تعتبر مرحلة تجميع البيانات الشخصية، المرحلة الأولى ونقطة البدء في مجال الحديث عن وجود عملية معالجة للبيانات الشخصية من عدمه، ومن ثم مدى وجود خطأ مدني أم لا. أي أن ركن المحل في عملية المعالجة هو وجود بيانات ذات طبيعة شخصية يلزم معالجتها.

ويقصد بعملية تجميع البيانات الشخصية، كل عمل أو إجراء يكون الغرض منه جمع وترتيب بيانات أحد الأشخاص، ووضعها على بطاقة معلومات، أياً كانت طبيعة هذه البطاقة، إلكترونية كانت أم تقليدية [١].

وليس كل تجميع للبيانات الشخصية يعد تجميعاً غير مشروع. فهذا التجميع قد يكون مشروعاً ولا مجال للحديث عن أي خطأ مدني يمكن أن يُنسب إلى القائم بعملية التجميع، وذلك إذا أخبر هذا الأخير صاحب البيانات بعملية التجميع والغرض منه وأنواع البيانات محل التجميع[٢]. وهذا هو الضابط العام الذي يضفي على عملية التجميع وصف المشروعية.

---

[1] - CHASSI GNEUX (C.) : L'encaclrement juridique du traitment des données personnelles sur les sites de commerce en ligne , Thése , Université Panthéon Assas , 2003 , p. 154.

[٢] – د/ سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، القسم الأول، بحث منشور في مجلة الحقوق الكويتية، العدد الثالث، المجلد الخامس والثلاثون، سنة

وضرورة مشروعية تجميع البيانات الشخصية، **نص عليه المشرع المصري في القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية، وجاء ذلك في المادة (١/٣) التي نصت على أنه :**" يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية ..... ١- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني ".

أما التجميع غير المشروع للبيانات الشخصية، فهو الذي يتوافر في كل عملية تجميع لم يُخبر صاحب البيانات بها – أي بعملية التجميع – ، أو إذا أُخبر ولكن ظل القائم بعملية التجميع، يستعمل هذه البيانات أو يعالجها أو يخزنها بعد انتهاء الغرض من تجميعها، وذلك أياً كانت وسيلة التجميع.

وتتعدد صور التجميع غير المشروع للبيانات الشخصية، فقد يحدث عن طريق تقنية الكوكيز(Cookies) (مطلب أول)، أو عن طريق بيانات النقر (مطلب ثان)، أو عبر تقنية (R F I D) (مطلب ثالث)، أو عبر وسائل التواصل الاجتماعي (مطلب رابع)، أو عبر تقنية دمج المعلومات (مطلب خامس)، أو عبر تقنية فك تشفير الأنماط (مطلب سادس)، أو عن طريق ممارسات التسويق الخادعة (مطلب سابع). وذلك على التوضيح التالي:

٢٠١١، ص ٤١٤.

المطلب الأول

التجميع غير المشروع للبيانات الشخصية عبر تقنية الكوكيز (Cookies)

يُقصد بتقنية الكوكيز، ملفات تضعها مواقع الويب التجارية على القرص الصلب الخاص بمستخدم الإنترنت عند قيامه بزيارة أو تصفح هذه المواقع. وتكمن خطورة هذه المواقع في أنه يمكن عن طريقها تخزين كميات هائلة من المعلومات عن المستخدم، كالمواقع التي يفضل زيارتها، والمنتجات التي يُفضِّل شراؤها، واسمه وعنوانه ورقم هاتفه، ورقم بطاقة الإئتمان، وعنوان البريد الإلكتروني الخاص بالمستخدم، وأي بيانات أخرى يقوم المستخدم بإدراجها أثناء قيامة بزيارة هذه المواقع أو تصفحها[١] .

وتتكون تقنية الكوكيز من أربعة مكونات. يتمثل المكون الأول في سطر ترويسة للكوكيز في رسالة طلب، ويتمثل المكون الثاني في رسالة رد، أما المكون الثالث فهو ملف كوكيز مخزن على النظام الطرفي لمستخدم الإنترنت ويُدار بمتصفح المستخدم، والمكون الرابع يتمثل في قاعدة بيانات على موقع الويب [٢].

---

[1] - Fabrice NAFTALSKL , OEUVRE COLLECTIVE Sous LA DIRECTION DEPHILIPPE – HENRI DU THEIL , Fonctionnement de l'association , partie 4 , 2016 (actualization : Avril 2019) , N:3.
- L'utilisation de cookies constitue un traitement de données – conseil d'Etat 6 juin 2018 – Le bon 2018 , Recueil Lebon – Recueil des decisions du conseil d'Etat 2018 …… www. Dalloz . fr . com.

[٢] – د/ جيمس كيروز؛ د/ كيث روس، شبكات الحاسب والإنترنت " أسس ومبادئ الشبكات والإنترنت "، ترجمة : د/ السيد محمد الألفي؛ د/ رضوان السعيد عبد العال، دار العبيكان، سنة ٢٠١١، الطبعة الرابعة، ص ١٦٣..... هذا الكتاب متاح على الموقع التالي:
- https : // books . google . com . eg.

وتتمثل الخطورة من جمع البيانات الشخصية عبر تقنية الكوكيز، في أن لهذه التقنية أبعاد خطيرة وتأثيرات جلية على تجميع وأمن البيانات الشخصية لمستخدمي مواقع الإنترنت؛ حيث أصبحت معظم عمليات الشراء والبيع للكثير من السلع والمنتجات تتم عبر تقنية الكوكيز، الأمر الذي يستلزم إفصاح المستخدم عن الكثير من بياناته الشخصية.

وأحياناً تتطور عمليات تجميع البيانات الشخصية عبر تقنية الكوكيز، إلى الحد الذي تصبح فيه وسيلة لبناء قاعدة معلومات كاملة، ربما تكون سرية أو محددة التداول. ويستوي في هذا الشأن وسيلة التجميع عبر هذه التقنية، أي سواء باستخدام الاتصالات أو المكالمات الرقمية وأجهزة كمبيوترات الجيب المرتبطة عبر تقنيات الإئتمان عن بعد أو ما يُعرف بالأقمار الصناعية [١].

ويتسم تجميع البيانات الشخصية عبر تقنية الكوكيز بالصفة النسبية، بمعنى أن أنه لا يعد أمراً مشروعاً أو غير مشروع بصورة مطلقة. بل إن المشروعية تدور في إطار الضابط العام الآنف ذكره، وعدم المشروعية تدور في إطار مخالفة هذا الضابط . أي أن مشروعية تجميع البيانات عبر هذه التقنية تتوقف على الغرض من التجميع [٢].

---

[١] – د/ سامح عامر، التميز الإداري في القرن الحادي والعشرين، الناشر : دار المنهل، سنة ٢٠١٣، ص ١٦٠.

[2] - Céline CASTETS-RENARD , La protection des données personnellesdans les relations internes à l'Union européenne , Dalloz , Octobre 2018. N: 267.

المطلب الثاني

التجميع غير المشروع للبيانات الشخصية عن طريق بيانات النقر

يُقصد ببيانات النقر، المعلومات التي يعرفها الموقع عن المستخدم لمجرد قيام هذا الأخير بتصفح هذا الموقع. فبمجرد دخول المستخدم إلى الموقع، يُكشف عنوان يُعرف بالـ (I P/T C P) الخاص بالمستخدم ونوع الحاسب الذي استخدمه الشخص والمتصفح محل الاستخدام، وبعض المعلومات عن هذا التصفح كوقت حدوثه وتاريخه وعنوان الموقع السابق الذي كان يتصفحه الشخص قبل أن يتصفح الموقع الحالي [١].

وتكمن الخطورة من عمليات تجميع البيانات الشخصية عن طريق بيانات النقر، في أنه غالباً ما يتطلب الدخول إلى الموقع ضرورة إفصاح المستخدم عن بعض المعلومات ذات الطبيعة الشخصية على نحو يهدد خصوصيته.

وتعد هذه الوسيلة من الطرق الأكثر شيوعاً من الناحية العملية في تجميع البيانات الشخصية؛ لأن أغلب عمليات استخدام الأفراد لمواقع الإنترنت تتم عن طريق التصفح، ومن الممكن أن يتصفح الفرد في اليوم الواحد الكثير من مواقع الويب، وربما يدلي ببعض البيانات عنه في سبيل السماح له بالدخول إلى هذه المواقع. وتتنوع هذه البيانات على حسب الموقع الذي يتصفحه المستخدم والغرض من هذا التصفح، على نحو يعلن فيه الشخص عن كم هائل من بياناته الشخصية.

---

[١] – د/ وليد السيد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، سنة ٢٠١٢، ص ٢٢٤.

المطلب الثالث

التجميع غير المشروع للبيانات الشخصية عبر تقنية (R F I D)

تُعرف تقنية الـ (R F I D) باسم موجات الراديو، وتعتمد هذه التقنية على جهاز يُعرف بـ (R F I D Tags)، يتم وضعه بالمنتجات أو الحيوانات أو حتى الإنسان، ويحتوي هذا الجهاز على شريحة من السيليكون الهوائي، تتمثل وظـيفـته في إرسال واستقبال البيانات والاستعلام عبر موجات الراديو (R F I D) [١].

وتتمثل خطورة تجميع البيانات الشخصية عبر هذه التقنية، في أنها – أي تقنية R F I D– تقنيــة ذات انتشار واسع وممتد لكثير من المجالات والأماكن. حيث يمكن استخدامها في بطاقات تحديد الهوية لمعرفة أماكن تواجد أصحابها، وكذلك تحديد أماكن تواجد السيارات إذا كانت لوحة هذه السيارة تحمل شريحة السيليكون، ونفس الأمر بالنسبة لجوازات السفر والتأشيرات. وفي هذه الحالة الأخيرة تكون الشريحة مصدر كبير للإفصاح عن العديد من البيانات الشخصية أهمها صورة المسافر وجنسيته واسمه وبعض المعلومات عن حالته الاجتماعية[٢].

---

[1] - AVOINE (G.): Sécurité de la R F I D , Comprendre la technique sans être technician , in la secrete de l'individu numérise , réflexions prospectives et internationals , sous la direction de LACOUR (S.) , L'Harmattan , 2008 , p. 17 et s.

[٢] – للمزيد حول تقنية الـ (R F I D):

- Réglment caropéen (UE) 2018 / 608 de la commission du la avril établissant les critéres technique applicables aux etiquettes électronique pour les équipements marins (JOUE n° l Loi , 20 avril 2018).
- Mike Puglia , Albert Puglia , V.Daniel Hunt , R F I D , AGuide to Radio Frequency identification , John Wiley , Sans , 2007 , p. 1 – 5.

المطلب الرابع

التجميع غير المشروع للبيانات الشخصية عبر مواقع التواصل الاجتماعي

يُقصد بمواقع التواصل الاجتماعي، تلك المواقع التقنية التي تُنشأ وتُستخدم بقصد تبادل المحتوى الإعلامي والثقافي الذي يتميز بالطابع الشخصي بين طرفين أو أكثر، يُعبر عن أحدهما بالمرسِل والآخر بالمستقبل، وذلك عبر شبكة اجتماعية كفيس بوك أو واتس آب مثلاً، مع اعطاء المرسِل حرية الإرسال واعطاء المستقبل حرية التجاوب مع المعطيات المرسلة [١].

وتعتبر مواقع التواصل الاجتماعي ركيزة أساسية وفعالة إلى حد كبير في عمليات تجميع البيانات الشخصية. فالتحول التكنولوجي، ترتب عليه ذيوع وانتشار الإعلام الشخصي عن طريق هذه المواقع، وأصبح له دور فعال من الناحية العملية في حياة الأفراد أكثر من الإعلام الجماهيري. حيث أصبح عدد مستخدمي تلك المواقع كبير جدا في كل أنحاء المعمورة، وأصبحت تقنية لا غنى عنها بين الأفراد.

وتكمن الخطورة على البيانات الشخصية في هذا الصدد، في أن الاشتراك في أي موقع تواصل اجتماعي يتطلب الإفصاح عن العديد من البيانات الشخصية. وتحت حاجة الأفراد إلى استعمال هذه المواقع، فلا يجدون أي غضاضة في الإفصاح عن كل ما يُطلب منهم من بيانات والتي تمس بلا شك حقهم في الخصوصية. وهذا الأمر يترتب عليه، أن يكون لدى القائمين على تلك المواقع، بنوك من البيانات الشخصية عن المشتركين في هذه المواقع.

---

[١] – د/ أيمن أحمد الدلوع، المسئولية المدنية الناشئة عن الممارسات غير المشروعة عبر مواقع التواصل الاجتماعي، دار الجامعة الجديدة، سنة ٢٠١٨، ص ٢٥.

فعلى سبيل المثال، نجد أن الاشتراك في موقع الفيس بوك [١] يتطلب من الفرد الإفصاح عن اسمه الشخصي واسم أبيه وربما لقبه، وسنة الميلاد وشهره ويومه، ورقم الهاتف المحمول، بالإضافة إلى تحديد جنسه وما إذا كان ذكراً أم انثى. كما أنه من خلال استعمال هذا الموقع، نجد أن الشخص يعرض الكثير من الأمور عن حياته الاجتماعية والشخصية، كعلاقاته العاطفية سواء بالتلميح أو بالتصريح وعلاقاته العملية، وكل هذه أمور تتسم بالطابع الشخصي، والتي يعد تجميعها بتجاوز الغرض منها، تجميعاً غير مشروعٍ على نحو يثير مسؤولية القائم بالتجميع المدنية.

المطلب الخامس

التجميع غير المشروع للبيانات الشخصية عبر تقنية دمج المعلومات (Data Fusion)

تفترض تقنية دمج المعلومات، وجود مواقع غير مرتبطة ببعضها البعض، وفي الكثير من هذه المواقع قد يستخدم الأشخاص أسماء مستعارة ثم يفاجئون بوجود بعض بياناتهم الشخصية التي تم تجميعها، وذلك من خلال برامج تقوم بمسح قواعد البيانات المختلفة، والتي يكون لديها القدرة على معرفة المستخدمين المشتركين أو المرتبطين ببعضهم البعض [٢]. أي أنها عملية دمج مصادر بيانات

---

[١] – الفيس بوك، هو موقع إلكتروني للتواصل الاجتماعي، يتيح للأشخاص الطبيعيين والاعتباريين، أن يبرزوا أنفسهم وأن يعززوا مكانتهم عبر أدوات الموقع للتواصل مع أشخاص آخرين ضمن نطاق ذلك الموقع أو عبر التواصل على مواقع تواصل أخرى، وإنشاء روابط تواصل مع الآخرين ..... د/ أيمن أحمد الدلوع، المرجع السابق، ص ٤٠.

[٢] – د/ وليد السيد سويلم، المرجع السابق، ص ١٨٨.

متعددة لإنتاج معلومات أكثر اتساقاً ودقة عن المعلومات التي يوفرها أي مصدر بيانات فردي [١].

ويتم تجميع البيانات الشخصية عبر هذه التقنية باستخدام البرامج سالفة الذكر عن طريق قراءة معلومات عن شخص ما من قاعدة بيانات، وشخص آخر له اسم مختلف من قاعدة معلومات أخرى. بمعنى أنه يوجد شخصان مختلفان إلا أن النظام يعثر على معلومة جديدة من قاعدة معلومات أخرى، لكنها تحتوي على معلومات أخرى تشترك مع الشخص الأول، كرقم رخصة القيادة ورقم الهاتف، ويفترض النظام حينها أن هذه المعلومات مرتبطة بنفس الشخص [٢].

المطلب السادس

التجميع غير المشروع للبيانات الشخصية عبر تقنية فك تشفير الأنماط

تقوم تقنية فك تشفير الأنماط على أساس تخزين المعلومات والبيانات الشخصية على قواعد بيانات الحاسب ومعالجتها بطريقة تجعلها تتخطي الحدود المكانية والزمانية لمكان وجود هذه البيانات أو مكان تخزينها أو معالجتها. فبمجرد تخزين هذه البيانات في أي قاعدة بيانات، فإنها تكون قابلة لأن يتم تجميعها وإعادة ماضي الإنسان إلى ذاكرة الوجود، أي أنها تقنية تحول دون الشخص ودخوله في طي النسيان بالنسبة لبعض بياناته أو بعض الوقائع

[1] - https : // en. m.wikipedia.org/ Wikipedia/ Data – Fusion.

[٢] – د/ وليد السيد سويلم، المرجع السابق، ص ١٨٨، ١٨٩.

التي قام بها لأي سبب من الأسباب، لا سيما في ظل التحول من السجلات الورقية إلى السجلات الإلكترونية [١].

وتتمثل الخطورة على البيانات الشخصية من خلال تقنية فك تشفير الأنماط ، في أنه باستخدام قواعد البيانات يمكن انشاء ملفات تعريف للهوية الشخصية، ويكون البحث فيها على درجة من السرعة والشمولية لأكبر قدر من البيانات الشخصية عن الشخص بقاعدة البيانات محل البحث. فبمجرد تسجيل البيانات الشخصية على قواعد البيانات، فإنها تحقق درجة عالية من المصداقية على نحو يسهل التعرف عليه سواء بطريق مباشر أو غير مباشر.

وتزداد المشكلة صعوبة وخطورة في حالة بيع هذه القواعد، سواء تم البيع بعلم أو بدون علم الشخص المعني بالبيانات، مما يترتب عليه سهولة سرعة ونقل وانتشار هذه البيانات عبر نطاق جغرافي كبير وفي فترة زمنية قصيرة وبإجراءات تقنية بسيطة وسريعة [٢].

المطلب السابع

التجميع غير المشروع للبيانات الشخصية عن طريق ممارسات التسويق الخادعة

يُقصد بالتسويق الخادع، الممارسات التجارية المضللة التي تتضمن معلومات كاذبة وغير صادقة بأي طريقة، إذا كان تقديمها يحتوي على تحريض

[١] – د/ وليد السيد سليم، المرجع السابق، ص ٢١٦، ٢١٧.

[٢] – د/ وليد السيد سليم، المرجع السابق، ص ٢١٨.

أو احتمالية تضليل المستهلك، حتى ولو كانت المعلومات المقدمة صحيحة من الناحية الواقعية [١].

ويعــد التسويق خادعاً إذا كان الكذب منصباً على أيٍ من البيانات الآتية: وجود المنتج أو طبيعته أو خصائصه الرئيسية، أو التزامات المورد وطبيعة عمله، والسعر وطريقة حسابه وطريقة دفعه، ومدى وجود قطع غيار للمنتج وامكانية استبداله أو اصلاحه، وطبيعة وخصائص وحقوق التاجر أو من ينوب عنه.

وتتمثل خطورة ممارسات التسويق الخادعة على تجميع البيانات الشخصية، في أن بعض الجهات قد تستخدم هذه الممارسات كوسيلة ضغط من أجل تجميع هذه البيانات من فئة معينة من الأشخاص، فيضطر هؤلاء الأخيرون تحت تأثير احتياجهم للسلعة أو المنتج المعلن عنه بصورة خادعة، إلى الإفصاح عن بعض بياناتهم الشخصية، الأمر الذي يشكل تجميعاً غير مشروع لهذه البيانات على نحو يعد فيه القائم بالتجميع مرتكباً لخطأٍ مدني يستوجب مساءلته مدنياً.

ونظراً لخطورة تجميع البيانات الشخصية عن طريق الممارسات التسويقية الخادعة، **فقد وضع المشرع المصري في القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية**، الضوابط القانونية لممارسة التسويق الإلكتروني المباشر [٢] بصورة تحقق التوازن بين رغبة الفرد واحتياجه للسلع

---

[1]- Céline CASTETS – RENARD , commerce électronique , Dalloz , Juillet 2016 (actualization : octobre 2018) . N: 20.

– د/ عبد العزيز بن محمد العبيد، المسئولية الجنائية في الإعلانات التجارية، دراسة تأصيلية مقارنة، الناشر : دار المنهل، سنة ٢٠١٦، ص ١٧٥.

[٢] – عرف المشرع المصري التسويق الإلكتروني في المادة (١) من القانون رقم ١٥١ لسنة

والخدمات التي تتطلب إفصاحاً عن بعض أو كل البيانات الشخصية وبين الحفاظ على سرية وخصوصية هذه البيانات بالنسبة لصاحبها. وجاء هذا التوازن في المادتين (١٧، ١٨) من القانون المذكور.

فالمادة (١٧) من هذا القانون، نصت على أنه:" يُحظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات، إلا بتوافر الشروط الآتية..... ١- الحصول على موافقة من الشخص المعني بالبيانات. ٢- أن يتضمن الاتصال هوية منشئه ومرسله. ٣- أن يكون للمرسل عنوان صحيح وكافٍ للوصول إليه. ٤- الإشارة بأن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر. ٥- وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها ".

كما نصت المادة (١٨) من ذات القانون على أنه:" يلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر بالالتزامات الآتية..... ١- الغرض التسويقي المحدد. ٢- عدم الإفصاح عن بيانات الاتصال للشخص المعني بالبيانات. ٣- الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها، أو عدم اعتراضه على استمراره بشأن تلقي الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال " [١].

٢٠٢٠ الخاص بحماية الشخصية، بأنه:" إرسال أي رسالة أو بيان أو محتوى إعلاني أو تسويقي بأي وسيلة تقنية أياً كانت طبيعتها أو صورتها، تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى أشخاص بعينهم ".

[١] – وفيما يتعلق بالقواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر، فتحدده اللائحة التنفيذية للقانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات

وبعد التعرض لأغلب حالات تجميع البيانات الشخصية على النحو الآنف ذكره، فإن تجميع البيانات في كل هذه الحالات يعتبر أمر مشروع إذا ما أُخبر صاحب البيانات بعملية التجميع أو إذا لم يحدث تجاوز للغرض من تجميع هذه البيانات. ويعد التجميع غير مشروع إذا لم يُخبر صاحب الشأن بعملية التجميع ، أو إذا حدث تجاوز للغرض من التجميع. وإذا حدث الفرض الأخير، فإن ذلك يعتبر خطأً مدنياً يستوجب مساءلة القائم بالتجميع المدنية، يستوي في ذلك وسيلة التجميع كما سلف الذكر.

وتطبيقاً لما تقدم، فإن قيام إحدى الشركات بإرسال رسائل عبر البريد الإلكتروني للأفراد الذين حصلت على عناوين بريدهم الإلكتروني من خلال شبكة الإنترنت عن طريق البرامج التي سجلت البيانات الشخصية الخاصة بأصحاب البريد من ملف استخدام لاحق، وكذلك من خلال استخدام برنامج آخر يوجه الرسائل الإعلانية إلى العناوين التي تم تجميعها دون أن تكون محفوظة في ملف، يعتبر تجميعاً غير مشروعٍ لهذه البيانات؛ لعدم توافر موافقة أصحاب هذه البيانات بعملية التجميع، كما أنهم لم يُخبروا بها [1].

كما يعد تجميعاً غير مشروع للبيانات الشخصية، قيام النادي الرياضي بتجميع عناوين البريد الإلكتروني لأعضائه – والتي كان الغرض من تجميعها إرسال المعلومات إليهم حول حياة النادي – وإرسال إعلانات الشركاء التجاريين إليهم؛ وذلك بسبب عدم توافر الموافقة المسبقة من هؤلاء الأعضاء. كما يجب

الشخصية..... المادة (١٨) من هذا القانون.

[1] - Fréderique CHOPIN , Cybercriminalité , Juillet 2013 (actualization : Avril 2018) , Dalloz , N: 56.

ألا يحدث تجاوز للغرض من التجميع، فلا يجوز استخدام الضمان الاجتماعي لموظفي النادي إلا لتنفيذ عمليات كشوف المرتبات [١].

وتطبيقاً لذلك قضت محكمة النقض الفرنسية، بأن تجميع عناوين البريد الإلكتروني للأشخاص واستخدامها في غير الغرض الذي جُمعت من أجله هذه العناوين، يعتبر تجميعاً غير مشروعاً ويعاقب عليه القانون[٢].

وينشأ الخطأ المدني أيضاً في حق القائم بعملية حفظ البيانات الشخصية، إذا ما تخلفت شروط وضوابط هذا الحفظ . فهذا الخطأ ينشأ في الفرض الذي تُحفظ فيه البيانات على نحو لا تحدد فيه هوية صاحب هذه البيانات، فلا يجوز الحفظ العشوائي. وتكمن العلة في منع الحفظ العشوائي، في تخويل صاحب هذه البيانات مكنة ممارسة سلطاته على بياناته، كالحق في الاطلاع عليها، والحق في تعديلها أو تصحيحها، والحق في طلب الدخول في طي النسيان [٣].

وينشأ الخطأ المدني أيضاً، إذا قام الشخص أو الجهة المنوط بها حفظ البيانات الشخصية أو معالجتها، بحفظ هذه البيانات بعد المدة اللازمة لهذا الحفظ . فمن المعلوم أن حفظ البيانات الشخصية يجب أن يكون لمدة محددة وهي المدة اللازمة لتحقيق الهدف من جمع هذه البيانات [٤].

أي أن حفظ البيانات الشخصية يكون مكوناً لخطأٍ مدني، إذا ما تم الاحتفاظ بها بعد انتهاء الغرض من تجميعها، على قاعدة بيانات نشطة يمكن

---

[1] - Tiphaine Bessiére , Le collecte de données personnelles : Un cadre précis ā respecter , Jurisport 2011 , n° 111 , p. 22.

[2] -Cass Crim , 14 mars 2006 , n° 05 – 83 . 423 . Dalloz , 2007 . Pan . 404 , obs . Garé.

[٣] – د/ سامح عبد الواحد التهامي، المرجع السابق، ص ٤١٦.

[٤] – د/ سامح عبد الواحد التهامي، المرجع السابق، ص ٤١٧.

لأي شخص أن يطلع عليها أو يصل إليها في أي وقت، بما يهدد خصوصية صاحب هذه البيانات.

ونصت على ذلك، المادة السادسة من القانون رقم ٧٨ – ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، بقولها :" أن يتم الاحتفاظ بها – أي بالبيانات الشخصية – بصورة تسمح بتحديد هوية الأشخاص المعنيين، خلال فترة زمنية لا تجاوز المدة اللازمة لتحقيق الغرض الذي جُمعت وعُولجت من أجله هذه البيانات " [١].

غير أنه يجوز مخالفة القيد السابق في نص المادة المذكورة والخاص بتأقيت مدة الاحتفاظ بالبيانات الشخصية، في الحالة التي تتم فيها معالجة البيانات لأهداف تاريخية أو أهداف متعلقة بالبحث العلمي أو العمل الإحصائي، كل ذلك في إطار رقابة اللجنة الوطنية للمعلوماتية والحريات (C N I L) [٢].

وتطبيقاً لهذا الحكم الأخير، فقد وافقت اللجنة الوطنية للمعلوماتية والحريات على إجازة مد فترة حفظ البيانات الشخصية إلى مدة العشر سنوات، وجاءت هذه الموافقة في إطار الطلب الذي تقدمت به إدارة النظام المعلوماتي لمتابعة الطلاب الجامعيين، باعتبارها الجهة المسؤولة عن هذه المعالجة. وبررت الإدارة المذكورة طلبها، بحاجة إدارة الخدمات الإحصائية المركزية ورئاسة قطاع

---

[1] - Art. 6 , loi n° 78 – 17 :" Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : ……..

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. ".

[2] - La Commission National de L’informatique et libertés.

البرمجة والتنمية وإدارة الخدمات الإحصائية برئاسة الجامعات، لهذه البيانات التي تمت معالجتها؛ من أجل القيام بدراسات إحصائية عامة [١].

وذات الحكم السابق الذي أقره المشرع الفرنسي، **نص عليه المشرع المصري في القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية، في المادة (٤/٣) بقولها** :" يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية ..... ٤- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها ".

غير أن الخطأ ينتفي في حالة ما إذا تم التخلص من البيانات الشخصية نهائياً، أي بإعدامها وزوالها من جميع محركات البحث الإلكتروني بحيث لا يعد لها أي وجود. وأحياناً يُتبع ما يُعرف بالأرشفة الإلكترونية للبيانات الشخصية، والتي هي عبارة عن مجموعة من الوثائق الرقمية الإلكترونية سواء كانت كذلك من البداية أو كانت ورقية وتم تحويلها لإصداره إلكترونية بواسطة الماسح الضوئي، أي أنها تعني مجموعة الوثائق المحفوظة ومتاحة في بيئة رقمية [٢]، والتي تتم من خلال نظم الأرشفة الإلكترونية [٣].

---

[1] - CNIL : Délibération n° 03 – 013 du 23 mars 2003 portant avis sur le projet d'arrêté présenté le ministére de la jeunesse , de l'éducation nationale et de la recherché concernant la modification du traitment SISE , 24e rapport d'activité 2003 , p. 272 et s …… http:// www. Cnil . fr.

[٢] – د/ أحمد أبو بكر الهوش، الأرشفة الإلكترونية " الأسس النظرية والمعرفة العملية " ، دار حميثر للنشر والترجمة، سنة ٢٠١٨، ص ١٨.

[٣] – ويُقصد بنظم الأرشفة الإلكترونية، تلك النظم التي تعتمد على تكنولوجيا الحواسيب والتي تتيح العمليات والإجراءات من أجل الإدارة والسيطرة على عمليات تخزين الوثائق الإلكترونية واسترجاعها..... د/ أحمد أبو بكر الهوش، المرجع السابق، ص ١٩.

فعن طريق عملية الأرشفة، يمكن الاحتفاظ بالبيانات الشخصية لفترة أطول، بتحويلها إلى وسيط منفصل، والذي يقتصر حق الوصول إليه على عدد محدد من الأشخاص [١]، بما يحفظ حق الشخص في سرية بياناته من العبث بها أو الوصول إليها من قبل أي شخص.

فعلى سبيل المثال، قررت اللجنة الوطنية للمعلوماتية والحريات (C N I L)، أن البيانات المتعلقة بالمرخص له في النادي الرياضي، لا يمكن حفظها في قاعدة بيانات نشطة بعد انتهاء صلاحية الترخيص للمرخص له، ومع ذلك فإنه يمكن أرشفة تلك البيانات بدلاً من حذفها [٢]. لذلك قُضي بأن البيانات المؤرشفة والخاصة بحساب البريد الإلكتروني للشخص، يكون له عليها ملكية شخصية [٣].

المبحث الثاني

الخطأ المدني الناشئ عن عدم مشروعية معالجة البيانات الشخصية

– تقسيم:

سنتتعرض في هذا المبحث لماهية معالجة البيانات الشخصية (مطلب أول)، وصور الخطأ المدني الناشيء عن عدم مشروعية معالجة البيانات الشخصية (مطلب ثان). وذلك على النحو التالي:

[1]- Tiphaine Bessiére , op . cit , n° 111 . p. 22.
[2] - Tiphaine Bessiére , op . cit , n° 111 . p. 22.
[3] - Le juge référé mesures utiles et la messagerie électronique du détenu – Conseil d'Etat , 5 mars 2018 , n°: 414859 , Recueil Lebon.

المطلب الأول

ماهية معالجة البيانات الشخصية

بادئ ذي بدأ، وقبل التعرض لصور الخطأ المدني في الحالة التي تتم فيها عملية معالجة البيانات الشخصية بصورة غير مشروعة، يتوجب علينا تحديد المقصود بعملية معالجة هذه البيانات والشخص الذي يقوم بها أولاً.

لذلك سنبدأ حديثنا في هذا المطلب بتحديد المقصود بمعالجة البيانات الشخصية (فرع أول)، ثم بيان القائم بهذه المعالجة (فرع ثان)، وذلك على النحو التالي:

الفرع الأول

المقصود بمعالجة البيانات الشخصية

تعتبر عملية معالجة البيانات الشخصية، بمثابة الإجراء المفترض والضروري اللازم للحديث عن مدى وجود خطأ مدني يُعزى إلى المسؤول عن عملية معالجة البيانات إذا أخل بضوابط مشروعية هذه المعالجة، فقبل هذه الأخيرة، لا يمكن الحديث عن وجود حماية قانونية لهذه البيانات أو خطأ مدني عن ذلك، فهذا الأخير – أي الخطأ المدني – لا ينشأ إلا مع نشوء وجود عملية المعالجة.

ولقد تعرض لتعريف عملية معالجة البيانات الشخصية، كل من المشرع الفرنسي، والمشرع المصري، والمشرع الأوربي. فعرفها المشرع الفرنسي في القانون رقم ٧٨–١٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤، في المادة الثانية بفقرتها الثالثة، بأنها:" كل عملية أو مجموعة من العمليات التي تجري على هذه البيانات بصرف النظر عن الطريقة المستخدمة، بما في ذلك

جمعها وتسجيلها وتنظيمها وتخزينها أو حفظها، واقتباسها أو تعديلها، ومحوها، واستخدامها، والاطلاع عليها والكشف عنها بالنقل أو بالنشر أو خلاف ذلك مما هو متاح، وأيضاً غلقها أو محوها، أو تلفها " [١].

وتعرض المشرع المصري أيضاً لتعريف عملية معالجة البيانات الشخصية، **في المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية، وعرفها 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 ".

وعرفها المشرع الأوربي في المادة (٢/٤) من اللائحة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ الخاصة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية وحرية نقل هذه البيانات، التي نصت على أن المعالجة هي :" عملية أو مجموعة من العمليات تتم على البيانات الشخصية أو على مجموعة منها، يستوي في ذلك أن تكون هذه المعالجة قد تمت بصورة آلية أو غير ذلك، ويشمل ذلك جمع البيانات أو تسجيلها أو تنظيمها أو هيكلتها أو تخزينها أو تعديلها أو

[1] - Art: 2/3 , Loi n° 78 – 17(Modifié par LOI n°2018-493 du 20 juin 2018 - art. 9) :" …. un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ".

تغييرها أو استرجاعها أو الإفصاح عنها عن طريق الإرسال أو النشر أو غير ذلك من وسائل الإتاحة أو المواءمة أو الجمع أو التقييد أو المحو أو التدمير "[١].

ويلزم لتطبيق التعريفات السابقة والتي وردت في التشريعات المذكورة، ضرورة وجود عملية معالجة للبيانات الشخصية، من أجل أن يكون هناك خطأ مدني في الإخلال بضواط هذه المعالجة. ويتمثل هذا المعنى في وروده على واحدة أو أكثر من العمليات السالف ذكرها في التعريف السابقة.

وتطبيقاً لذلك، قضت محكمة العدل التابعة للاتحاد الأوربي، بأن نشاط محرك البحث عن المعلومات المنشورة أو مجرد وضعها على الإنترنت من قبل الغير أو جهات خارجية، من أجل فهرستها تلقائياً وتخزينها بصورة مؤقتة لإتاحتها على الإنترنت بترتيب معين، يعد معالجة لبيانات شخصية، ويعد القائم بهذا الأمر هو الشخص المسؤول عن عملية المعالجة وفقاً لما نصت عليه المادة " ٢/ د " من القانون رقم ٧٨ – ١٧ لسنة ١٩٧٨ [٢].

وفي هذا الصدد، أخذت محكمة العدل الأوربية في الاعتبار، حقيقة نشاط محرك البحث بصفته ممثلاً عن محرر المحتوى، على أساس أنه يقوم بوظيفة تسهيل تجميع المعلومات والوصول إليها، وهذا الأمر يترتب عليه أن يتحمل

---

[1] - Art 4/2 of Regulation (EU) 2016/679 :" 2- Processing means any operation or set of operations which is performed on personal data or on sets of personale data , whether or not by automated means , such as collection , recording , organization , structuring , storage , adaptation or alteration , retrieval , consultation , use , disclosure by transmission , dissemination or otherwise making available , alignment or combination , restriction , erasure or destruction ".

[2] - C J U E , 13 mai 2014 , Google Spain , aff C-131/ 12 .

– وفي التعليق على هذا الحكم:

- Céline CASTETS – RENARD , op. cit , N: 23.

مشغل المحرك مسؤولية مباشرة ومستقلة غير مرتبطة بمسؤولية الوسطاء التقنيين المصممين [١].

وأوضحت ذات المحكمة، العلاقة بين معالجة البيانات الشخصية والكشف عن هذه البيانات على شبكة الإنترنت في حكم (Lindquist). وقررت المحكمة أن عملية الإحالة على صفحة الإنترنت إلى أشخاص مختلفين، وتحديد هويتهم إما بالاسم أو بوسائل أخرى كرقم الهاتف مثلاً أو المعلومات الخاصة بظروف العمل وهواياتهم، يعتبر ذلك معالجة لبيانات شخصية سواء حدث ذلك بصورة كلية أو جزئية [٢].

الفرع الثاني

القائم بمعالجة البيانات الشخصية

ويقوم بعملية المعالجة شخص يسمى " المعالج " – أي المسؤول عن معالجة البيانات الشخصية – والذي عرفه المشرع الفرنسي في قانون المعلوماتية والحريات في المادة الثالثة بفقرتها الأولى، بأن :" المسؤول عن معالجة البيانات الشخصية هو – ما لم يعين صراحة في نصوص القوانين أو اللوائح المتعلقة

---

[1] - Moteur de recherché (Google) : responsabilité du traitement des données personnelles – cour de justice de l'Union européenne , 13mai 2014 , Recueil Dalloz , 2014 , p. 1476.

[2] - C J U E , 6 november 2003 , Lindquist , aff : c- 101/ 01 , EU : C : 2003 , 596.

– وفي التعليق على هذا الحكم:

- Céline CASTETS – RENARD , op. cit , N: 24.

بهذه المعالجة – الشخص أو السلطة العامة أو الوكالة أو المنظمة، التي تحدد أهداف المعالجة ووسائلها " [١].

وعلى الرغم من أن المشرع الفرنسي لم يفرق بين المسؤول عن عملية معالجة البيانات الشخصية وبين المعالج، إلا أن المشرع الأوربي وكذلك المشرع المصري، قد وضعا تعريفاً مستقلاً لكل منهما:

أ- تعريف المسؤول عن عملية معالجة البيانات الشخصية: أطلقت اللائحة الأوربية على هذا الشخص مسمى " المراقب "، وعرفته المادة الرابعة من هذه اللائحة بأنه :" الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو الهيئة التي تضع بمفردها أو بالاشتراك مع غيرها، أغراض ووسائل معالجة البيانات الشخصية " [٢].

وهذا الشخص أطلق عليه المشرع المصري في القانون رقم ١٥١ لسنة ٢٠٢٠، مسمى " المتحكم "، وعرفه في المادة (١) منه بأنه :" أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه ".

---

o [1] - Art : 3/ I , loi n° 78 – 17:(Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004)". Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

[2]- Art 4 of Regulation (EU) 2016/679 :" Controller means the natural or legal person , public authority , agency or other body which , alone or jointly with others , determins the purposes and means of the processing of personal data ……".

ب- تعريف المعالج: عرفته المادة الرابعة من اللائحة الأوربية بأنه :" الشخص الطبيعي أو القانوني أو السلطة العامة أو الوكالة أو أي هيئة أخرى تقوم بمعالجة البيانات الشخصية نيابة عن المراقب " [١].

وعرف المشرع المصري في المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠، المعالج بأنه :" أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقاً لتعليماته ".

والسؤال هنا: هل يقتصر مفهوم المسؤول عن عملية معالجة البيانات الشخصية على المعالج الرئيسي؟ أم أنه يمتد ليشمل أي شخص آخر يكون له دور في في هذه العملية كالمعالج الفرعي مثلاً؟

أجابت على هذا التساؤل، محكمة العدل التابعة للاتحاد الأوربي، بحكم لها قضت فيه بمسؤولية المعالج الثانوي أو الفرعي الذي كان له دور في عملية المعالجة إلى جانب مسؤولية المعالج الرئيسي، في قضية تتلخص وقائعها في قيام شركة ألمانية (Wirtsch aftsakademie) والتي كانت متخصصة في مجال التعليم، بالحصول على الكثير من المعلومات الإحصائية المجهولة عن من يزور صفحتها على الفيس بوك، وذلك بفضل ميزة (Facebook sight)، بالإضافة إلى أن بيانات زوار الصفحة الشخصية يتم تخزينها على ملفات الارتباط على فيس بوك.

وبسبب حدوث معالجة لهذه البيانات الشخصية من قبل الطرفين – أي من قبل مدير صفحة الشركة المذكورة على فيس بوك، وشركة فيس بوك

[1] - Art 4 of Regulation (EU) 2016/679 :" Processor means a natural or legal person , public authority , agency or other body which processes perspnal data on behalf of the controller ".

نفسها – قضت المحكمة بمسؤولية الطرفين معاً عن عمليات المعالجة التي تمت؛ فمدير الصفحة قد ساهم بصورة ثانوية في عملية المعالجة إلى جانب المعالجة الرئيسية التي قامت بها شركة فيس بوك.

وأوضحت المحكمة أن ما قضت به يتماشى مع مفهوم معالج البيانات الشخصية بأنه هو الشخص الطبيعي أو الاعتباري أو السلطة العامة أو أي هيئة أخرى تقوم بمفردها أو بالاشتراك مع جهة أخرى بعملية معالجة البيانات الشخصية. وأن هذا التعريف واسع، والهدف منه هو ضمان حماية فعالة وكاملة للبيانات الشخصية، كما أن كل من الطرفين السابقين يملك حق الوصول إلى البيانات الشخصية المعنية [١].

وترتيباً على ما تقدم، فإن تعيين الشخص الذي يُناط به مهمة معالجة البيانات الشخصية، قد يكون ذلك بموجب نص في القانون، ويحدث ذلك في الحالة التي تتولى فيها التشريعات أو اللوائح تعيين هذا الشخص. وأحياناً يتم تعيينه بصورة فعلية من خلال البحث عن الشخص الطبيعي أو الاعتباري الذي يُعهد إليه بتحديد أهداف المعالجة وطرقها [٢].

وبعد التوطئة السابقة، نجد أن كل من المشرع الفرنسي والمشرع المصري قد وضع العديد من الضوابط التشريعية لضمان مشروعية معالجة البيانات الشخصية. فالضوابط التي وضعها المشرع الفرنسي، جاء النص عليها في المادة

---

[1] - C J U E , gr . ch , 5 juin 2018 , aff. C- 210/ 16.

– وفي التعليق على هذا الحكم:

- Nicolas Nalepa , La notion de responsible du traitement – version large , 25 juin 2018 , Dalloz actualité , 25 juin 2018.

[2] - EVSOUSSAN (A.): In formatiqe et libertés , Edition francis Lefebvre , 2008 , p. 41.

السادسة من قانون المعلوماتية والحريات رقم ٧٨ – ١٧ لسنة ١٩٧٨، ، والتي منها يمكن أن نوجز هذه الضوابط في النقاط الآتية:

١- ضرورة أن يكون جمع ومعالجة البيانات الشخصية، قد حدث بصورة عادلة ومشروعة.

٢- ضرورة أن يكون الجمع لأغراض محددة وواضحة ومشروعة.

٣- ضرورة أن تكون البيانات كافية ومناسبة ولها علاقة بالغرض الذي من أجله تم جمعها ومعالجتها.

٤- ضرورة أن تكون البيانات دقيقة وكاملة ومناسبة لأغراض المعالجة وأن يتم تحديثها.

٥- ضرورة الاحتفاظ بالبيانات في شكل يسمح بتحديد هوية الأشخاص المعنيين بهذه البيانات لفترة لا تزيد على ما هو ضروري لتحقيق الغرض من جمع هذه البيانات ومعالجتها [١].

---

[1] - Art: 6 , loi n° 78- 17(Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193) :" Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :
1° Les données sont collectées et traitées de manière loyale et licite ;
2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des

وعلى غرار ما نص عليه المشرع الفرنسي في هذا الصدد، نجد أن المشرع المصري قد أقر ذات الضوابط ، **وجاء هذا الإقرار في المادة (٣) من القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية**، والتي أكدت على ضرورة أن تتم عملية المعالجة بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها، وأن تكون محددة ومعلنة للشخص المعني بهذه البيانات.

ومن مجمل ما جاء بالمادتين السابقتين، نستخلص أن المقصود بمشروعية معالجة البيانات الشخصية، هو ضرورة أن يكون لعملية المعالجة هدف واضح ومحدد ومشروع ومتوافق مع الهدف من المعالجة، وأن تتم هذه الأخيرة بدقة وملائمة للهدف من المعالجة، وكذلك ضرورة توافر موافقة صاحب البيانات على إجراء المعالجة.

وبمفهوم المخالفة للمعنى المتقدم، نجد أن المقصود بعدم مشروعية معالجة البيانات الشخصية والذي يثير الخطأ المدني الذي نحن بصدد دراسته، هو أن تتم عملية المعالجة بصورة عشوائية، وغامضة الهدف، وبطريقة غير مشروعة، وأيضاً إذا شاب عملية المعالجة عدم الدقة وعدم الملائمة للهدف من هذه

---

personnes concernées ;
3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;
5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées".

المعالجة، وكذلك إذا تخلف التزام أو أكثر من الالتزامات الملقاة على عاتق المسؤول عن عملية المعالجة، وأخيراً إذا تمت المعالجة بدون علم صاحب البيانات محل المعالجة أو رغم معارضته.

وترتيباً على ما تقدم، فإن جمع أومعالجة البيانات الشخصية يكون غير مشروع، ومن ثم تُثار مشكلة الخطأ المدني عن ذلك، إذا وُجدت صورة من الصور التي سنتعرض لها في المطلب التالي:

المطلب الثاني

صور الخطأ المدني الناشيء عن عدم مشروعية معالجة البيانات الشخصية

– تقسيم:

سنبدأ الحديث عن صور الخطأ المدني الناشيء عن عدم مشروعية معالجة البيانات الشخصية، بالحديث عن العشوائية في معالجة هذه البيانات (فرع أول)، والغموض في معالجة البيانات الشخصية (فرع ثان)، وعدم مشروعية الهدف من معالجة البيانات الشخصية (فرع ثالث)، ومخالفة الالتزامات الملقاة على عاتق المسؤول عن عملية معالجة البيانات الشخصية (فرع رابع)، ومعالجة البيانات الشخصية رغم عدم علم صاحبها أو معارضته (فرع خامس). وذلك على النحو التالي:

الفرع الأول

العشوائية في معالجة البيانات الشخصية

لقد أوجبت المادة السادسة سالفة الذكر من قانون حماية البيانات الشخصية الفرنسي، وكذلك المادة (١/٣) من قانون حماية البيانات الشخصية

المصري، أن يكون لعملية المعالجة هدف محدد، والغرض من ذلك هو منع عمليات المعالجة العشوائية للبيانات الشخصية، التي تحدث دون توافر الهدف المحدد. فعملية المعالجة تدور في إطار مبدأ تخصيص الهدف من هذه المعالجة، ومخالفة ذلك يضفي عليها عدم المشروعية، ومن ثم وجود خطأ مدني.

بالإضافة إلى أن عمليات المعالجة العشوائية للبيانات الشخصية، تتضمن تهديداً لحق الشخص في خصوصيته. فكلما انتفى عن عملية المعالجة شرط تحديد الهدف، انعكس ذلك بالتبعية على المساس بخصوصية الفرد في كل ما يتعلق ببياناته الشخصية، لاسيما مع تعدد وانتشار طرق تجميع البيانات الشخصية على النحو الذي بينَّاه في المبحث السابق.

وتعتبر مسألة تحديد الهدف من معالجة البيانات الشخصية، من مهمام الشخص المسؤول عن عملية المعالجة، وبدون توافر هذا التحديد لن يُسمح له بإجراء المعالجة. وإذا خالف المسؤول هذا الالتزام ثارت مسؤوليته المدنية لوجود خطأ مدني في هذه الحالة.

وتطبيقاً لذلك، ألزم مجلس الدولة الفرنسي إحدى الشركات التي قامت بعملية معالجة للبيانات الشخصية للكيانات المرتبطة بها، بأن تحدد الهدف من جمع ومعالجة هذه البيانات، وأن تحدد الشركة حق الوصول إليها، وذلك في إطار رقابة من اللجنة الوطنية للمعلوماتية والحريات، وذلك بعد أن حددت الشركة مدة صلاحية البيانات وأدخلت تصحيحات على معالجتها. وهذا الأمر يعني أن الشركة باعتبارها المسؤولة عن عملية المعالجة، هي الملتزمة بتحديد

أغراض ووسائل المعالجة، وتعيين مراقب لحماية البيانات من قبل الكيانات الأخرى التي لا تملك بذاتها التأثير الذي يجعلها مسؤولة عن المعالجات [١].

وفي إطار الحديث عن الهدف المحدد لعملية معالجة البيانات الشخصية، يثور تساؤلان على قدر من الأهمية، وهما:

١- التساؤل الأول: هل يعني ضرورة أن يكون لعملية المعالجة هدف محدد، وجوب اقتصار هذه المعالجة على هدف واحد؟ أم أنه يجوز أن تتعدد الأهداف عن نفس عملية المعالجة؟

أجابت عن هذا التساؤل اللجنة الوطنية الفرنسية للمعلوماتية والحريات، قائلة أن وجوب توافر الهدف المحدد لعملية المعالجة، لا يعني اقتصارها على وجود هدف واحد ترمي المعالجة إلى تحقيقه، بل يجوز أن تتعدد هذه الأهداف رغم أنها منبثقة عن عملية معالجة واحدة، ولكن بشرط أن تكون هذه الأهداف محددة بصورة لا تثير أي لبس أو غموض، وأن يكون تحديدها سابقاً لإجراءات المعالجة، أي أن يتم التحديد قبل إجراء المعالجة.

٢- التساؤل الثاني: هل يتعارض الأخذ بالدراسات السابقة مع ضابط تحديد الهدف من عملية معالجة البيانات الشخصية؟

تعني الدراسات السابقة، كل الأمور البحثية والدراسات المتصلة بموضوع ما، مما قد تم نشرها بأي شكل من الأشكال شريطة أن تكون مساهمة ذات قيمة علمية. وقد يكون النشر بالطباعة أو بواسطة المحاضرات أو الأحاديث المذاعة

---

[1] - Traitement de données ā caractére personnel identification de la personne responsible
– Conseil d'Etat , 12 mars 2014 , n°: 354629 , Recueil Lebon , 2014.

بالصوت فقط أو بالصوت والصورة معاً، أو تم تقديمها لمؤسسة علمية للحصول على درجة علمية أو على مقابل مادي أو لمجرد الرغبة في المساهمة العلمية [١].

يدور التساؤل السابق في إطار مدى جواز تحديد الهدف من معالجة البيانات الشخصية عن طريق الاستعانة بالدراسات السابقة وخصوصاً في مجال البحوث الطبية وغيرها.

أجابت عن ذلك اللجنة الوطنية الفرنسية للمعلوماتية والحريات، قائلة بجواز تحديد الهدف من معالجة البيانات الشخصية عن طريق الاستعانة بمعالجات سابقة في دراسات وأبحاث لاحقة؛ تأسيساً على أن المنهج الأكثر شيوعاً في البحث العلمي يقوم على أساس الدراسات السابقة. وعلى ذلك سمحت اللجنة بجواز الاستعانة بالملفات الإدارية في حالة كون معالجة البيانات الشخصية المدرجة في هذه الملفات تدعم هدفاً آخر ولها علاقة به، وكان هذا الهدف يقع في ذات مجال الدراسة [٢].

الفرع الثاني

الغموض في معالجة البيانات الشخصية

لقد اشترط المشرع الفرنسي في المادة السادسة سالفة الذكر من قانون المعلوماتية والحريات، وكذلك المشرع المصري في المادة (١/٣) من قانون حماية البيانات الشخصية، ضرورة أن يكون الهدف المحدد من عملية المعالجة،

---

[١] – أ/ عبد السلام عبد الجبار، الدراسات السابقة، ورقة بحثية ضمن متطلبات الحصول على درجة الماجستير من كلية الدعوة وأصول الدين بالجامعة الإسلامية بالمدينة النبوية، سنة ١٤٣٢ – ١٤٣٣ هـ .

[2] - C N I L : 3éme rapport d'activité , 15 octobre 1981 – 15 octobre 1982 , La document Française , Paris , 1983 , p. 148.

واضحاً. ويعني الوضوح ضرورة ألا ينتاب الهدف من المعالجة أي غموض يخلق نوعاً من اللبس في ذهن صاحب البيانات بشأن الهدف من معالجة بياناته. أي وجوب أن يكون الشخص المعني على بصر وبصيرة كاملين فيما يتعلق بالهدف من إجراء المعالجة.

ويـعد ضابط الوضوح في عملية المعالجة، امتداد منطقي لضابط التحديد. فالهدف من معالجة البيانات الشخصية يعني التصريح به وإيضاحه، وهذا الأمر يحدث بطريق رسمي من خلال النص عليه صراحة في الطلب المقدم إلى اللجنة الوطنية الفرنسية للمعلوماتية والحريات، والذي يلتزم المعالج بتقديمه إلى هذه اللجنة قبل إجراء عملية المعالجة ذاتها.

ويعد ضابطي التحديد والوضوح، من أهم مظاهر مبدأ الشفافية في إجراء أي معالجة للبيانات الشخصية. وهذا الأمر أقرته اللجنة الوطنية للمعلوماتية والحريات في واقعة تدور أحداثها في أن منظمتين غير هادفتين لتحقيق الربح، تقدمتا بشكوى إلى اللجنة المذكورة – عن طريق عدة شكاوى جُمعت من حوالي ٩٩٧٤ فرد – ضد شركة (Google)، على سند أن هذه الشركة لم تلتزم بمبدأ الشفافية عند جمعها للبيانات الشخصية للمستخدمين، وذلك من ناحيتين:

أ– الناحية الأولى: وتتمثل في أن أنظمة الآندرويد للهواتف الذكية والتي طورتها الشركة المذكورة، تتضمن نوعاً من الاستغلال لهذه البيانات؛ لكونها منتشرة – أي الأنظمة – على عدة صفحات تتطلب إفصاح المستخدم عن بيانات ذات طبيعة شخصية، بما يزيد من فرص التلاعب بها.

ب– الناحية الثانية: وتتمثل في أن موافقة الأشخاص بالحصول على خدمات المواقع المذكورة محل انتقاد؛ لأنها تفتقد إلى ضابط التحديد: فإما أن

يقبل المستخدم الشروط بصورة كلية والخاصة بكل برنامج، أو أن يُحرم من استخدامه.

وفي الأخير، حكمت اللجنة على الشركة المذكورة، بمبلغ (١٥٠) ألف يورو. وبسبب تكرار الأمر، حكمت ذات اللجنة على ذات الشركة بمبلغ (٥٠) مليون يورو [١].

والقاعدة أن ضابطي التحديد والوضوح لا يُفترضا، بل لابد من البحث عنهما في كل عملية معالجة بيانات شخصية؛ حفاظاً على هذه البيانات ونزولاً على أهميتها وخطورتها وما تمثله من قيمة معنوية ومادية في بعض الأحيان لأصحابها.

غير أن المشرع الفرنسي خالف هذه القاعدة في حالة تجميع ومعالجة هذه البيانات لأغراض تاريخية أو احصائية أو علمية؛ حيث أقام المشرع قرينة على أن التجميع أو المعالجة في هذه الحالة يكونا بهدف محدد وواضح بصورة مفترضة، بشرط أن تُراعى المبادئ والإجراءات المنصوص عليها في هذا القانون والواردة في الفصل الرابع والمادة الأولى من الفصل الخامس والفصلين التاسع والعاشر من هذا القانون. والقرينة هنا بسيطة، أي قابلة لإثبات العكس بأن لم تُراع القواعد والإجراءات القانونية آنفة الذكر [٢].

---

[1]- C N I L: Délibération , n°: 2019 – 001 , du 21 janvier 2019 : Delphine Castel , protection des données personnelles – Réglementation – Des association Font condemner . Google ā un amende – juris association , 2019 , n°593 , p. 11 , Dalloz , 15 Février 2019.

[2] - Art 6 , loi n° 78 – 17: " …… Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre,

الفرع الثالث

عدم مشروعية الهدف من معالجة البيانات الشخصية

لقد سبق الذكر بأن المادة السادسة من القانون رقم ٧٨ – ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، وكذلك المادة (٣/٣) من قانون حماية البيانات الشخصية المصري، قد أقرا صراحة ضرورة أن تكون عملية جمع ومعالجة البيات الشخصية مشروعة. والمشروعية هنا تعني وجوب أن يكون الجمع أو المعالجة متفقين مع الغرض المحدد والواضح لعملتي الجمع أو المعالجة.

وبعد أن أرسى المشرع المصري المبدأ العام الذي يقضي بضرورة أن تكون عملية المعالجة مشروعة في المادة (٣/٣) من القانون رقم ١٥١ لسنة ٢٠٢٠، **فقد حدد حالات مشروعية وقانونية المعالجة الإلكترونية للبيانات الشخصية في المادة (٦) من القانون المذكور، والتي تتمثل في الآتي:**

أ- حالة وجود موافقة من الشخص المعني بهذه البيانات على عملية المعالجة، من أجل تحقيق غرض محدد أو أكثر.

ب- حالة ما إذا كانت عملية المعالجة لازمة وضرورية تنفيذاً لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنه.

ج- حالة المعالجة الخاصة بتنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً على حكم قضائي.

---

au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées .

د- حالة المعالجة التي يكون الهدف منها تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

والهدف من هذا الشرط ، هو المحافظة على البيانات الشخصية ومنع استغلالها والمتاجرة بها والحيد عن الهدف الرئيسي من جمعها أو معالجتها. فهذه البيانات لا تشكل خطراً في حد ذاتها، غير أن الخطر يكمن في استخدامها، أي الغاية من معالجتها.

فعلى سبيل المثال، إذا تم تجميع البيانات الصحية أو معالجتها بهدف إجـراء بـحث عـلمي طبي، كان ذلك بمثابة غاية مشروعة للتجميع أو المعالجة. أما إذا تم تجميعها أو معالجتها من أجل تحقيق أغراض تجارية، فهنا تفقد عملية التجميع أو المعالجة مشروعيتها [١].

واهتماماً من اللجنة القومية الفرنسية للمعلوماتية والحريات، في التأكيد على ضابط مشروعية جمع ومعالجة البيانات الشخصية، فقد استلزمت اللجنة ضرورة سبق اخطارها بعمليات الجمع أو المعالجة [٢]، ولا يجوز إتيان أي منهما بالتجاوز للأغراض الواردة في اخطار هذه اللجنة، وإلا أصبح الجمع أو المعالجة غير مشروعين.

وتطبيقاً لذلك، قضت محكمة النقض الفرنسية بعدم مشروعية جمع البيانات الشخصية من قبل شركة الخطوط الجوية الفرنسية (Air France)، والتي قامت بوضع أداة كمبيوتر تسمى (F I D E L E)، والتي كان لها – أي

---

[١] – د/ سامح عبد الواحد التهامي، المرجع السابق، ص ٤١٥.

[2] -M. Falala , Réponse ministérielle à question écrite n° 29894 , JOAN Q 19 octobre 2004 , p. 8112 …. www.dalloz.fr.

أداة الكمبيوتر – غرض مزدوج تم إعلان اللجنة الوطنية به، والذي كان يتمثل في ناقل لحركة المعلومات بين أطقم الرحلات الفنية ومديريها بخصوص النشاط اليومي والأحداث الهامة المتعلقة بتشغيل الأسطول، هذا من ناحية. ومن ناحية أخرى، إدارة جدول الطيارين.

وأسست المحكمة ما قضت به، تأسيساً على تجاوز الغرض من جمع البيانات الشخصية من قبل الشركة المذكورة، حيث تم جمع جمع بيانات ذات طبيعة شخصية دون علم أصحابها ودون أن تُدرج ضمن الأغراض التي أعلنت بها شركة الخطوط الجوية الفرنسية اللجنة الوطنية الفرنسية للمعلوماتية والحريات[١].

وضابط المشروعية الذي نحن بصدده، ما هو إلا التزام يقع على عاتق المعالج بأن يكون أميناً عند إجراء عملية المعالجة. وهذا الالتزام يعني أمرين متلازمين هما:

أ- الأمر الأول: ضرورة أن تكون البيانات محل الجمع أو المعالجة ملائمة: وتعني الملائمة أن تكون البيانات كافية ومناسبة وذات صلة بالغرض الذي من أجله تم جمعها أو معالجتها، أي ليست زائدة عن المطلوب فيما يتعلق بالأغراض التي على أساسها تم جمع هذه البيانات أو الهدف من عملية معالجتها [٢].

ب- الأمر الثاني: ضرورة أن تكون البيانات محل الجمع أو المعالجة، دقيقة وكاملة ومناسبة لأغراض المعالجة، وأن يتم تحديثها وأن تُتخذ الإجراءات

---

[1] - Cass . soc , 6 Avril 2004 , n°: 01 – 45 . 227 , Dalloz . 2004 , 2736.

[2] - Art 6 , loi n° 78 – 17: "…… 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs".

اللازمة للتأكد من أن البيانات غير الصحيحة أو غير الكاملة من منظور الغرض أو الهدف من الجمع أو المعالجة، سيتم تصحيحها، وفي حالة تعذر ذلك وجب محوها [١].

وتطبيقاً لذلك، قضى مجلس الدولة الفرنسي بأن جمع البيانات الشخصية للأفراد، يجب أن يتسم بالمشروعية وأن يكون متفقاً مع الأغراض المشروعة للجمع والمعالجة، ويجب أن تتم عملية المعالجة للبيانات بطريقة دقيقة [٢].

كما أبدت اللجنة الوطنية الفرنسية للمعلوماتية والحريات بعض الملاحظات فيما يتعلق باستخدام أنظمة المراقبة الآلية غير المتماثلة من قبل إحدى الشركات، بهدف مراقبة التصرفات الإجرامية المحتملة لبعض العملاء؛ حيث اعتبرت اللجنة أن الأنظمة الآلية المتماثلة فقط هي التي توفر ضمان دقة وسلامة البيانات المعالجة [٣].

والدقة هنا، تعني التناسب بين جمع البيانات أو معالجتها وبين الهدف من ذلك. فعلى سبيل المثال، إذا كانت عملية الجمع أو المعالجة تتم لأغراض صحية، وجب اقتصار الجمع أو المعالجة على المعلومات الصحية فقط دون التطرق لغيرها من البيانات الشخصية، سواء كانت ذات طابع مالي أو مهني أو شخصي. وكذلك إذا كان الجمع أو المعالجة من أجل حصول على خدمة أو

---

[1] - Art 6 , loi n° 78 – 17: ".....4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifies".

[2] - Conceil d'Etat , 11 mars 2013 . n°: 332886.

[3] - C N I L: Délibération , n°: 2006 – 048 , du 23 Février 2006…. www. Legifrance.gouv.fr.

سلعة معينة، وجب اقتصار جمع ومعالجة بيانات هذا الشخص على ما يكون لازماً ومتناسباً مع الحصول على هذه الخدمة أو السلعة.

وتأييداً لذلك، أكدت اللجنة الوطنية الفرنسية للمعلوماتية والحريات على ذات المعنى، بخصوص انشاء نظام رقمي لمعالجة البيانات الشخصية لتنظيم دخول الطلاب لمطعم في إحدى المدارس. حيث قالت اللجنة أن هذا النظام قائم على أساس وضع بصمة اليد في جهاز على باب المطعم، ولا يجوز تجميع بيانات أكثر من تلك اللازمة لعمل هذا النظام. وزيادة من اللجنة في التأكيد على هذا الأمر، فقد حددت هذه البيانات أيضاً [١].

وتطبيقاً لما تقدم، فقد قضى مجلس الدولة الفرنسي، بأن تسجيل رقم الهوية الوطنية للمستخدم، لا يلبي نظام حوسبة إدارة ملفات الأجانب الذين تقدموا بطلب للحصول على تصريح إقامة، والذي يُعرف برقم (AGDREF)؛ لأنه لم تكن هناك ثمة فائدة من حوسبة أو معالجة هذا البيان. لذلك تعتبر عملية المعالجة هنا غير متوافقة مع أحكام القانون رقم ٧٨ – ١٧ لسنة ١٩٧٨؛ وذلك لتجاوز الغرض من عملية الجمع والمعالجة [٢].

وفي هذا الصدد أيضاً، قضت محكمة استئناف باريس بعدم مشروعية استعمال ملفات الأجَراء وعناوينهم الإلكترونية بقصد استخدامها في الدعاية السياسية [٣]. وقضت ذات المحكمة كذلك، بأن المعلومات المسجلة على برنامج

---

[1] - C N I L , Délibération 2006 – 103 , du 27 avril 2006.

[2] - Appréciation de la légalité du décretcréant un traitement de la données personnelles relative aux étrangers faisant l'object d'une mesure d'éloignement , dit Elol – Conseil d'Etat 30 décembre 2009 , n°: 31 2051 31 760 , Recueil Lebon – Recueil des décisions du Conseil d'Etat , 2009.

[3] - Cour d'apple de paris , 31 mai 1995.

الحاسب الآلي من أجل حجز تذاكر النقل، لا يجوز استعمالها من قبل رب العمل لمراقبة أنشطة العمال [١].

وبمفهوم المخالفة لما تقدم، إذا التزم المعالج حدود المعالجة أو الجمع والغرض من كلاهما بالملائمة والدقة السابقين، فلا يشكل فعله خطأ مدنياً يستوجب مسؤوليته المدنية. وتطبيقاً لذلك، قضى مجلس الدولة الفرنسي بأنه لا يتعارض مع واجب الأمانة والمشروعية، جمع ومعالجة البيانات الخاصة بالقروض المستحقة على العميل، إذا كان الهدف من تبادلها بين مؤسسات الائتمان، كي تتخذ قرارها بشأن قبول أو رفض طلبه للقرض أو الائتمان. وأساس هذا القضاء هو أن عدم وجود تعارض بين عملية المعالجة في هذه الحالة وبين واجب الأمانة والمشروعية الملقى على عاتق المعالج، لاسيما وأن المعالجة لن تتم إلا بعد موافقة العميل على نقل بياناته قبل رد البنك عليه بقبول أو رفض طلبه [٢].

الفرع الرابع

مخالفة الالتزامات الملقاة على عاتق المسؤول عن معالجة البيانات الشخصية

لقد نص كل من المشرع الفرنسي والمشرع المصري، على مجموعة من الضوابط والالتزامات القانونية التي يتعين على الشخص المسؤول عن عملية معالجة البيانات الشخصية الالتزام بها، والتي يترتب على مخالفتها وجود خطأ مدني. وعلى ذلك سنتعرض لتخلف التزامات المسؤول عن المعالجة في القانون الفرنسي (غصن أول)، ثم لتخلف التزاماته في القانون المصري (غصن ثان):

---

[1] - Cour d'apple de paris , 31 mai 1995.

[2] - Conseil d'Etat , 30 décembre 2009 , n°: 306173 , Recueil Lebon: 535.

الغصن الأول

تخلف التزامات المسؤول عن عملية المعالجة قبل صاحب البيانات الشخصية في القانون الفرنسي

جاء النص على التزامات معالج البيانات الشخصية في القانون الفرنسي، في المادة الثانية والثلاثين من القانون ٧٨ – ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات. ويُستفاد من هذه المادة أن معالج البيانات، يلتزم بإعلام صاحب البيانات محل المعالجة بهويته – أي هوية المعالج – وهوية من يمثله إذا لزم الأمر، وعليه أن يعلمه بالغرض من إجراء هذه المعالجة، وبالطابع الإلزامي أو الإختياري للإجابات، وبالعواقب المحتملة في حالة وجود خطأ في إجابات صاحب البيانات.

ويلتزم المعالج أيضاً بإعلام صاحب البيانات بالأشخاص المُرسل إليهم البيانات أو فئات المُرسل إليهم، وعليه أن يعلمه كذلك بالحقوق المقررة له طبقاً لأحكام القسم الثاني من هذا الفصل، ويلتزم كذلك عند الاقتضاء بإعلانه بالإجراءات المقترحة في حالة نقل البيانات الشخصية لدولة غير عضو في الاتحاد الأوربي، وأخيراً عليه أن يعلمه بفترة حفظ بياناته الشخصية وفي حالة تعذر ذلك وجب عليه إعلامه بالمعايير اللازمة لتحديد هذه المدة [1]. وسنتعرض

[1] - Art 32/ I , loi n° 78 – 17: " I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

2° De la finalité poursuivie par le traitement auquel les données sont destinées ;

3° Du caractère obligatoire ou facultatif des réponses ;

4° Des conséquences éventuelles, à son égard, d'un défaut de

لحالات خطأ المعالج المدني بخصوص هذه الالتزامات بشيء من التوضيح على النحو الآتي:

أ- عدم إعلام صاحب البيانات بهوية القائم بعملية المعالجة: ألزم المشرع الفرنسي في نص المادة الذكورة، معالج البيانات بأن يفصح عن هويته. وتحديد هذه الأخيرة يعني أن يذكر المعالج من المعلومات والبيانات ما يستطيع معه صاحب البيانات محل المعالجة من التعرف على حقيقة الشخص الذي يعالج بياناته الشخصية، بحيث يسهل عليه أن يرجع على هذا الشخص بشأن أي أمر يتعلق بعملية المعالجة . ومن هذه المعلومات على سبيل المثال: اسم المعالج، وعنوانه أو عناوينه في حالة ما إذا كان للمعالج أكثر من عنوان، ووظيفته.

ونظراً لأن المعالج قد لا يقوم بعملية المعالجة بنفسه، فقد يعهد بذلك إلى شخص يمثله في القيام بعملية المعالجة، فهنا يجب على الممثل ذكر البيانات التي تحدد هويته لصاحب البيانات. ونفس الأمر ينطبق في الحالة التي يتولى فيها عملية المعالجة أكثر من شخص، كالمعالج الرئيسي والمعالج الثانوي.

---

réponse ;

5° Des destinataires ou catégories de destinataires des données ;

6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;

7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;

8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

وتكمن الحكمة من تطلب هذا الالتزام، في أمرين: أحدهما معنوي والآخر اقتصادي، وهما:

*** الأمر الأول (المعنوي):** ويتمثل في أن تطلب هذا الالتزام، يخلق نوعاً من الثقة بين المسؤول عن عملية المعالجة وبين صاحب البيانات محل المعالجة. فهذه الثقة لا تتوافر في ما إذا كانت هوية المعالج غير معلومة أو غامضة.

*** الأمر الثاني (الاقتصادي):** ويتمثل في البعد الإقتصادي لوجود هذا الالتزام. وتفسير ذلك، أن معظم – إن لم يكن جميع – السلع والخدمات التي تُعرض للبيع، أصبح شراؤها يتطلب من المشتري الإفصاح عن الكثير من البيانات الشخصية، الأمر الذي قد يخلق تخوفاً لدى بعض الأفراد في الإفصاح عن بياناتهم إلا في ظل وجود ضمانات قانونية تمنع العبث بها أو استعلالها. ولا شك أن من أهم هذه الضمانات، هومعلومية هوية الشخص المنوط به مهمة معالجة البيانات. وهذا الأمر تكون نتيجته في الأخير، إقبال الأفراد على الشراء بدون تخوف. وهذا الأمر يتعذر وجوده في الفرض العكسي، الذي تكون فيه هوية المعالج غير معلومة.

ب– عدم إعلام صاحب البيانات بالغرض من عملية المعالجة: وهنا يلتزم المعالج بأن يخبر صاحب البيانات بكل أمانة وشفافية، الغرض من معالجة بياناته الشخصية. وضرورة التأكيد على أن البيانات محل المعالجة لن تُستخدم إلا في الغرض الذي من أجله تمت معالجتها، وأن أي أمر أو غرض بخلاف ذلك يعتبر خطأ مدني من المعالج يستوجب مسؤوليته المدنية. وقد سبق بأن بينًا ذلك منذ قليل.

ج- عدم إعلام صاحب البيانات بمدى إلزامية أو إختيارية البيانات محل المعالجة: إن البيانات التي تخضع لعملية المعالجة، لا تكون على درجة واحدة من حيث طابعها الإختياري أو الإلزامي بالنسبة لصاحب البيانات. وهذا يعني أن هناك بيانات لابد من توافرها بصورة حتمية ولا تتم عملية المعالجة إذا تخلف ذكرها أو الإفصاح عنها أي أنها تتسم بالطابع الإلزامي، وهناك بيانات لا يترتب على تخلفها عدم اتمام عملية المعالجة نزولاً على طابعها الإختياري.

وهنا يقع على عاتق المسؤول عن معالجة البيانات الشخصية، التزام بتبصير صاحب البيانات، بالبيانات ذات الطابع الإلزامي وتلك ذات الطابع الاختياري التي ربما يفضل صاحبها عدم ذكرها حسبما يتراءى له.

د- عدام إعلام صاحب البيانات بالعواقب المحتملة للخطأ في الإجابة على البيانات محل المعالجة: لاشك أن الدور الأكبر في عملية معالجة البيانات الشخصية، يقع على عاتق المسؤول عن هذه المعالجة. غير أن ذلك لا ينفي الدور الجوهري لصاحب هذه البيانات، فهو الذي يدلي بها ويقدمها للمعالج، ومن ثم يكون هو المسؤول عن مدى مصداقيتها من عدمه.

لذلك يجب على المعالج أن ينبه صاحب البيانات بأنه في حالة ما إذا أخطأ في الإجابة على أمر تستلزمه عملية المعالجة، سيترتب على ذلك جزاءات توقع عليه – أي على صاحب البيانات – وذلك من أجل أن يولي هذا الأخير مسألة الإفصاح عن هذه البيانات درجة من الأهمية؛ تقديراً لخطورتها وأهميتها.

هـ – عدم إعلام صاحب البيانات بالمرسل إليهم بياناته: تتمثل الحكمة من هذا الالتزام في أنه قد يترتب على علم صاحب البيانات محل المعالجة بأن بياناته سوف تُرسل لفئة معينة أو شخص ما، رفضه لعملية المعالجة. وهذا الأمر يقوم على اعتبارات الملاءمة التي يقدرها صاحب البيانات. فهذه الأخيرة

بمثابة إرث معنوي لصاحبها وله مطلق الحرية في تحديد الشخص أو الأشخاص الذين يجوز لهم الاطلاع على بياناته أو معرفتها.

و- عدم إعلام صاحب البيانات بالحقوق المقررة له على بياناته: من التزامات المعالج، تبصير صاحب البيانات بكل حق يثبت له على بياناته الشخصية. فالمشرع الفرنسي أعطى لصاحب البيانات الشخصية مجموعة من الحقوق على بياناته، لا يجوز حرمانه منها، والتي تتمثل في حق صاحب البيانات في الاعتراض على معالجة بياناته، وحقه في الاطلاع عليها، وحقه في الدخول في طي النسيان بالنسبة لها.

ومبرر هذا الالتزام، هو أن عملية معالجة بيانات الشخص، لا يترتب عليها غل يده عن هذه البيانات، بل يظل هو المالك لها وهو صاحب القرار بشأنها، وله مطلق الحقوق عليها بما لا يتعارض أو يخل بالتزاماته مع الغير فيما يخص بياناته التي تم معالجتها.

ز- عدم إعلام صاحب البيانات بالإجراءات المقترحة في حالة نقل بياناته لدولة غير عضو في الاتحاد الأوربي: يعتبر هذا الالتزام حق رئيسي لصاحب البيانات محل المعالجة، في أن يطمئن أن بياناته لن تغادر الحدود الجغرافية لبلده عند اللزوم، إلا في إطار مجموعة من الضوابط والإجراءات تحفظ له حقوقه عليها وخصوصيته بشأنها.

ح- عدم إعلام صاحب البيات بمدة حفظ بياناته: أوجب المشرع الفرنسي على معالج البيانات ضرورة أن يخبر صاحب البيانات بمدة حفظ هذه البيانات واللازمة لتحقيق الغرض من معالجتها [1]. وإذا تعذر تحديد مدة محددة، التزم

[1] - Matthieu Dary , L'enjeu de la conformité ā la réglementation des données personnelles pour les collectivités territoriales , Nina Gosse , A J Colletivités terrtoriales , 2018 , p. 322.

المعالج بإعلام صاحب البيانات بالمعايير اللازمة لتحديد هذه المدة، ويتحدد ذلك على ضوء الهدف من المعالجة. والحكمة من هذا الالتزام، هي منع الاحتفاظ المؤبد بالبيانات الشخصية للأفراد على نحو يهدد خصوصياتهم ويتعارض مع الضوابط الأخرى لمعالجة هذه البيانات.

ونظراً لخطورة هذا الالتزام، فقد أوجب المشرع الفرنسي على كل مسؤول عن عملية معالجة للبيانات الشخصية، أن يتضمن الإخطار أو طلب الترخيص بمعالجة هذه البيانات والمقدم إلى اللجنة الوطنية للمعلوماتية والحريات، شرطاً في الطلب أو الإخطار بالمدة التي تُحفظ فيها هذه البيانات، من أجل إحكام رقابة اللجنة الوطنية على عملية المعالجة.

وتطبيقاً لذلك، فقد أوصت اللجنة الوطنية للمعلوماتية والحريات، بضرورة أن تكون مدة حفظ البيانات الشخصية والخاصة بالمعالجة التي قامت بها وزارة التعليم الفرنسية لإدارة الأمور التربوية والمالية للطلاب في المدارس الثانوية الحكومية، هي سنتان؛ على أساس أن هذه المدة كافية لتحقيق الغرض من عملية المعالجة [١]. وذلك بإستثناء المعالجات التي تكون لأحداث تاريخية أو احصائية أو علمية، ولكن تحت رقابة اللجنة الوطنية للمعلوماتية والحريات [٢].

---

[1] - C N I L : Délibération n°: 92 – 130 , du 24 november 1992 , portant avis sur la mise en oeuvre , par le minister de l'education nationale , d'un traitement automatisé d'informations nominatives dénommé scolarité….. www.legimonible.fr/cnil.

[2] - Art 36 , loi n° 78 – 17 Modifié par (LOI n°2018-493 du 20 juin 2018 - art. 14): " Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine.

وتطبيقاً لما تقدم، فقد أعلنت اللجنة الوطنية الفرنسية للمعلوماتية والحريات بصورة صريحة بعض الالتزامات السابقة بمناسبة فحصها للشروط الخاصة بالتحقيق الذي أجراه أحد المعاهد؛ حيث أوجبت اللجنة ضرورة أن يتعهد المعهد بتعديل الرسائل التابعة للاستبيانات التي وجهها المعهد للأفراد الذين خضعوا للمسح، بهدف إعلامهم بالطابع الإختياري للأسئلة، وكذلك بالمستفيدين من الإجابات، وكيفية ممارسة حقهم في الولوج إلى بياناتهم الخاصة، وكيفية القيام بتصحيحها أو محوها إذا لزم الأمر [١].

والقاعدة أن المشرع الفرنسي تطلب الضوابط السابقة في أي عملية معالجة تُجرى للبيانات الشخصية للأشخاص، غير أن المسؤول عن المعالجة يُعفى من الالتزامات السابقة إذا كانت المعالجة تخص المجال الصحي [٢]، وذلك بالإستثناء من حكم المادة (٣٢) سالفة الذكر من قانون المعلوماتية والحريات الفرنسي.

---

[1] - C N I L : Délibération n°: 96 – 035 du 16 avril 1996 , relative ā la mission de verification sur place effectuée le 4 avril 1996 auprés de l'Institut Louis Harris ….. www.legifrance.gouv.fr/.

[2] - Art 53 , loi n° 78 – 17(Modifié par LOI n°2018-493 du 20 juin 2018 - art. 16) " Outre aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, les traitements contenant des données concernant la santé des personnes sont soumis aux dispositions du présent chapitre, à l'exception des catégories de traitements suivantes :

1° Les traitements relevant des 1° à 6° du II de l'article 8 ;

2° Les traitements permettant d'effectuer des études à partir des données recueillies en application du 6° du même II lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;

3° Les traitements mis en œuvre aux fins d'assurer le service des prestations ou le contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;

4° Les traitements effectués au sein des établissements de santé

وتتمثل علة هذا الاستثناء، في مراعاة مصلحة المريض، إذا كان هناك أسباب مشروعة يقدرها الطبيب المعالج؛ فهنا يجوز عدم إعلام المريض بتشخيصه المرضي أو بالمضاعفات التي ربما تحدث له [١]. وإجمالاً كل ما يمكن أن يؤثر على صحة المريض بالسلب.

الغصن الثاني

تخلف التزامات المسؤول عن معالجة البيانات الشخصية أو المتحكم في القانون المصري

وضع المشرع المصري في القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية، مجموعة من الالتزامات على عاتق معالج هذه البيانات. وبالإضافة إلى ذلك، أقر – أي المشرع المصري – مجموعة من الالتزامات على الأشخاص الذين يكون لهم دور في جمع ومعالجة وحماية البيانات غير المعالج كالمتحكم والمسؤول عن حماية البيانات. وسنتعرض في هذا الغصن لبيان التزامات كل منهم لوجود بعض الترابط بين الالتزامات الملقاة على عاتقهم وذلك على النحو التالي:

أولاً: تخلف التزامات المعالج:

---

par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;

5° Les traitements effectués par les agences régionales de santé, par l'Etat et par la personne publique qu'il désigne en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article L. 6113-8

[1] - LABOILE (X.): Aspects Juridique et éthiques du recueil des donnée médicales aux fins d'analyses épidémiologiques , Thése , Université de Bordeaux IV , 2000 , P. 23 ET S.

حدد المشرع المصري التزامات معالج البيانات الشخصية في المادة (٥) من القانون رقم ١٥١ لسنة ٢٠٢٠، والتي يترتب على مخالفة أياً منها وجود خطأ مدني يثير مسؤولية المعالج المدنية، وتتمثل في الأمور الآتية:

١- 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.

٢- أن تكون أغراض المعالجة وممارستها مشروعة، ولا تخالف النظام العام أو الآداب العامة.

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

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

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

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

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

٨- عدم إلحاق أي ضرر بالشخص المعني بالبيانات بشكل مباشر أو غير مباشر.

٩- إعداد سجل خاص بعمليات المعالجة لديه، على أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسؤول حماية البيانات لديه، ووصفاً للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعملية المعالجة.

١٠- توفير الإمكانيات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز – أي مركز حماية البيانات الشخصية – من التفتيش والرقابة للتأكد من التزامه بذلك.

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

١٢- يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية، وذلك على النحو الذي تبينه اللائحة التنفيذية.

وللتأكيد على أهمية دور المعالج في مسألة حماية البيانات الشخصية، فقد قرر المشرع بنهاية المادة (٥) السابقة، حكماً مفاده أنه في حالة وجود أكثر من معالج، يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وذلك في حال عدم وجود عقد يحدد التزامات ومسئوليات كل منهم بوضوح.

ثانياً: تخلف التزامات المتحكم :

نص المشرع المصري في المادة (٤) من القانون رقم ١٥١ لسنة ٢٠٢٠، على مجموعة من الالتزامات على عاتق المتحكم، والتي يترتب على مخالفة أياً منها وجود خطأ مدني يثير مسؤولية المتحكم المدنية، وهي:

١- الحصول على البيانات الشخصية أو تلقيها من الحائز [١] أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانوناً.

٢- التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها.

٣- وضع طريقة وأسلوب ومعايير المعالجة طبقاً للغرض المحدد، ما لم يقرر تفويض المعالج في ذلك بموجب تعاقد مكتوب.

٤- التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها.

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

٦- 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.

٧- محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها. أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض، فيجب ألا تبقى في صورة تسمح بتحديد الشخص المعني بالبيانات.

---

[١] – الحائز هو أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليا ببيانات شخصية في أي صورة من الصور، أو علي أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة .... المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

٨- تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به.

٩- إمساك سجل خاص للبيانات، على أن يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات.

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

١١- يلتزم المتحكم خارج جمهورية العربية بتعيين ممثل له في جمهورية العربية وذلك على النحو الذي تبينه اللائحة التنفيذية.

١٢- توفير الإمكانيات اللازمة لإثبات التزامه بتطبيق إحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك.

وحرصاً من المشرع المصري في التأكيد على أهمية وخطورة دور المتحكم في حماية البيانات الشخصية، فقد أورد في ذيل المادة (٤) من القانون رقم ١٥١ لسنة ٢٠٢٠، مفاده أنه في حالة وجود أكثر من متحكم، يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعني ممارسة حقوقه تجاه كل متحكم على حدة.

ثالثاً: تخلف التزامات المسؤول عن حماية البيانات الشخصية:

لقد تفرد القانون المصري رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية، بوجود شخص يُعرف بالمسؤول عن حماية البيانات الشخصية. وتتمثل مهمة هذا الشخص في مسؤوليته عن تنفيذ أحكام هذا القانون

ولائحته التنفيذية وقرارات المركز، ومراقبة الإجراءات المعمول بها داخل كيانه والإشراف عليها، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقاً لأحكام هذا القانون [١].

ووضع المشرع المصري بموجب المادة (٩) من القانون رقم ١٥١ لسنة ٢٠٢٠ مجموعة من الالتزامات على عاتق المسؤول عن حماية البيانات الشخصية، بحيث يترتب على تخلف أياً منها، وجود خطأ مدني في حقه يثير مسؤوليته المدنية، والتي تتمثل في الأمور الآتية:

١- إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها.

٢- العمل كنقطة اتصال مباشرة مع المركز وتنفيذ قراراته، فيما يخص تطبيق أحكام هذا القانون.

٣- تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في هذا القانون.

٤- إخطار المركز في حال وجود أي خرق أو انتهاك للبيانات الشخصية لديه.

٥- الرد على الطلبات المقدمة من الشخص المعني بالبيانات أو كل ذي صفة، والرد على المركز في التظلمات المقدمة إليه من أي منهما وفقاً لأحكام هذا القانون.

[١] – المادة (٩) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

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

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

٨- تنظيم البرامج التدريبية اللازمة لموظفي كيانه، لتأهيلهم بما يتناسب مع متطلبات هذا القانون.

وأخيراً، يجدر بنا التنويه إلى أن الالتزامات سالفة الذكر، هي التزامات تقع على عاتق المسؤول عن عملية المعالجة قبل صاحب البيانات، أي من الممكن أن نسميها بالالتزامات الشخصية. وبالإضافة إلى هذه الالتزامات، فإن المسؤول عن المعالجة، يلتزم ببعض الالتزامات المهنية أو الموضوعية تجاه صاحب البيانات، والتي سنتعرض لها بمشيئة الله في الفصل الثاني من هذا البحث.

الفرع الخامس

معالجة البيانات الشخصية رغم عدم علم صاحبها أو رغم معارضته

لقد استلزم المشرع الفرنسي وكذلك المشرع المصري، ضرورة توافر موافقة صاحب البيانات الشخصية على معالجة بياناته، وجعل كل منهما هذا الأمر التزاماً يقع على عاتق المسؤول عن عملية المعالجة أو المتحكم لصالح صاحب البيانات؛ بقصد توفير الحماية اللازمة للحياة الخاصة للشخص على بياناته.

غير أن المشرعان الفرنسي والمصري، لم يستلزما هذا الضابط أو الالتزام على نحو الدوام، بل تغاضا عنه في بعض الأحيان لاعتبارات معينة سنتعرض

لها في حينه. وعلى ذلك سنتعرض للقاعدة العامة لهذا الالتزام (غصن أول)، ثم بعد ذلك للاستثناءات الواردة عليها (غصن ثان)، وذلك على النحو التالي[١]:

الغصن الأول

القاعدة العامة (وجوب رضاء صاحب البيانات الشخصية بعملية المعالجة)

سبق الذكر أن المشرع الفرنسي، استلزم توافر رضاء صاحب البيانات الشخصية بعملية المعالجة، وذلك في المادة السابعة من القانون رقم ٧٨ – ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات؛ فصاحب البيانات هو الذي يملك وحده حق التحكم في كل ما يتعلق ببياناته الشخصية من حيث جمعها أو حفظها أو

[1] - Art 53 , loi n° 78 – 17 Modifié par (LOI n°2018-493 du 20 juin 2018 - art. 19) " Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée, dans les conditions mentionnées au 11) de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée".

معالجتها بطريقة آلية وكذلك استخدامها، بصورة تحقق له أكبر قدر من السيطرة على بياناته [1].

وكذلك الأمر بالنسبة للمشرع المصري، الذي نص على هذا الأمر في المادة (٢) من القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية، بقولها :" لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانوناً ".

والأمر محل البحث، يقتضي منا التعرض لطبيعة الرضاء، وشروطه، ووقت صدوره من صاحب البيانات. وذلك على التوضيح الآتي:

أولاً– طبيعة رضاء صاحب البيانات الشخصية بعملية المعالجة: البيِّن من نص المادة السابعة، أن المشرع الفرنسي قد تطلب فقط مجرد رضاء الشخص بعملية المعالجة دون أن يتعرض صراحة لنوع أو طبيعة هذا الرضاء، وما إذا كان رضاءً صريحاً أم ضمنياً. لذلك، فكلاهما يصلح لأن يكون مظهراً يجوز به التعبير عن إرادة صاحب البيانات بالموافقة على المعالجة.

وترتيباً على ذلك، يجوز إجراء عملية معالجة البيانات الشخصية إذا توافر رضاء صاحب البيانات بذلك، يستوي أن يكون الرضاء صريحاً سواء بالفعل أو القول أو الإشارة، أو كان القبول ضمنياً على نحو يُستخلص من الظروف المحيطة بعملية المعالجة شريطة ألا يكون هناك ما يخلق أي لبس أو غموض

[1] - Fanny Rogue , Capacité et consentement au traitement de données à caractère personnel et au contrat , AJ contrat 2019, p.370.

بشأن توافر هذا الرضاء، وذلك على النحو الوارد في القواعد العامة لنظرية الالتزامات.

وتأييداً لذلك، لم تقر اللجنة الوطنية الفرنسية للمعلوماتية والحريات، سوى توافر رضاء الشخص فقط بعملية المعالجة، دون تحديد خاص لطبيعة هذا الرضاء. وهذا الرضاء أكدت على وجوده المواد الرابعة والسادسة والسابعة من اللائحة الأوربية رقم (٦٧٩) الصادرة في ٢٧ أبريل ٢٠١٦.

غير أن المشرع الفرنسي قد تطلب الموافقة الصريحة بعملية المعالجة في بعض الحالات، منها ما نصت عليه المادة (٣٣) من القانون رقم ٧٨– ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، والتي تفيد بأنه يلزم الموافقة الصريحة بالمعالجة إذا كانت هذه الأخيرة تتم من قبل مزودي خدمات التصديق الإلكتروني لغرض إصدار شهادات التصديق والحفاظ على التوقيعات الإلكترونية[١].

وعلى عكس موقف المشرع الفرنسي الذي ساوى بين الموافقة الصريحة والموافقة الضمنية لقانونية إجراء عملية معالجة البيانات الشخصية، نجد أن المشرع المصري قد استلزم الموافقة الصريحة في هذا الأمر، ولم يكتف بالموافقة الضمنية، وذلك على النحو المنصوص عليه صراحة في المادة (٢) آنفة الذكر.

---

[1] - Art 53 , loi n° 78 – 17 (Modifié par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004) " Sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par les prestataires de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies".

وقد اشترط المشرع الأوربي في لائحته رقم ٦٧٩ لسنة ٢٠١٦ في المادة السادسة ضرورة توافر الموافقة الصريحة بعملية المعالجة بما لا يُثار معه شك بشأن تلك الموافقة الصريحة. وعرفت المادة الرابعة من ذات اللائحة الأوربية، الموافقة بأنها:" كل إشارة تُعطى بحرية مستنيرة لا لبس فيها، تدل على رغبة أو موافقة صاحب البيانات المعدة للتجهيز على معالجتها " [١].

ثانياً– شروط الرضاء بعملية المعالجة: كما أن المشرع الفرنسي لم يتعرض صراحة لتحديد طبيعة الرضاء بعملية المعالجة، فإنه لم يتعرض أيضاً لشروط هذا الرضاء. فهذه الشروط يمكننا استخلاصها من التعريف الذي وضعته المادة الرابعة من اللائحة الأوربية رقم (٦٧٩) لسنة ٢٠١٦، للموافقة على معالجة البيانات، والتي تتمثل في الآتي:

* **يجب أن تكون هناك إرادة** تمكن الشخص من التعبير عن رضاه بالمعالجة، أي ألا يكون صاحب البيانات مصاب بعارض من عوارض الأهلية أو مانع من موانعها. وعلى ذلك إذا كان هذا الشخص عديم الأهلية أو ناقصها، وجب على المسؤول عن عملية المعالجة أن يحصل على رضاء ممثله القانوني. وهذا الأمر الأخير أكدته اللجنة الوطنية الفرنسية للمعلوماتية والحريات بضرورة الحصول على رضاء الممثل القانوني لأي شخص غير قادر على التعبير عن رضائه بمعالجة بياناته الشخصية [٢].

---

[1] - Art 4 of Regulation(EU) 2016/679 :" consent' of the data subject means any freely given , specific , informed and unambiguous indication of the data subject's wishes by which he or she , by a ststement or by a clear affirmative action , signifies agreement to the processing of personal data relating to him or her ".

[2] - C N I L : Internet et la collecte de données personnelles auprés des mineurs , rapport adopté le 21 juin 2001 , present par Mme Céile ALVERQNAT ……www.cnil.fr/.

*** يجب أن يكون الرضاء حر** [١]: ويعني ذلك خلو رضاء صاحب البيانات الشخصية من عيوب الإرادة المتمثلة في الغلط والتدليس والإكراه والغبن والاستغلال، على نحو يكون فيه هذا الرضاء بناءً على موافقة مستنيرة يصحبها علم بنتائج المعالجة.

*** يجب أن يكون الرضاء محدد:** ويعني ذلك حظر الرضاء العشوائي الذي يتضمن معالجة أي بيانات شخصية لصاحبها دون تحديد لهذه المعالجة في أي وقت وبأي صورة كانت دون مراعاة الضوابط السابقة. فلقد سبق الذكر أنه يلزم لمشروعية المعالجة أن يكون لها هدف محدد وواضح. فلا يجوز أن تكون هذه الموافقة ضمن بنود العقد العامة [٢]، بل يجب أن تكون بصورة منفصلة[٣].

ويعد الرضاء الواضح، امتداد مطلوب لضابط الهدف المحدد من المعالجة. أي أن الرضاء يجب أن ينصب على كل عملية من عمليات المعالجة بصورة مستقلة، حتى ولو انصب على كل إجراءات المعالجة مرة واحدة شريطة وحدة الهدف المبتغى من كل هذه الإجراءات. أما إذا تمت المعالجة لهدف غير الذي تم الحصول على رضاء الشخص بهذه المعالجة، افتقدت هذه الأخيرة ضابط موافقة الشخص عليها [٤].

---

[1] - Fanny Rogue , op. cit , p. 370.

[2] - Fanny Rogue , op. cit , p. 370.

[3]- Céline CASTETS-RENARD , La protection des données personnelles dans les relations internes à l'Union européenne – La protection des données personnelles en matière civile et commercial , Dalloz , Octobre 2018 (actualisation : Mai 2019) , N: 115.

[٤] – د/ سامح عبد الواحد التهامي، مرجع سابق، ص ٤٢٢، ٤٢٣.

ويحق لصاحب البيانات الشخصية أن يحتاط أكثر بخصوص مسألة موافقته على عملية المعالجة، بأن يشترط على المسؤول عن هذه العملية أن يأخذ موافقته على كل إجراء يخص إجراءات المعالجة ذات الهدف الواحد والمحدد. فلا ريب أن من حق كل شخص أن يشترط الحماية القانونية التي يراها مناسبة لتأمين بياناته والحفاظ عليها.

ثالثاً– وقت صدور الرضاء بمعالجة البيانات الشخصية: يجب أن يصدر رضاء الشخص بعملية المعالجة بصورة مسبقة، أي يلزم أن تسبق موافقة الشخص على معالجة بياناته البدء في المعالجة ذاتها [١]. فالغرض من هذا الضابط هو توفير الفعالية الحقيقية لحماية البيانات الشخصية؛ وذلك احتراماً لحقوق أصحابها عليها، فهم الذين يقررون السماح للمسؤولين عن المعالجات القيام بذلك. فإذا بادر المعالج بالحصول على موافقة الشخص بعد إجراء المعالجة، كانت المعالجة غير مشروعة، ومن ثم تثير مسؤولية المعالج المدنية.

وحاصل ما تقدم، أنه يلزم توافر الضوابط السابقة في مسألة الموافقة على عملية المعالجة، وخصوصاً أنه بمجرد تسجيل البيانات الشخصية على أي موقع أو مكان فإنها تحقق مصداقية عالية عن الشخص المعني بها. وما يؤيد ذلك أن التطور السريع للتقنيات التي تستخدمها الحكومات والشركات، كثيراً ما تقوم بتجميع ومعالجة البيانات الشخصية دون الأخذ في الاعتبار موافقة صاحبها، كالتجميع الروتيني لبيانات التعامل الإلكترونية، والمراقبة الآلية المتزايدة في الأماكن العامة والمرتبطة بالإنترنت، وتقنية التعرف على الوجه، والقياسات الحيوية، وتقنية تعقب الهواتف المحمولة وتعقب السيارات، والمراقبة من خلال الأقمار الصناعية، ومراقبة أماكن العمل، والتعقب في الإنترنت عبر برامج

[1] - Fanny Rogue , op. cit , p. 370 ؛ Hugues Ciray , Du contrôle d'un systéme de traitment automatisé de données personnelles , 2 juillet 2018 , Dalloz actualité , 2 juillet 2018.

الكوكيز وبيانات النقر – كما شرحنا ذلك سابقاً – . فكل هذه الأمور تتجاهل في الكثير من الأحيان الحصول على رضاء الأفراد بجمع ومعالجة بياناتهم الشخصية [١].

الغصن الثاني

حالات عدم اشتراط الرضاء لقانونية معالجة البيانات الشخصية

على الرغم من أن المشرع الفرنسي قد تطلب ضرورة موافقة الشخص على معالجة بياناته الشخصية، سواء كان ذلك بصورة صريحة أو ضمنية، إلا أنه استثني بنص المادة السابعة من القانون رقم ٧٨– ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات بعض المعالجات من هذا القيد [٢]. وتتمثل هذه الحالات المستثناة في الآتي:

---

[١] – د/ وليد السيد سليم، مرجع سابق، ص ٢١٨، ٢٢٠.

[2] - Art 53 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 19) :" Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée, dans les conditions mentionnées au 11) de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la

أولاً– إذا كانت عملية المعالجة تُجرى تنفيذاً لالتزام قانوني: في هذه الحالة يقع على عاتق المعالج التزاماً بنص القانون يوجب عليه ضرورة إجراء المعالجة. ويلزم لإعفاء المعالج من الحصول على موافقة صاحب البيانات، أن يكون مصدر التزام المعالج هو نص القانون، فإن كان غير ذلك وجب الرجوع إلى القاعدة العامة سابقة البيان. كمان أن هذا الالتزام وفقاً لصريح نص المادة السابعة، قاصر على المسؤول عن عملية المعالجة دون صاحب البيانات محل المعالجة.

وتتمثل الحكمة من هذا الاستثناء، في أن عدم تعليق المعالجة هنا على الحصول على موافقة صاحب البيانات يكون بناءً على نص قانوني. وهذا الأخير يلتزم الجميع باحترامه سواء كانوا أصحاب بيانات تخضع للمعالجة أم مسؤولين عن عمليات المعالجة ذاتها. بالإضافة إلى أن هذا الاستثناء القانوني دائماً ما يكون لمبررات قوية ومشروعة تبرر الحيد عن القاعدة العامة، وهذه المبررات دائماً ما تعلو حق الأفراد في أن تُعلق المعالجة على موافقتهم.

ثانياً– إذا كانت عملية المعالجة تتم بغرض الحفاظ على حياة الشخص المعني بمعالجة بياناته الشخصية: ومبرر هذا الاستثناء هو النزول على حالة الضرورة التي يكون فيها الشخص ولا تسمح بالحصول على موافقته بمعالجة بياناته، أو كانت حالته تسمح بذلك غير أن الرفض سيضر به. لذلك أجاز المشرع الفرنسي حدوث المعالجة بصرف النظر عن موافقة صاحب البيانات.

ومن أمثلة هذا الاستثناء، معالجة بيانات شخص يحتاج لتدخل جراحي ضروري، يترتب على التأخير فيه وفاته أو إصابته بضرر جسيم. وكذلك عمليات المعالجة التي تتم بقصد حصر المصابين بمرض انتشر في مكان

---

personne concernée".

معين. فيمكن تأسيس هذا الاستثناء على القاعدة القاضية بأن الضرورات تبيح المحظورات.

ثالثاً– إجراء عملية المعالجة تنفيذاً لمهمة عامة يتولاها الشخص المسؤول عن المعالجة أو متلقي المعالجة: وفي هذا الاستثناء، يقع على عاتق المسؤول إجراء المعالجة دون أن يتوقف ذلك على موافقة صاحب البيانات، إذا كان الأمر يتعلق بالصالح العام وكان هذا المسؤول يتولى هذا الأمر الذي بسببه أُجريت المعالجة. أي أن وظيفة القائم بالمعالجة تحتم عليه إجراء هذه المعالجة، كما لو تعلق الأمر بالمعالجات اللازمة لسير المرافق العامة في الدولة كمرفق الاتصالات أو الغاز الطبيعي أو الكهرباء.

رابعاً– إذا كانت المعالجة لتنفيذ عقد كان صاحب البيانات محل المعالجة طرفاً فيه: ويعني هذا الاستثناء أن صاحب البيانات قد أبرم عقداً مع شخص، وكان من مستلزمات اتمام هذا العقد إجراء معالجة لبيانات هذا المتعاقد. فهنا يحق للمتعاقد الآخر – أي الطرف الثاني في العقد – أن يعالج بيانات الطرف الأول بهدف تنفيذ العقد محل الإبرام بينهما دون الحصول على موافقة صاحب البيانات بعملية المعالجة [١].

فعلى سبيل المثال، من يتعاقد مع شركة الغاز الطبيعي على توصيل الغاز لمنزله، فإن هذه الشركة تتطلب من هذا الشخص بعض البيانات الشخصية، والتي يحق لها معالجتها بمقتضي العقد المبرم بينهما بهدف تنفيذه. ويُقاس على ذلك أي عقد يكون صاحب البيانات طرفاً فيه دون تفرقة بين عقد وآخر.

[١] – د/ سامح عبد الواحد التهامي، مرجع سابق، ص ٤٢٥.

وجدير بالذكر، أن هذا الاستثناء كما ينطبق على العقد خلال إبرامه وتنفيذه، فإنه ينطبق كذلك على الإجراءات التي تسبق إبرام العقد، بشرط أن تكون عملية المعالجة مرتبطة بهذه الإجراءات، أي لها علاقة بها وغير منفصلة عنها. وهو ما يجد مجاله الرحب في المعاملات الإلكترونية التي تقدم أو تُبرم من خلال الإنترنت، كالإجراءات الخاصة بتسجيل الطلبات أو الاشتراكات المقدمة من العملاء [١].

خامساً– إذا كان الغرض من عملية المعالجة، تحقيق مصلحة مشروعة للمسؤول عن المعالجة أو لمتلقي البيانات: وفي هذه الحالة، ونزولاً على مشروعية المصلحة من المعالجة، سواء كان ذلك للمعالج أو لمتلقي البيانات، جاز له إجراء المعالجة شريطة مراعاة المصالح أو الحقوق الأساسية لصاحب البيانات.

والحقيقة أن بإقرار المشرع الفرنسي لهذا الاستثناء، فإنه قد انقص من الضمانات المبتغاة لحماية البيانات الشخصية وأهمية موافقة صاحبها على معالجتها؛ لأنه لم يضع معياراً محدداً منضبطاً يوضح حدود ونطاق إعمال هذا الاستثناء الذي يعد مصادرة على ضرورة تطلب موافقة صاحب البيانات بالمعالجة دون تحديد يحول دون وجود تعسف أو استغلال هذا الأمر.

غير أنه يمكن الحد من الانتقاد السابق عن طريق إعمال التوازن بين مصلحة القائم بعملية المعالجة وبين مصلحة من تُعالج بياناته، وذلك من خلال السلطات القانونية التي أعطاها المشرع الفرنسي للجنة الوطنية الفرنسية

[1] - FERAL-SCHUHL , Cyber droit , le droit ā l’épreuve de l’internet , Dalloz , paris , 2000 , p. 100et s.

للمعلوماتية والحريات، وكذلك القضاء صاحب السلطة العليا في الرقابة على مدى تحقق هذا التوازن على نحو يضمن لكل طرف مصلحته وحقوقه [١].

وبالنسبة لموقف المشرع المصري من الاستثناءات محل الحديث، نجد أنه على الرغم من تطلبه الموافقة الصريحة لصحة القيام بمعالجة البيانات الشخصية، نجد أنه لم يستلزم أي موافقة من صاحب البيانات بالنسبة لبعض المعالجات، التي ورد النص عليها في المادة الثالثة من القانون رقم ١٥١ لسنة ٢٠٢٠، والتي تتمثل في الآتي:

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

٢- البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقاً لنص قانوني.

٣- البيانات الشخصية التي تتم معالجتها حصراً للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تُستخدم في أي أغراض أخرى، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام.

٤- البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية.

٥- البيانات الشخصية لدى جهات الأمن القومي، وما تقدره لاعتبارات أخرى. ويجب على المركز، بناءً على طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات

[١] – د/ سامح عبد الواحد التهامي، مرجع سابق، ص ٤٢٦.

الشخصية، خلال مدة زمنية محددة، وفقاً لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة.

٦- البيانات الشخصية لدى البنك المركزي والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة، على أن يُراعى في شأنهما القواعد المقررة من البنك المركزي المصري بشأن التعامل مع البيانات الشخصية.

وإجمالاً لما تقدم في هذا المبحث، فإن عدم مشروعية معالجة البيانات الشخصية والذي يعد خطأً مدنياً حال حدوثه، يتخذ العديد من المظاهر: كعدم تحديد الهدف من عملية المعالجة، وعدم وضوحه، وتخلف الالتزامات الشخصية الملقاة على عاتق المعالج قبل صاحب هذه البيانات، وعدم مشروعية الهدف من المعالجة، وحدوث المعالجة رغم عدم علم أو معارضة صاحب البيانات.

وما سبق ذكره ينطبق على كل من المعالجة الآلية للبيانات الشخصية والمعالجة اليدوية [١]:

أ- <u>المعالجة اليدوية</u>: وهي التي تكون عن طريق وضع البيانات الشخصية وتصنيفها في ملفات ورقية عادية وجمعها في ملف واحد، دون استخدام أي برامج إلكترونية [٢].

---

[1] - Art 2 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 9) :" La présente loi s'applique aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5…… ".

[٢] – د/ سامح عبد الواحد التهامي، مرجع سابق، ص ٤١٢.

ب- المعالجة الآلية: وهي المعالجة التي لا تكون إلا للملفات أو البطاقات. وعرفتها المادة الثانية من القانون رقم ٧٨- ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، بأنها:" جميع البيانات الشخصية المنظمة والثابتة للشخص ويمكن الدخول إليها وفقاً لمعايير محددة على نحو يسمح بالتعرف على شخص معين" [١]. ولا يُؤخذ في الاعتبار في هذه المعالجة، نوع الدعامة أو الوسيلة الفنية التي تكون عليها البيانات محل المعالجة. فكل ما يهم هو قابلية هذه البيانات للظهور في شكل ملفات.

المبحث الثالث

الخطأ المدني الناشئ عن مخالفة ضوابط معالجة البيانات الشخصية ذات الطابع الخاص شخصياً وأمنياً

- تقسيم:

وضحنا في المبحث السابق، حالات الخطأ المدني للمسؤول عن عملية المعالجة؛ لإخلاله بالضوابط اللازمة لمشروعية عملية معالجة البيانات الشخصية، وذلك إذا لم يكن لعملية المعالجة هدف محدد وواضح ومشروع، وإذا تمت المعالجة بدون موافقة صاحب البيانات، بالإضافة إلى الخطأ المعالج الناشئ عن الإخلال ببعض الالتزامات الشخصية قبل صاحب البيانات. وهذه الضوابط وفقاً للأصل العام، تنطبق على جميع عمليات المعالجة، ما لم يُستثن من ذلك بنصوص صريحة غير قابلة للافتراض.

[1] - Art 2 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 9) :" Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères determines……..".

غير أنه واستثناءً على الأصل المتقدم، نجد أن هناك فئة من البيانات الشخصية تتمتع بنوع من الخصوصية القانونية فيما يتعلق بمعالجتها، أي أنها لا تخضع في هذه المعالجة للضوابط التي ذكرناها سلفاً. وتندرج هذه البيانات تحت نوعين هما: البيانات ذات الطابع الخاص على المستوى الشخصي، والبيانات ذات الطابع الخاص على المستوى الأمني والجنائي. وعلى ذلك، نتعرض لدراسة هذا المبحث من خلال مطلبين هما:

المطلب الأول: الخطأ المدني الناشئ عن مخالفة ضوابط معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الشخصي.

المطلب الثاني: الخطأ المدني الناشئ عن مخالفة ضوابط معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الأمني والجنائي.

المطلب الأول

الخطأ المدني الناشئ عن مخالفة ضوابط معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الشخصي

سنتناول في هذا المطلب القاعدة العامة بشأن حظر معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الشخصي (فرع أول)، والاستثناءات الواردة على هذه القاعدة (فرع ثان)، وذلك على العرض التالي:

الفرع الأول

القاعدة العامة بشأن حظر معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الشخصي

يُقصد بهذه الفئة من البيانات، تلك ذات الطابع الحساس التي تمس الحياة الاجتماعية والصحية للفرد ومعتقداته الديبنية وآرائه السياسية وانتمائاته النقابية وكذلك أصوله العرقية والجنسية.

والبيانات الشخصية ذات الطابع الحساس عرفها المشرع المصري في المادة (١) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، بأنها البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية " البيومترية " أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة.

وبسبب خصوصية وخطورة النتائج المترتبة على معالجة هذه الفئة من البيانات، فقد حظر كل من المشرع الفرنسي والمشرع المصري واللائحة الأوربية معالجة تلك الفئة من البيانات:

١- بالنسبة للحظر التشريعي في القانون الفرنسي: جاء النص على حظر معالجة تلك البيانات في المادة الثامنة من القانون رقم ٧٨- ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، والتي نصت على أنه:" يُحظر جمع أو معالجة البيانات الشخصية التي تكشف بشكل مباشر أو غير مباشر عن

الأصول العرقية أو الجنسية أو الآراء السياسية أو الفلسفية أو الدينية أو الإنتماءات النقابية للأشخاص، أو التي تتعلق بحالتهم الجنسية أو الصحية " [١].

٢- بالنسبة للحظر التشريعي في القانون المصري: ورد الحظر التشريعي لمعالجة البيانات الشخصية ذات الطابع الحساس في قانون حماية البيانات الشخصية المصري في المادة (١٢) منه، والتي اشترطت لصحة معالجة هذه البيانات ضرورة وجود ترخيص من مركز حماية البيانات الشخصية للمتحكم أو المعالج بذلك، بالإضافة إلى الموافقة الصريحة المكتوبة من الشخص الذي تخصه البيانات محل المعالجة، باستثناء الحالات التي لم يشترط فيها القانون مثل هذه الموافقة.

حيث نصت المادة المذكورة على أنه:" يُحظر على المتحكم أو المعالج سواء كان شخصاً طبيعياً أو اعتبارياً، جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز. وفيما عدا الأحوال المصرح بها قانوناً، يلزم الحصول على موافقة كتابية صريحة من الشخص المعني. وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر. ويجب ألا تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر مشروطة بتقديم بيانات شخصية للطفل تزيد عما هو ضروري للمشاركة في ذلك ".

---

[1] - Art 8/I , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" I. - Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique…..".

٣- بالنسبة للحظر التشريعي في اللائحة الأوربية: فقد نصت المادة (١/٩) من اللائحة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ على أنه:" يُحظر على الدول الأعضاء معالجة البيانات الشخصية التي تكشف عن الأصول العرقية أو الجنسية أو الآراء السياسية أو المعتقدات الدينية للأشخاص أو الفلسفية أو الإنتماءات النقابية للعمال أو البيانات الجينية والبيومترية أو تلك المتعلقة بالصحة أو بالحياة الجنسية للشخص الطبيعي أو جنسه، بغرض التعرف على هذا الشخص بشكل متفرد " [١].

وتختلف العلة من حظر معالجة الفئات السابقة من البيانات الشخصية، باختلاف نوع البيان محل الحظر، كالتالي:

١- الحكمة من حظر معالجة البيانات الشخصية المتعلقة بالأصول العرقية أو الجنسية للشخص: تتمثل هذه الحكمة في أنه يترتب على السماح بمعالجتها وجود العديد من قضايا التمييز العنصري بين أفراد المجتمعات [٢]، على نحو قد يثير الضغينة والكراهية والفتن بين أبناء هذه المجتمعات، وخصوصاً في المجتمعات التي تتكون من سلالات عرقية مختلفة كالمجتمع الأمريكي.

فجميع أشكال التمييز العنصري تتعارض مع ما تنادي به المجتمعات الحديثة في شتى بقاع الأرض من ضرورة احترام حقوق الإنسان، وما تتضمنه

---

[1] - Art 9 of Regulation (EU) 2016/679 :"1- Processing of personal data revealing racial or origin , political opinions , religious or philosophical beliefs , or trade union membership , and the processing of genetic data , biometric data for the purpose of uniquely identifying a natural person , data concerning health or data concerning a natural person's sex orientation shall be prohibited ".

[2] - Céline CASTETS. RENARD , op.cit , N: 41.

الدساتير المختلفة من المساواة بين الأفراد بصورة مجردة من التعويل على أصولهم العرقية أو الجنسية.

وتأييداً للعلة المتقدمة من الحظر، فقد رأت اللجنة الوطنية الفرنسية للمعلوماتية والحريات، عدم جواز الدراسة البحثية التي أجراها أحد المراكز الصحية من أجل القيام بعملية مسح وبائي بخصوص الحالات المرضية والوفيات بسبب الحوادث في بعض الدول الأوربية والأفريقية؛ تأسيساً على أن هذا الأمر يتعارض مع حظر معالجة مثل هذه الفئة من البيانات الشخصية التي تؤدي عملية معالجتها إلى وجود تمييز عنصري [١].

٢- الحكمة من حظر معالجة البيانات الخاصة بالمعتقدات الدينية أو السياسية أو الفلسفية أو الانتماءات النقابية: لاشك أن الأمور السابقة هي من الأشياء الخاصة التي قد يفضل الفرد عدم إخبار الغير بها أو السماح باطلاعه عليها؛ لأن معرفتها في الغالب ستؤدي إلى خلق تصور عام حول شخصية الفرد المعني بهذه البيانات، أو رسم صورة كاملة عنه تكون ظاهرة للغير على نحو قد يأباه صاحب هذه البيانات.

وتعد المعتقدات الدينية والسياسية في هذه الفترات الثورية التي يشهدها العالم من أخطر البيانات الشخصية مدعاةً للعنف وخلقاً الكراهية. فعلى سبيل المثال، نجد أن معالجة بيان الحالة الدينية لشخص مسلم في بعض المجتمعات الغربية المتشددة بشأن الإسلام، قد يضر به ضرراً جسيماً، وهو ما نلاحظه في هذه الآونة. وكذلك الأمر بالنسبة للمعتقدات أو الآراء السياسية، التي أصبحت سبباً كبيراً للخلاف والشقاق بين الكثير من الأفراد في معظم المجتمعات. لذلك فحظر معالجة هذه البيانات له من الأهمية ما لا يُنكر.

---

[1] - C N I L : 6 éme rapport d'activité , 1985 , La documentation Française , paris , 1986 , p. 95.

وتطبيقاً لذلك، قضت محكمة النقض الفرنسية بدائرتها المدنية الأولى، بأن انتماء الشخص إلى الدين الكاثوليكي يعتبر من البيانات المتعلقة بحياته الخاصة، ويعتبر كذلك التعميد الخاص به، ولا تجوز معالجته [١].

٣- الحكمة من حظر معالجة البيانات الخاصة بالحالة الصحية للفرد:

تتمثل هذه الحكمة في أن هذه البيانات تمس صميم خصوصية صاحبها، وأن معالجتها كغيرها من البيانات فيه تعدي صريح وواضح على كرامته الإنسانية. فأسرار المريض يلتزم بها الطبيب المعالج، ولا يحق له إفشاءها وإلا تعرض للمسؤولية. فإذا كان ذلك بالنسبة لمن يعالج الشخص، فما بالنا بعملية معالجة هذه البيانات من الأساس!

وفي هذا الصدد، نجد أن المشرع المصري قد أحسن صنعاً عندما اشترط صراحة في نص المادة (١٢) من القانون رقم ١٥١ لسنة ٢٠٢٠ موافقة ولي الأمر في أي إجراء يتطلب ذكر بيانات شخصية حساسة عن الطفل، وتقييد الأطفال بذكر بيانات شخصية حساسة بصورة محدودة حال اشتراكهم في لعبة أو مسابقة تتطلب إفصاحاً عن هذه البيانات. ويرجع هذا الأمر إلى تطور وخطورة الألعاب الموجودة على الشبكة العنكبوتية، والتي غالباً ما يتطلب مبرمجوها ضرورة الإفصاح عن الكثير من البيانات الشخصية الحساسة للأطفال، الذين لا يلقون بالاً ولا أهمية في الإفصاح عنها، ثم تكون النتيجة بعد ذلك، توافر هذه البيانات واعتبارها صيداً سهلاً لدى أصحاب المواقع الإلكترونية مما قد يضر بالأطفال الذي يفصحون عن هذه الفئة من البيانات، مما يجعلهم عرضة للتنمر الاجتماعي في بعض الأحيان.

[1] - Cass. Civ , chamber civile 1 , 19 november 2014 , No: 13-25156.

الفرع الثاني

الاستثناءات التشريعية الواردة على القاعدة العامة الخاصة بحظر معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الشخصي

إذا كان المشرع الفرنسي قد حظر معالجة البيانات الشخصية للفئات السابقة كأصل عام، إلا أنه أورد عدة استثناءات على هذا الأصل، بأن سمح بإجراء عملية المعالجة لهذه الطائفة من البيانات ذات الطابع الخاص في بعض الحالات، وذلك بنص المادة الثامنة من القانون رقم ٧٨–١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات. وتتمثل هذه الاستثناءات في الآتي:

١– حالة المعالجة التي تتم بموجب الموافقة الصريحة للشخص صاحب البيانات محل المعالجة، مالم يوجد نص قانوني يقضي بعدم المعالجة حتى مع وجود هذه الموافقة[١]: فكما سبق الذكر أن الحكمة من حظر معالجة البيانات محل الحديث، هي إما منع حدوث تمييز عنصري أو نشوء ضغائن بين الأفراد، وإما المحافظة على الكرامة الإنسانية لكل فرد. وفي الحالتين يتعلق أمر الحظر بإرادة صاحب الشأن المقرر الحظر لمصلحته، والذي يحق له التنازل عن ذلك بالسماح بإجراء المعالجة ولكن بشرطين:

[1] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée….".

أ- توافر الموافقة الصريحة بعملية المعالجة، فلا تكفي هنا مجرد الموافقة الضمنية من صاحب الشأن.

ب- ضرورة عدم وجود نص قانوني يقضي بحظر عملية المعالجة – أي الرجوع إلى الأصل العام – حتى مع توافر الموافقة الصريحة؛ وذلك لاعتبارات يقدرها المشرع. ويمثل ذلك استثناءً على استثناء بما يمثل رجوع إلى القاعدة العامة ألا وهي الحظر.

وهذا الاستثناء أكدته اللائحة الأوربية رقم ٦٧٩ لسنة ٢٠١٦، وذلك في المادة (٢/٩)، التي نصت على أنه:" لا ينطبق الحظر الخاص بالبيانات الشخصية الواردة بالفقرة الأولى، إذا أعطى صاحب البيانات موافقة صريحة على معالجة تلك البيانات " [١].

٢- حالة ما إذا كانت عملية المعالجة ضرورية ولازمة للحفاظ على حياة الإنسان [٢]: وهنا أجاز المشرع الفرنسي إجراء المعالجة للحفاظ على حياة صاحب البيانات إذا كان لا يستطيع إبداء موافقته بسبب عجزه القانوني أو لوجود استحالة مادية في التعبير عن هذه الموافقة. وهنا تأتي مخالفة الحظر المتقدم بسبب حتمية المعالجات حفاظاً على حياة الشخص.

---

[1] - Art 9 of Regulation (EU) 2016/679 :" 2- Paraghraph 1 shall not apply if one of the following applies : (a)- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes , except …".

[2] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I: 2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle …."

٣- حالة المعالجات التي تنفذها الجمعيات أو المنظمات الأخرى ذات الطابع الديني أو الفلسفي أو السياسي أو النقابي [١]: وهنا أجاز المشرع الفرنسي مخالفة الحظر المتقدم بعدة ضوابط تمنع الحيد عن العلة من الاستثناء في هذا الفرض، والتي تتمثل في الشروط الآتية:

أ- ضرورة ألا تكون الجمعيات أو المنظمات الأخرى التي تقوم بعملية معالجة الفئات محل الحظر، تهدف إلى تحقيق الربح، فإن كانت تهدف إليه انتفت الحكمة من الاستثناء. وتظهر الصفة غير الربحية من خلال الطابع الديني أو الفلسفي أو السياسي أو النقابي لعملية المعالجة. فهذه معالجة تحدث إما لتثقيف الناس وإما لتوعيتهم دون تحقيق أي ربح.

ب- ضرورة وجود تناسب بين البيانات الشخصية الخاضعة للمعالجة، وبين الغرض من الجمعية أو الهيئة: وهذا الشرط ما هو إلا تأكيد لضابط ملائمة البيانات وعدم تجاوزها للغرض من معالجتها. فعلى سبيل المثال إذا كان الغرض من المعالجة ديني فلا يجوز أن يكون له بعد سياسي والعكس صحيح. أي أنه

[1] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 3° Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :

- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;

- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;

- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément

في جميع الأحوال يلزم أن تتقيد عملية المعالجة بالهدف الذي ترمي إليه الجمعية أو الهيئة.

ج- يلزم أن تكون عملية معالجة الفئات السابقة قاصرة فقط على معالجة البيانات الخاصة بأعضاء الجمعية أو الهيئة، وكذلك الأشخاص الذين تربطهم بالجمعية أو الهيئة علاقة عقدية مشروعة تتصل بأنشطتهم [١].

د- يجب أن تقتصر المعالجة على البيانات غير المعروفة لدى الآخرين، مالم يكن هناك رضاء صريح من الأشخاص الخاضعة بياناتهم للمعالجة بذلك.

٤- حالة المعالجة التي يكون محلها بيانات تخص الشخص، وقد أفصح عنها بنفسه قبل ذلك [٢]: فهنا الحكمة من حظر عملية المعالجة لم تعد موجودة؛ لأن ما يخضع للمعالجة أصبح معلوماً للناس بفعل صاحب البيانات. كما أن معالجة تلك البيانات يمكن اعتبارها بمثابة رضاء ضمني منه بذلك. غير أنه ينبغي ملاحظة أن مخالفة الحظر في هذه الحالة تقتصر على البيانات التي يكون صاحبها قد أفصح عنها، أما تلك التي لم يفصح عنها فنرجع في إعمال معالجتها للحظر السابق ذكره.

٥- حالة المعالجات اللازمة لإثبات حق أو الدفاع عنه أمام العدالة: فأحياناً يكون من دواعي إثبات حق متنازع عليه، ضرورة إجراء معالجة لبيان

---

[١] – د/ شريف خاطر، حق الاطلاع على البيانات الشخصية في فرنسا، بحث منشور في مجلة القانون الكويتية العالمية، العدد التاسع، السنة الثالثة، مارس ٢٠١٥، ص ٣١١.

[2] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I: 4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée".

شخصي أو أكثر يخص أحد المتنازعين أو كلاهما، ونفس الحكم في حالة ممارسة حق قضائي معين [١].

٦- حالة المعالجات التي تتطلبها أنشطة الطب الوقائي وحالات التشخيص الطبي وتوفير الرعاية أو العلاج أو إدارة الخدمات الصحية وتنفيذها عن طريق عضو يعمل في المهن الصحية أو من قبل شخص آخر يقع على عاتقه التزام بالمحافظة على السر المهني إعمالاً لما هو وارد بالمادة ١٣/٢٢٦ من قانون العقوبات [٢].

٧- حالة المعالجات التي تُجرى بمعرفة المعهد الوطني للإحصاء والدراسات الإقتصادية أو إحدى الدوائر الإحصائية الوزارية وفقاً للقانون رقم ٥١-٧١١ المؤرخ في ٧ يونيو لسنة ١٩٥١، بشأن الالتزام والتنسيق والسرية في الإحصاءات، بعد أخذ رأي المجلس الوطني للمعلومات الإحصائية [٣].

---

[1] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice".

[2] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I: 6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ".

[3] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I: 7° Les traitements statistiques réalisés par

٨- حالة المعالجات اللازمة في الأبحاث الخاصة بمجال الصحة، على النحو المنصوص عليه في الفصل التاسع من هذا القانون [١].

٩- حالة المعالجات التي يقوم بتنفيذها أصحاب العمل أو الإدارات، وذلك فيما يتعلق بالبيانات البيومترية اللازمة لمراقبة الوصول إلى أماكن العمل، وكذلك الأجهزة والتطبيقات المستخدمة في المهام المعهود بها إلى الموظفين أو الوكلاء أو المتدربين أو مقدمي الخدمات [٢].

١٠- حالة المعالجة الخاصة بإعادة استخدام المعلومات العامة الواردة في الأحكام والقرارات المذكورة في المادة العاشرة من قانون العدالة الإدارية، والمادة

---

l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique ".

[1] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I: 8° Les traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX de la présente loi ".

[2] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 9° Les traitements conformes aux règlements types mentionnés au b du 2° du I de l'article 11 mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires ".

(١٣/١١١) من قانون التنظيم القضائي، بشرط ألا يكون القصد من هذه المعالجة هو إعادة تحديد هوية الأشخاص المعنيين [١].

١١- حالة المعالجات اللازمة للبحوث العامة بالمعنى الذي تقصده المادة (١/١١٢) من قانون البحوث، والتي تنفذ بموجب الشروط المنصوص عليها في المادة (٢/٩) من لائحة الاتحاد الأوربي رقم ٦٧٩ لسنة ٢٠١٦ المؤرخة في ٢٧ أبريل ٢٠١٦، وذلك تبعاً لرأي معلن ومنشور من اللجنة الوطنية للمعلوماتية والحريات وفقاً لأحكام المادة (٢٨) من هذا القانون [٢].

وفي هذا الصدد يجب ملاحظة أيضاً أن الحظر المشار إليه لا ينطبق في حالتين أخريين هما:

---

[1] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 10° Les traitements portant sur la réutilisation des informations publiques figurant dans les jugements et décisions mentionnés, respectivement, à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées ".

[2] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 11° Les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, mis en œuvre dans les conditions prévues au 2 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, après avis motivé et publié de la Commission nationale de l'informatique et des libertés rendu selon les modalités prévues à l'article 28 de la présente loi".

أ- إذا كانت البيانات الشخصية التي ينطبق عليها الحظر، قد تم الحصول عليها لتكون وسيلة لإخفاء الهوية المعترف بها سابقاً وفقاً لأحكام هذا القانون من قبل اللجنة الوطنية للمعلومات والحريات [١].

ب- كما أنه لا يخضع للحظر السابق، المعالجة الآلية أو غيرها التي تبررها المصلحة العامة وأُذن لها – أي بالمعالجة – وفقاً للشروط المنصوص عليها في المادة (٢٦) من هذا القانون[٢].

وبالنسبة لموقف المشرع المصري من الاستثناءات الواردة على القاعدة العامة الخاصة بحظر معالجة البيانات الشخصية الحساسة، نجد أنه قد أورد في ذلك عدة استثناءات في المادة الثالثة من القانون رقم ١٥١ لسنة ٢٠٢٠، والتي سبق وأن تعرضنا لها في الحالات التي لا يُشترط فيها تطلب الرضاء لقانونية معالجة البيانات الشخصية، وسنحيل إليها في ذلك منعاً للتكرار [٣].

وترتيباً على ما تقدم، فإن عملية المعالجة في هذا المقام تشكل خطأً مدنياً ومن ثم تثير المسؤولية المدنية للمسؤول عن المعالجة، إذا حدثت عملية معالجة

---

[1] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" III. - N'entrent pas dans le champ de l'interdiction prévue au I les données à caractère personnel mentionnées au même I qui sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés".

[2] - Art 8/II , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8):" IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au II de l'article 26".

[٣] – أنظر في هذه الحالات المستثناة ص ٧٤، ٧٥.

لبيانات شخصية تتعلق بالأصول العرقية أو الجنسية أو كانت تخص الآراء السياسية أو الفلسفية أو الدينية أو الانتماءات النقابية للأشخاص، أو كانت تتعلق بالحالة الصحية أو الحياة الجنسية لهم. كل ذلك ما لم تكن هناك موافقة صريحة من صاحب البيانات بالمعالجة، أو توافر في حق القائم بعملية المعالجة استثناء من الاستثناءات التي ذكرناه تفصيلاً أعلاه.

المطلب الثاني

الخطأ المدني الناشئ عن مخالفة ضوابط معالجة البيانات الشخصية ذات الطابع الخاص على المستوى الأمني والجنائي

ذكرنا في المطلب السابق أن كل من المشرع المصري والمشرع الفرنسي، قد أسبغ نوعاً من الخصوصية فيما يتعلق بمعالجة بعض الفئات الخاصة بالبيانات الشخصية، وذكرنا بعضها في المطلب السابق. وفي هذا المطلب أيضاً، سنجد أن المشرع الفرنسي قد استثنى طائفة أخرى من البيانات، وهي التي تتعلق بمعالجة البيانات الخاصة بالجرائم والإدانات والتدابير الأمنية. فبموجب المادة التاسعة من القانون رقم ٧٨–١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، قصر المشرع معالجة تلك البيانات على الفئات الآتية [1]:

[1] - Art 9 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 13):" Les traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peuvent être effectués que [dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2018-765 DC du 12 juin 2018.] par :

1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ainsi que les personnes morales de droit privé collaborant au service public de la justice et appartenant à des

أ- المحاكم والسلطات العامة والشخصيات الاعتبارية التي تدير خدمة عامة وتعمل في إطار صلاحياتها القانونية. وكذلك الكيانات القانونية للقانون الخاص التي تتعاون في أداء الخدمة العامة للعدالة والتي تنتمي إلى فئات محددة بقوائمها بمقتضى مرسوم صادر عن المجلس الوطني للإحصاء، وذلك بعد رأي معلن ومنشور من اللجنة الوطنية للمعلوماتية والحريات، وذلك بما يتناسب والقدر اللازم الضروري للقيام بمهامها.

ب- معاوني القضاء، وذلك في إطار تلبية الاحتياجات اللازمة لممارسة المهام الموكولة إليهم بموجب القانون.

---

catégories dont la liste est fixée par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, dans la mesure strictement nécessaire à leur mission ;

2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

3° Les personnes physiques ou morales, aux fins de leur permettre de préparer et, le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci et de faire exécuter la décision rendue, pour une durée strictement proportionnée à ces finalités. La communication à un tiers n'est alors possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite de ces mêmes finalités ;

4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits ;

5° Les réutilisateurs des informations publiques figurant dans les jugements mentionnés à l'article L. 10 du code de justice administrative et les décisions mentionnées à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées".

ج- الأشخاص الطبيعيون أو الاعتباريون من أجل تمكينهم من الاستعداد وعند اللزوم لممارسة ومتابعة إجراء قانوني كجناة أو مجني عليهم أو نيابة عن هؤلاء من أجل انفاذ القرار الصادر لمدة تتناسب مع تلك الأغراض.

د- الأشخاص الاعتباريون المذكورون في المادتين (١/٣٢١ ، ١/٣٣١) من قانون الملكية الفكرية والذين يتصرفون بموجب الحقوق التي يديرونها أو نيابة عن ضحايا انتهاكات الحقوق المنصوص عليها في الكتاب الأول والثاني والثالث من ذات القانون بغرض الدفاع عن هذه الحقوق.

هـ – القائمون على إعادة استخدام المعلومات العامة الواردة في الأحكام المذكورة في المادة (١٠) من قانون العدالة الإدارية والقرارات المذكورة في المادة (١٣/١١١) من قانون التنظيم القضائي، بشرط ألا يكون للمعالجات غرض أو تأثير يسمح بإعادة تحديد هوية الأشخاص المعنيين.

وتتمثل العلة من قصر عمليات معالجة البيانات المذكورة على الفئات السابقة، في أن هذه البيانات أو المعالجات الخاصة بها، تتعلق بالاختصاص السيادي للدولة بخصوص تلك المسائل، وأن أي أمر بخلاف ذلك ينطوي على خطر تقويض احتكار العدالة الممنوح للدولة أو يمكن أن يقوض افتراض البراءة[١].

وتطبيقاً لذلك، قضت محكمة النقض الفرنسية بأن جمع ومعالجة بصمات الأصابع في نظام محوسب لمعالجة البيانات الشخصية، لا يمكن أن يتم إلا تحت سيطرة السلطة القضائية، وأن النيابة العامة لا تعتبر سلطة قضائية بالمعنى المقصود في الأحكام المذكورة أعلاه، أي في هذه الواقعة [٢].

[1] - Cléline CASTETS-RENARD , op.cit , N: 110.

[2] - Cass.civ , chamber civile 1 , 7 octobre 2015 , No: 14-20370. Publié

كما أن جمع البيانات الشخصية الآلية وجمع الأدلة وتحديد الهوية للجناة من خلال ربط الأفراد أو الأحداث أو الجرائم والجرائم ذات الطبيعة التسلسلية، لا تجوز معالجته إلا تحت إشراف السلطة القضائية [١].

وتطبيقاً لذلك، فإن دليل البيانات الشخصية التي يتم جمعها في إطار الإجراءات القضائية والتي تحتفظ بها خدمة السجلات الجنائية تحت سلطة وزير العدل، توضع تحت سيطرة قاضي التحقيق. وفي حالة رفض الدعوى أو صدور حكم بالبراءة، يتم مسح البيانات المتعلقة بالشخص الذي تتم محاكمته على الفور، من خلال نظام اتصالات آمن وللسلطة القضائية فقط [٢].

ويجب ملاحظة أن حظر معالجة البيانات الشخصية المتعلقة بالمخالفات والإدانات ذات الطابع الجنائي والمدني على حد سواء دون تفرقة بين مخالفة أو إدانة وأخرى؛ ويرجع ذلك لأمرين هما:

أ- عموم نص المادة التاسعة من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، التي جاء بمطلعها :" يُحظر معالجة البيانات الشخصية المتعلقة بالمخالفات والإدانات والتدابير الأمنية التي تُتخذ في مواجهة الشخص المعني بهذه البيانات ".

---

au bulletin , 2016 , n°: 837 , 1re civ , n°: 335.

[1] - Virginie GAUTRON , Fichiers de police – Fichiers princip alement destines aux missions de police judiciaire , Avril 2015 , (actualisation : mars 2019) , N : 149.

[2] - Christian GUERY , instruction preparation pouvoirs propres du juge d›instruction , juin 2018 (actualisation : juillet 2019) , Dalloz , N: 523.

ب- ما قضى به مجلس الدولة الفرنسي، بأن الحظر الخاص بمعالجة البيانات ذات الطبيعة الأمنية أو الجنائية والواردة في المادة التاسعة – سالفة الذكر – ينطبق على المخالفات والإدانات الجنائية والمدنية [١].

وترتيباً على ما تقدَّم، فإن الشخص المسؤول عن عملية المعالجة، يرتكب خطأً مدنياً في عملية معالجة البيانات الشخصية ذات الطابع الخاص جنائياً وأمنياً، إذا أجرى هذه المعالجة بالمخالفة للقيد التشريعي الذي حظر معالجة هذه الفئة من البيانات إلا من قِبل الجهات الخمس السالف ذكرها.

الفصل الثاني

الخطأ المدني الناشئ عن مخالفة الضوابط الإجرائية والتأمينية لعملية معالجة البيانات الشخصية

- تمهيد وتقسيم:

لقد سبق وأن تعرضنا في الفصل الأول لحالات الخطأ المدني الناشئ عن مخالفة بعض أو كل الالتزامات الملقاة على عاتق المسؤول عن عملية معالجة البيانات الشخصية، والتي تتمثل في عدم مشروعية الهدف من المعالجة وعدم توافق الهدف من المعالجة مع هذه المعالجة، وكذلك عدم التزامه بالشفافية في إجراء المعالجة بأن كانت البيانات غير ملائمة وغير دقيقة، وكذلك إذا لم يحصل المعالج على موافقة صاحب البيانات بعملية المعالجة، وأخيراً مخالفته لضوابط معالجة البيانات ذات الطابع الخاص شخصياً وأمنياً.

[1] - conseil d'Etat , 28 juillet 2004 , n°: 26-2851 , CNIL . 25 éme rapport d›activité 2004 , p. 78.

وبالإضافة إلى الحالات السابقة، فإن الخطأ المدني للمسؤول عن عملية المعالجة – في هذا الفصل – ينشأ بسبب عدم التزامه باتباع الضوابط الإجرائية اللازمة لصحة عملية المعالجة. وكذلك عدم التزامه بالمحافظة على سرية وسلامة وأمان البيانات محل المعالجة. وعلى ذلك سنتعرض لدراسة هذا الفصل من خلال المبحثيين التاليين:

المبحث الأول: الخطأ المدني الناشئ عدم اتباع الضوابط الإجرائية اللازمة لمعالجة البيانات الشخصية.

المبحث الثاني: الخطأ المدني الناشئ عن الإهمال في تأمين البيانات الشخصية.

المبحث الأول

الخطأ المدني الناشئ عدم اتباع الضوابط الإجرائية اللازمة لمعالجة البيانات الشخصية

– تقسيم:

هناك بعض الضوابط القانونية التي يلتزم المسؤول عن عملية المعالجة بالقيام بها، والتي من أهمها: وجوب حصول هذا المسؤول على إجازة قانونية مسبقة من الجهة الإدارية صاحبة الاختصاص بذلك (مطلب أول)، وكذلك التزامه بإجراء تقييم يوضح مدى تأثير عملية المعالجة على حماية البيانات الشخصية الخاضعة للمعالجة (مطلب ثان). ويترتب على مخالفة ذلك وجود خطأ مدني في حق المسؤول. وعلى ذلك سنتعرض في هذا المبحث لمطلبين هما:

المطلب الأول : الخطأ المدني الناشئ عن عدم الحصول على إجازة قانونية مسبقة بمعالجة البيانات الشخصية.

المطلب الثاني: الخطأ المدني الناشئ عن عدم إجراء تقييم تأثيري لعملية المعالجة على حماية البيانات الشخصية.

المطلب الأول

الخطأ المدني الناشئ عن عدم الحصول على إجازة قانونية مسبقة بمعالجة البيانات الشخصية

سنبدأ بحثنا في هذا المطلب بالتعرض لموقف المشرع الفرنسي (فرع أول)، ثم بيان موقف المشرع المصري (فرع ثان). وذلك على النحو التالي:

الفرع الأول

موقف المشرع الفرنسي

ألزم المشرع الفرنسي الشخص المسؤول عن عملية معالجة البيانات الشخصية، بضرورة الحصول على تصريح مسبق من الجهة الإدارية المختصة، وهي اللجنة الوطنية الفرنسية للمعلوماتية والحريات قبل البدء في عملية المعالجة. ويتم ذلك عن طريق أخذ رأي اللجنة الوطنية الفرنسية للمعلوماتية

والحريات أو الحصول على ترخيص منها بالمعالجة. ويعتبر هذا الأمر، التزام يقع على عاتق المسؤول عن عملية المعالجة قبل القيام بها [١].

---

[1] - Art 11/2 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 1) :" I. - La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité. Elle exerce les missions suivantes :

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en oeuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.

A ce titre :

a) Elle donne un avis sur les traitements mentionnés aux articles 26 et 27 ;

a bis) Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle prend en compte la situation des personnes dépourvues de compétences numériques. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs, et des besoins spécifiques des collectivités territoriales, de leurs groupements et des micro-entreprises, petites entreprises et moyennes entreprises ; elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel ;

b) En concertation avec les organismes publics et privés

représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. A ce titre, sauf pour les traitements mis en œuvre pour le compte de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, génétiques et de santé en application du 4 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et des garanties complémentaires en matière de traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions conformément à l'article 10 du même règlement ;

c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en oeuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en oeuvre ou envisagent de mettre en oeuvre des traitements automatisés de données à caractère personnel ;

e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;

f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;

f bis) Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et à la présente loi. Elle prend en considération, à cette fin, les besoins spécifiques des collectivités territoriales, de leurs groupements et des micro-entreprises, petites entreprises et moyennes entreprises. Elle agrée, aux mêmes fins, des organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'organisme national d'accréditation

وتتمثل الحكمة من أخذ رأي اللجنة الوطنية للمعلوماتية والحريات أو أخذ ترخيص منها بالمعالجة، في الأمريين التاليين [١]:

أ- إن هذه اللجنة هي الجهة الإدارية المسؤولة عن حماية البيانات والمعلومات والخصوصية الإلكترونية للأفراد وتمكينهم من نيل حقوقهم الإلكترونية المشروعة على بياناتهم الشخصية كالحق في الاستعلام والحق في الاطلاع والوصول والتصحيح والاعتراض. بالإضافة إلى دورها الرقابي والإشرافي على أنظمة المعلومات وتلقي الشكاوى من الأفراد والجهات عند وجود

---

mentionné au b du 1 de l'article 43 du même règlement ou décide, conjointement avec cet organisme, que ce dernier procède à leur agrément, dans des conditions précisées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément ;

g) Elle peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification, par des tiers agréés ou accrédités selon les modalités mentionnées au f bis du présent 2°, de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues au titre II du livre III du code des relations entre le public et l'administration.

Il en est tenu compte, le cas échéant, pour la mise en œuvre des sanctions prévues au chapitre VII de la présente loi.

h) Elle répond aux demandes ou saisines prévues aux articles 41, 42 et 70-22 ;

i) Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 70-4 ;

j) Elle mène des actions de sensibilisation auprès des médiateurs de la consommation et des médiateurs publics, au sens de l'article L. 611-1 du code de la consommation, en vue de la bonne application de la présente loi ".

[١] – د/ وليد السيد سليم، مرجع سابق، ص ٥٧٤، ٥٨٧.

مخالفات قانونية، وإصدار التراخيص اللازمة لأنشطة جمع ومعالجة المعلومات والتأكد من قيام النظام المعلوماتي الذي يتوافق مع الضوابط التشريعية المقررة في هذا الشأن.

ب- إن لهذه اللجنة سلطات واسعة قبل الجهات القائمة على الحواسب الآلية التي تتم عن طريقها عملية معالجة البيانات الشخصية. كما أن لهذه اللجنة سلطة اتخاذ القرارات التنظيمية العامة والفردية التي تراها لازمة وضرورية لتطبيق أحكام القانون. وما يؤيد ذلك أن سلطتها في تكليف أحد أعضائها بالتحقيق على الطبيعة وإجراء الفحص المناسب من أجل ضمان احترام نظم الأمن وتوجيه إنذار إلى ذوي الشأن حال اكتشاف مخالفات، وذلك على النحو الذي قررته المادة (١١) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات.

والأصل أن الترخيص بمعالجة البيانات الشخصية، يصدر من اللجنة الوطنية الفرنسية للمعلوماتية والحريات لبعض البيانات لطبيعتها أو للهدف منها أو بسبب نقلها. غير أن المشرع خرج على هذا الأصل في حالتين هما:

١- الاستثناء الأول: الترخيص الوزاري: وفي هذه الحالة تتوقف عملية المعالجة على الحصول على ترخيص من الوزير أو الوزراء المختصين في الحالات الآتية [١]:

[1] - Art 26/1 , loi n° 78 – 17 (Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004) :" I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat et :

أ- الحالة الأولى: المعالجات التي تتم لحساب الدولة والمتعلقة بأمنها أو بالدفاع عنها أو بأمنها العام. فمن أجل التوفيق بين حتمية معالجة البيانات الشخصية من أجل المحافظة على استقرار الدولة وحفظ الأمن فيها، وبين ضمان عدم حدوث اعتداء على بيانات الأفراد لا تتطلبه دواعي المحافظة على أمن الدولة والدفاع عنها؛ استلزم المشرع ضرورة الحصول على ترخيص وزاري لقانونية المعالجة.

ب- الحالة الثانية: المعالجات التي تتم لحساب الدولة بغية منع ارتكاب الجرائم الجنائية أو من أجل الاستدلال على جريمة معينة أو إثباتها أو ملاحقة مرتكبيها أو لتنفيذ العقوبات الجنائية أو الإجراءات الجنائية. فمن أجل التوفيق بين تحقيق أهداف السياسة الجنائية في الحفاظ على أمن المجتمع الداخلي ومواجهة الجريمة، وبين عدم حدوث تجاوز أو اعتداء على البيانات الشخصية التي يقتضي معالجتها تحقيق تلك الأهداف، يلزم الحصول على ترخيص وزاري لصحة المعالجة.

٢- الاستثناء الثاني: الترخيص القضائي: وهو الذي يعني تقييد إجراء عملية معالجة البيانات الشخصية بترخيص يصدر من مجلس الدولة. ويُستلزم ذلك في الحالات الآتية:

أ- معالجة البيانات الشخصية لحساب الدولة بهدف الحفاظ على أمنها أو الدفاع عنها أو الحفاظ على أمنها العام، ومن الممكن أن تؤدي هذه المعالجة

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de la commission est publié avec l'arrêté autorisant le traitement…..".

إلى الكشف عن الأصول العرقية أو الجنسية أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو الانتماءات النقابية للشخص الطبيعي، وكذلك البيانات الجينية والبيانات البيومترية التي تحدد هوية الشخص، وأيضاً البيانات الصحية وتلك المتعلقة بالحياة الجنسية أو التوجه الجنسي للشخص الطبيعي [١].

ب- معالجة البيانات الشخصية لحساب الدولة بهدف منع حدوث الجرائم الجنائية أو الاستدلال على هذه الجرائم وكذلك إثباتها أو تعقب مرتكبيها أو تنفيذ العقوبات الجنائية أو الإجراءات الأمنية وكان في ذلك مساس أو كشف عن الأمور السابق ذكرها بالبند (أ) والتي ورد النص عليها في المادة (١/٨) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ [٢].

---

[١] – وأشارت إلى تلك الحالة المادة (٢/٢٦) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، عندما تطلبت ترخيص من مجلس الدولة لمعالجة المسائل الواردة بالمادة (١/٨) من القانون المذكور. وجاء نصها كالتالي.....

- Art 26/2 , loi n° 78 – 17 (Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004) :" II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement…..".

- Art 8/1 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8) :" I. - Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique….".

[2] - Art 26/2 , loi n° 78 – 17 (Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004) :" I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de

ج- معالجة البيانات الشخصية التي تتم لحساب الدولة في حدود تحقيق الصالح العام، والتي تتعلق بالبيانات الجينية أو البيانات الحيوية اللازمة لتحديد هوية الأشخاص أو التحكم فيها [١].

وفي جميع الأحوال السابقة سواء كان الترخيص وزارياً أو قضائياً، يلزم الحصول على الرأي الاستشاري للجنة الوطنية الفرنسية للمعلوماتية والحريات.

وهناك أمران يتعين علينا التعرض لهما ونحن بصدد الحديث عن أخذ رأي اللجنة الوطنية للمعلوماتية والحريات أو الحصول على ترخيص من الجهة الإدارية المختصة، وهما: البيانات التي يلزم أن يتضمنها الترخيص، والمواعيد القانونية التي يجب أن يصدر خلالها الترخيص.

---

la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat et :

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de la commission est publié avec l'arrêté autorisant le traitement….".

[1] - Art 27 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 11):" Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes".

١- شكل الترخيص: ويعني ذلك تحديد الصورة التي يجب أن يُقدَّم بها طلب الترخيص إلى الجهة الإدارية المختصة، والبيانات التي يجب أن يشملها هذا الطلب. فلم يحدد المشرع الفرنسي وسيلة معينة للحصول على الترخيص بالمعالجة، لذلك يجوز تقديمه بأي وسيلة إلكترونية إلى هذه الجهة، سواء كانت اللجنة الوطنية للمعلوماتية والحريات أو الوزير المختص أو مجلس الدولة.

وبالنسبة للبيانات التي يلزم أن يتضمنها الترخيص بعملية المعالجة، فقد حددتها الفقرة الأولى من المادة الثلاثين من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، وهي كالآتي[1]:

[1] - Art 30/1 , loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 34):" I. - Les demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent :

1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;

2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 26 et 27, la description générale de ses fonctions ;

3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;

4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5° La durée de conservation des informations traitées ;

6° Le ou les services chargés de mettre en oeuvre le traitement ainsi que, pour les traitements relevant des articles 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° La fonction de la personne ou le service auprès duquel

أ- الهوية والعنوان الخاصان بالشخص المسؤول عن عملية المعالجة، أو هوية وعنوان من يمثله قانوناً في حالة ما إذا لم يكن هذا الشخص موجوداً على الإقليم الوطني أو على إقليم دولة عضو في الاتحاد الأوربي، وكذلك هوية وعنوان مقدم الطلب عند الاقتضاء.

ب- الهدف من عملية المعالجة، وفي حالة تعدد هذه الأهداف وجب ذكرها جميعاً.

ج- الترابط أو الدمج وجميع الأشكال الأخرى من الاتصالات مع عمليات المعالجات الأخرى.

د- فئات البيانات الشخصية الخاضعة لعملية المعالجة وأصل تلك البيانات، وكذلك فئات الأشخاص المعنيين بهذه المعالجة.

---

s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ;

9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum".

هـ – مدة حفظ المعلومات الناتجة عن عملية المعالجة أو ما يُعرف بالعمر الافتراضي للبيانات المعالجة.

و– تحديد الإدارة أو الإدرات المسؤولة عن تنفيذ المعالجة. وكذلك تحديد الأشخاص الذين يجوز لهم بسبب وظائفهم أو لإحتياج الإدارة لهم، الاطلاع أو الوصول المباشر إلى البيانات المسجلة والتي تم معالجتها وتندرج تحت المادتين (٢٦،٢٧) من القانون رقم ٧٨–١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات.

ز– المستلمون أو فئات المستفيدين الذين يحق لهم تلقي البيانات أو الاطلاع عليها.

ح– الإدارة أو الشخص الذي عن طريقه يمارس حق الولوج إلى البيانات محل المعالجة، وكذلك الإجراءات الخاصة بمباشرة هذا الحق.

ط – التدابير المتخذة من أجل ضمان تأمين المعالجات والبيانات وضمان سريتها التي كفلها القانون بنصوصه، والإشارة إلى مساعد القائم بعملية المعالجة (المعالج من الباطن أو المعالج الثانوي) إذا لزم الأمر ذلك.

ي– عند الاقتضاء، نقل البيانات الشخصية المعنية إلى دولة غير عضو في الاتحاد الأوربي بأي شكل من الأشكال، ما عدا المعالجات التي تُستخدم فقط من أجل العبور على الأراضي الفرنسية أو أراضي دولة أخرى في الاتحاد الأوربي.

٢– <u>الميعاد القانوني الذي يجب أن يصدر خلاله الترخيص:</u> لقد حددت المادتان (٥٤، ٢٨) من القانون رقم ٧٨–١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، الميعاد الذي يجب خلاله على اللجنة الوطنية الفرنسية للمعلوماتية والحريات الرد على طلب الحصول على ترخيص بمعالجة بعض البيانات السابق ذكرها.

وحددت المادتات المذكورتان، مدة شهرين من تاريخ استلام الطلب، تلتزم خلالهما اللجنة بالرد على هذا الطلب. وحرصاً من المشرع الفرنسي على حماية البيانات الشخصية التي تستلزم مثل هذا الإجراء لمعالجتها، فقد أجاز لرئيس اللجنة الوطنية الفرنسية بقرار مسبب منه أن يمد الفترة المذكورة لمرة أخرى بنفس المدة (أي شهرين آخرين). وإذا لم تصدر اللجنة قرارها بالقبول أو الرفض خلال المدد المذكورة، أُعتبر طلب الحصول على الترخيص مقبولاً [١].

وترتيباً على ما تقدم، فإن الشخص المسؤول عن عملية المعالجة يكون مرتكباً لخطأ مدني يستوجب مسؤوليته المدنية، إذا أجرى معالجة لبيانات

---

[1] - Art 54/ V, loi n° 78 – 17(Modifié par LOI n°2018-493 du 20 juin 2018 - art. 16) :" V. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être prolongé une fois pour la même durée sur décision motivée de son président ou lorsque l'Institut national des données de santé est saisi en application du second alinéa de l'article 61.

Lorsque la Commission nationale de l'informatique et des libertés ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée acceptée. Cette disposition n'est toutefois pas applicable si l'autorisation fait l'objet d'un avis préalable en application de la section 2 du présent chapitre et que l'avis ou les avis rendus ne sont pas expressément favorable ".

- Art 28 , loi n° 78 – 17 (Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004):" I. - La Commission nationale de l'informatique et des libertés, saisie dans le cadre des articles 26 ou 27, se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée du président.

II. - L'avis demandé à la commission sur un traitement, qui n'est pas rendu à l'expiration du délai prévu au I, est réputé favorable ".

شخصية تستلزم صدور ترخيص من الجهة الإدارية المختصة. كأن يُجري عملية معالجة تتم لحساب الدولة وتتعلق بأمنها أو بالدفاع عنها أو بأمنها العام، أو معالجة تهدف إلى منع ارتكاب الجرائم الجنائية أو الاستدلال على الجريمة أو إثباتها أو ملاحقة مرتكبيها أو تنفيذ العقوبات الجنائية أو الإجراءات الجنائية، دون الحصول على ترخيص وزاري.

وكذلك الأمر، يكون المسؤول عن عملية المعالجة مرتكباً لخطأٍ مدني إذا أجرى أياً من المعالجات السابقة وكان في ذلك مساس بالأصول العرقية أو الجنسية لصاحب البيانات أو آرائه السياسية أو معتقداته الدينية أو الفلسفية أو انتماءاته النقابية وكذلك بياناته الجينية والبيومترية التي تحدد هويته، وأيضاً بياناته الصحية والمتعلقة بحياته الجنسية، وكذلك المعالجات التي تتم لحساب الدولة في حدود تحقيق الصالح العام وتكون متعلقة بالبيانات الجينية أو البيانات الحيوية اللازمة لتحديد هوية الأشخاص أو التحكم فيها، دون الحصول على ترخيص بذلك من مجلس الدولة [١].

---

[١] – وجدير بالذكر أن المشرع الفرنسي كان يشترط إعلام اللجنة الوطنية الفرنسية للمعلوماتية والحريات عن طريق الإخطار والترخيص:

أ– الإخطار : وكان مقرراً بنص المادة (٢٢) من القانون رقم ٧٨–١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، حيث كان يلزم إخطار اللجنة بعملية المعالجة قبل القيام بها، وكان ذلك يسري على جميع المعالجات ما عدا المعالجات التي يكون الغرض منها إمساك سجل فقط وفقاً لأحكام القوانين أو اللوائح بقصد إعلام الناس فقط ، والتي تكون متاحة لأي شخص يكون له مصلحة مشروعة في ذلك. وكذلك المعالجات التي تقوم بها الجمعيات أو الهيئات الأخرى غير الهادفة لتحقيق الربح والمتعلقة بالمعتقدات الدينية والآراء الفلسفية والسياسية والنقابية. وأيضاً المعالجات التي تعبر عن الأمور الأدبية والفنية بشرط مراعاة القواعد الأخلاقية لتلك المهنة. **وقد ألغى المشرع الفرنسي تلك المادة ماعدا الاستثناء الأخير منها**.

الفرع الثاني

ب- الترخيص: وهو ثلاثة أنواع (الترخيص العام، والترخيص الوزاري، والترخيص القضائي). فالنوعين الأخيرين تعرضنا لهما سلفاً في المتن، وما زال المشرع الفرنسي مبقياً عليهما. أما الترخيص العام والذي كان يصدر من اللجنة الوطنية للمعلوماتية والحريات **فقد كان مقرراً بنص المادة (٢٥) وقد ألغاها المشرع الفرنسي**. وكانت هذه المادة تستوجب الحصول على ترخيص من هذه اللجنة في بعض الحالات: عمليات المعالجة الآلية وغيرها التي تتعلق بصورة مباشرة أو غير مباشرة بالأصول العرقية أو الآراء السياسية أو المعتقدات الدينية أو الإنتماءات النقابية أو تلك المتعلقة بحالة الفرد الصحية أو الجنسية. وكذلك المعالجات الآلية للبيانات الجينية ما عدا المعالجات التي يجريها الأطباء أو علماء علم الأحياء والتي تكون من مستلزمات الطب الوقائي وعمليات التشخيص الطبي وإدارة الرعاية والعلاج. وأيضاً عمليات المعالجة الآلية أو غيرها للبيانات الشخصية التي تخص الجرائم والإدانات أو التدابير الأمنية ما عدا المعالجات التي يقوم بها معاونوا القضاء والتي تكون لازمة لحاجات مهنتم في الدفاع عن الأشخاص الذين تعنيهم البيانات المعالجة. وحالة المعالجة التي تجري على بعض البيانات للأشخاص كرقم التسجيل في سجل الهوية الوطنية للأشخاص الطبيعيين والبيانات التي تستلزم فحص هذا السجل. وحالة المعالجات الآلية للبيانات التي يكون موضوعها إجراء تقييم للصعوبات الاجتماعية للأفراد. وحالة المعالجات الآلية التي يكون محلها معالجة بيانات بيومترية ضرورية للتحقق من هوية الأشخاص. وحالة المعالجات الآلية وغير الآلية التي يقوم بها المعهد الوطني للإحصاء والدراسات الاقتصادية. وحالة المعالجة الآلية للبيانات المتعلقة بالربط بين الملفات الخاصة بشخص أو بأكثر من الأشخاص الاعتبارية التي تتولى إدارة خدمة عامة والتي تتطابق أهدافها مع ما يقتضيه الصالح العام، وتلك المتعلقة بالربط بين الملفات الخاصة بأشخاص اعتباريين آخرين. وحالة المعالجة التي يكون الهدف منها إجراء بحث يخص الصحة أو علم الأوبئة أو علم الوراثة أو الإحصاء الحيوي. وحالة معالجة البيانات الشخصية التي يكون الغرض من إجرائها تقييم ممارسات وعائية ووقائية. وحالة نقل البيانات الشخصية خارج الاتحاد الأوربي.

موقف المشرع المصري

وضع المشرع المصري في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ، ضوابط إجرائية لمن يقوم بمهام جمع أو تخزين أو نقل أو معالجة البيانات الشخصية. نتعرض لها بالبيان التالي:

أولاً: ضرورة الحصول على ترخيص أو تصريح من مركز حماية البيانات الشخصية [١]:

[١] – وجود هذا المركز في القانون المصري يضاهي وجود اللجنة الوطنية الفرنسية للمعلوماتية والحريات في القانون الفرنسي. وأنشأه المشرع المصري بالقانون رقم ١٥١ لسنة ٢٠٢٠، وهو عبارة عن هيئة عامة اقتصادية تسمي «مركز حماية البيانات الشخصية»، تتبع الوزير المختص، وتكون لها الشخصية الاعتبارية، ويكون مقرها الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، وتهدف إلي حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، ولها في سبيل تحقيق أهدافها أن تباشر جميع الاختصاصات المنصوص عليها بهذا القانون، ولها علي الأخص الآتي : وضع وتطوير السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية ، والقيام علي تنفيذها، توحيد سياسات وخطط حماية ومعالجة البيانات الشخصية داخل الجمهورية، وضع وتطبيق القرارات والضوابط والتدابير والإجراءات والمعايير الخاصة بحماية البيانات الشخصية، وضع إطار إرشادي لمدونات السلوك الخاصة بحماية البيانات الشخصية ، واعتماد مدونات السلوك الخاصة بحماية البيانات الشخصية بالجهات المختلفة، التنسيق والتعاون مع جميع الجهات والأجهزة الحكومية وغير الحكومية في ضمان إجراءات حماية البيانات الشخصية، والتواصل مع جميع المبادرات ذات الصلة، دعم تطوير كفاءة الكوادر البشرية العاملة في جميع الجهات الحكومية وغير الحكومية القائمة علي حماية البيانات الشخصية، إصدار التراخيص أو التصاريح والموافقات والتدابير المختلفة المتعلقة بحماية البيانات الشخصية وتطبيق أحكام هذا القانون، اعتماد الجهات والأفراد، ومنحهم التصاريح اللازمة التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات

لم يعهد المشرع المصري القيام بمهام جمع أو تخزين أو نقل أو معالجة البيانات الشخصية لأي شخص، بل تطلب لمن يقوم بأي من هذه المهام ضرورة الحصول على ترخيص أو تصريح من مركز حماية البيانات الشخصية ووجود اعتماد بذلك.

أ- **الترخيص**: عرفه المشرع المصري بأنه وثيقة رسمية تصدر عن المركز للشخص الاعتباري تمنحه من خلالها الحق في مزاولة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الإلكتروني أو كل ما سبق والتعامل عليها بأي صورة، وتحدد التزامات

الشخصية، تلقي الشكاوي والبلاغات المتعلقة بأحكام هذا القانون، وإصدار القرارات اللازمة في شأنها، إبداء الرأي في مشروعات القوانين والاتفاقيات الدولية التي تنظم البيانات الشخصية أو تتعلق أو تنعكس نصوصها بصورة مباشرة أو غير مباشرة عليها، الرقابة والتفتيش علي المخاطبين بأحكام هذا القانون ، واتخاذ الإجراءات القانونية اللازمة، التحقق من شروط حركة البيانات عبر الحدود، واتخاذ القرارات المنظمة لها، تنظيم المؤتمرات وورش العمل والدورات التدريبية والتثقيفية، وإصدار المطبوعات لنشر الوعي والتثقيف للأفراد والجهات حول حقوقهم فيما يتعلق بالتعامل علي البيانات الشخصية، تقديم جميع أنواع الخبرة والاستشارات المتعلقة بحماية البيانات الشخصية، وعلي الأخص لجهات التحقيق والجهات القضائية، إبرام الاتفاقيات ومذكرات التفاهم والتنسيق والتعاون وتبادل الخبرات مع الجهات الدولية ذات الصلة بعمل المركز وفقًا للقواعد والإجراءات المقررة في هذا الشأن، إصدار الدوريات الخاصة بتحديث إجراءات الحماية بما يتوافق مع أنشطة القطاعات المختلفة وتوصيات المركز في شأنها، إعداد وإصدار تقرير سنوي عن حالة حماية البيانات الشخصية في جمهورية مصر العربية ..... المادة (١٩) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

المرخص له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية لهذا القانون ، وذلك لمدة ثلاث سنوات قابلة للتجديد لمدد أخرى [١].

ب- التصريح: عرفه المشرع المصري بأنه وثيقة رسمية تصدر عن مركز حماية البيانات الشخصية للشخص الطبيعي أو الاعتباري تمنحه من خلالها الحق في ممارسة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الإلكتروني أو كل ما سبق والتعامل عليها بأي صورة، أو لأداء مهمة أو مهام معينة، وتحدد هذه الوثيقة التزامات المصرح له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية، لمدة مؤقتة لا تجاوز سنة، ويجوز تجديدها لأكثر من مدة [٢].

ج- الاعتماد: عرفه المشرع المصري بأنه عبارة عن شهادة تصدر عن مركز حماية البيانات الشخصية، تفيد أن الشخص الطبيعي أو الاعتباري قد استوفي جميع المتطلبات الفنية والقانونية والتنظيمية المحددة باللائحة التنفيذية لهذا القانون، ويكون بموجبها مؤهلاً لتقديم الاستشارات في مجال حماية البيانات الشخصية [٣].

ثانياً: أنواع التراخيص والتصاريح والاعتمادات وإجراءاتها:

[١] – المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

[٢] – المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

[٣] – المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

حددت المادة (٢٦) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، أنواع التراخيص والتصاريح والاعتمادات التي يصدرها مركز حماية البيانات الشخصية لمن يعملون في مجال البيانات الشخصية، والتي تتمثل في الآتي:

١ – يقوم المركز بتصنيف التراخيص والتصاريح والاعتمادات وتحديد أنواعها، ووضع الشروط الخاصة بمنح كل نوع منها، وذلك وفقًا لما تحدده اللائحة التنفيذية لهذا القانون.

٢ – إصدار الترخيص أو التصريح للمتحكم أو المعالج لإجراء عمليات حفظ البيانات، والتعامل عليها ومعالجتها وفقًا لأحكام هذا القانون.

٣ – إصدار التراخيص أو التصاريح الخاصة بالتسويق الإلكتروني المباشر.

٤ – إصدار التراخيص أو التصاريح الخاصة بالمعالجات التي تقوم بها الجمعيات أو النقابات أو النوادي للبيانات الشخصية لأعضاء تلك الجهات وفي إطار أنشطتها.

٥ – إصدار التراخيص أو التصاريح الخاصة بوسائل المراقبة البصرية في الأماكن العامة.

٦ – إصدار التراخيص أو التصاريح الخاصة بالتحكم ومعالجة البيانات الشخصية الحساسة.

٧ – إصدار التصاريح والاعتمادات الخاصة بالجهات والأفراد التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات الشخصية، وإجراءات الامتثال لها.

٨ – إصدار التراخيص والتصاريح الخاصة بنقل البيانات الشخصية عبر الحدود [١].

وبالنسبة لإجراءات لإصدار التراخيص والتصاريح والاعتمادات، فتتمثل في تقديم طلبات التراخيص والتصاريح والاعتمادات علي النماذج التي يضعها مركز حماية البيانات الشخصية مشفوعة بجميع المستندات والمعلومات التي يحددها، مع تقديم ما يثبت قدرة المتقدم المالية وقدرته علي توفير وتنفيذ المتطلبات والمعايير الفنية المقررة، ويبت في الطلب خلال مدة لا تجاوز تسعين يومًا من تاريخ استيفائه لجميع المستندات والمعلومات وإلا اعتبر الطلب مرفوضًا. ويجوز للمركز طلب بيانات أو وثائق أو مستندات أخري للبت في الطلب، كما يكون له الحق في طلب توفير ضمانات إضافية لحماية البيانات الشخصية إذا تبين عدم كفاية الحماية المبينة بالمستندات المقدمة إليه. كما يجوز للمتحكم أو المعالج الحصول علي أكثر من ترخيص أو تصريح وفقًا لنوعية البيانات الشخصية المتعامل عليها [٢].

ثالثاً: تعديل شروط التراخيص والتصاريح وإلغائها:

[١] – وتحدد اللائحة التنفيذية لهذا القانون أنواع هذه التراخيص والتصاريح والاعتمادات وفئاتها ومستوياتها، وإجراءات وشروط إصدارها وتجديدها ونماذجها المستخدمة ، وذلك بمقابل رسوم لا تتجاوز مليوني جنيه بالنسبة للترخيص ، ومبلغ لا يتجاوز خمسمائة ألف جنيه للتصريح أو الاعتماد ..... المادة (٢٦) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

[٢] – المادة (٢٧) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

أعطى المشرع المصري لمركز حماية البيانات الشخصية، مكنة تعديل شروط الترخيص أو التصريح وفقاً لما تمليه اعتبارات المصلحة العامة، وكذلك في حالة الاستجابة إلي الاتفاقيات الدولية أو الإقليمية أو القوانين الوطنية ذات الصلة، وبناءً علي طلب المرخص له، وفي حالة اندماج المتحكم أو المعالج مع آخرين داخل جمهورية مصر العربية أو خارجها. وأخيراً في حالة ما إذا كان التعديل ضروريًا لتحقيق أهداف هذا القانون [١]. وفي غير هذه الحالات لا يجوز للمركز تعديل شروط الترخيص أو التصريح؛ لأن المشرع نص على هذه الحالات على سبيل الحصر لا المثال.

ومن السلطات التي أعطاها المشرع المصري لمركز حماية البيانات الشخصية في القانون رقم ١٥١ لسنة ٢٠٢٠، هي سلطة إلغاء الترخيص أو التصريح أو الاعتماد بعد إصدارة إذا توافرت حالة من الحالات التي نص عليها القانون، وهي: مخالفة شروط الترخيص أو التصريح أو الاعتماد، وحالة عدم سداد رسوم تجديد الترخيص أو التصريح أو الاعتماد، وحالة تكرار عدم الامتثال لقرارات المركز، وحالة التنازل عن الترخيص أو التصريح أو الاعتماد للغير دون موافقة المركز، وأخيراً حالة صدور حكم بإفلاس المتحكم أو المعالج [٢].

وترتيباً على ما تقدم، فإن الخطأ المدني يثور في هذا الصدد إذا قام الشخص الطبيعي أو المعنوي الذي كان له دور في عملية جمع أو حفظ أو معالجة أو نقل البيانات الشخصية، سواء كان هو المتحكم أو المعالج، بأي من العـمليات المذكورة دون أن يحصل على تصريح – للشخص الطبيعي والاعتباري – أو ترخيص – للشخص الاعتباري فقط – أو دون وجود اعتماد من مركز حماية البيانات الشخصية بذلك.

---

[١] – المادة (٢٨) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

[٢] – المادة (٢٩) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية

المطلب الثاني

الخطأ المدني الناشئ عن عدم إجراء تقييم تأثيري لعملية المعالجة على حماية البيانات الشخصية

سنتعرض لدراسة التزام المسؤول عن عملية معالجة البيانات الشخصية بإجراء تقييم لمدى تأثير عملية المعالجة على حماية البيانات، من خلال تحديد المقصود بهذا الالتزام (أولاً)، والنص التشريعي عليه (ثانياً). وذلك على النحو التالي:

أولاً: تحديد المقصود بالتقييم التأثيري:

يُقصد بالتقييم التأثيري، ذلك الإجراء الذي يلتزم المسؤول عن عملية المعالجة القيام به، سواء كان معالجاً أصلياً أو معالجاً من الباطن – ويقوم به في القانون المصري الشخص المسؤول عن حماية البيانات الشخصية – ، بهدف إجراء تحليل تقييمي لمدى تأثير عملية المعالجة على حماية البيانات الشخصية الخاضعة لتلك العملية ومدى كفالة حقوق أصحاب هذه البيانات عليها، وكذلك مدى التأكد من أن الوسائل المتبعة أو المتخذة لحماية هذه البيانات تتناسب مع المخاطر التي قد تكتنف عملية معالجتها وخصوصاً في الحالات التي تكون فيها مظاهر الخطورة التي تحيط بالمعالجة واضحة ولها ما يبررها حسبما يتراءى للقائم بعملية المعالجة، كل ذلك بهدف توفير أقصى حماية قانونية للبيانات الشخصية المعالجة ولمن تعنيهم هذه البيانات

ثانياً: النص التشريعي على التقييم التأثيري:

كان المشرع الفرنسي ينظم التزام المسؤول عن عملية معالجة البيانات الشخصية بإجراء تقييم تأثيري عن تلك المعالجة على حماية البيانات الخاضعة للمعالجة، وكان ذلك في المادة (٤/٧٠) من القانون رقم ٧٨–١٧ لسنة ١٩٧٨

بشأن المعلوماتية والحريات – وأنشئت تلك المادة بموجب القانون رقم ٤٩٣-٢٠١٨ المؤرخ في ٢٠ يونيه ٢٠١٨ والملغاة بالمرسوم رقم ١١٢٥-٢٠١٨ المؤرخ في ١٢ ديسمبر ٢٠١٨ – [١].

[١] – تعرض المشرع الفرنسي لالتزام المسؤول عن عملية المعالجة بإجراء تقييم تأثيري للمعالجة على حماية البيانات محل المعالجة، وذلك بموجب المادة (٤/٧٠) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، والتي كانت نفرق بين نوعين من التقييم هما:

١- التقييم التأثيري اللاحق : ويُقصد به ذلك التقييم الذي يجريه المسؤول عن عملية المعالجة بعد إتمام تلك العملية. وأقرته المادة (٤/٧٠) من القانون المذكور، وخصوصاً إذا كان هناك احتمال أن المعالجة نتج عنها خطورة كبيرة على حقوق وحريات الأشخاص الطبيعيين الذين تخضع بياناتهم للمعالجة، وخصوصاً البيانات التي ورد النص عليها في المادة (١/٨) – سالفة الذكر – من القانون المذكور.

فهذه البيانات الأخيرة، هي التي تكشف بأي صورة عن الأصول العرقية أو الجنسية أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو الإنتماءات النقابية للشخص الطبيعي، وكذلك بياناته الجينية والبيومترية التي تحدد هوية الشخص، وأيضاً البيانات الصحية، وتلك المتعلقة بالحياة الجنسية أو التوجه الجنسي للشخص الطبيعي.

فجميع البيانات السابقة، يلزم بعد معالجتها إجراء تقييم تأثيري بقصد تحليل أثر المعالجة على حماية تلك البيانات، من أجل تحقيق التوازن بين حتمية معالجتها في بعض الأحيان وبين صيانة حقوق الأشخاص على هذه البيانات؛ وذلك بسبب خطورة وحساسية معالجة تلك الفئة من البيانات الشخصية.

وتأكيداً على أهمية ما تقدم، فقد أوجبت المادة (١٤/٧٠) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، على كل من المسؤول عن المعالجة والمعالج من الباطن بالاحتفاظ بسجل الأنشطة التي تم معالجتها والتدابير والإجراءات التي تهدف إلى ضمان مستوى كاف من الأمان يتناسب لمواجهة المخاطر التي تحيط بعملية المعالجة وبيان الأساس القانوني لها [١].

٢- التقييم التأثيري السابق: وقررته المادة (٤/٧٠)، ويقوم به المعالج قبل إجراء عملية

غير أنه بعد إلغاء المادة المذكورة، وجدنا ضآلتنا في وجود التنظيم التشريعي للتقييم التأثيري في التشريع المصري والتشريع الأوربي:

١- نص المادة (١/٩) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠: والتي جاء بها :" يكون مسئول حماية البيانات الشخصية مسئولاً عن تنفيذ أحكام القانون ولائحته التنفيذية وقرارات المركز،

المعالجة عن طريق التشاور وأخذ رأي اللجنة الوطنية الفرنسية للمعلوماتية والحريات، إذا كان تقييم تأثير المعالجة على حماية البيانات يشير إلى أن هذه المعالجة ستشكل خطراً كبيراً في حالة ما إذا لم يتخذ المراقب تدابير لمنع هذه المخاطر. وكذلك إذا كانت عملية المعالجة تتضمن مخاطر كبيرة على حريات وحقوق الأشخاص المعنيين وكان ذلك بسبب استخدام آليات أو تقنيات أو اجراءات جديدة.

- Art 70/ 4, loi n° 78 – 17 (Créé par LOI n°2018-493 du 20 juin 2018 - art. 30 - Abrogé par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1) :" Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.
Si le traitement est mis en œuvre pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue à l'article 30.
Dans les autres cas, le responsable de traitement ou son sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement de données à caractère personnel :
1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable de traitement ne prenait pas de mesures pour atténuer le risque ;
2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées ".

ومراقبة الإجراءات المعمول بها داخل كيانه الإشراف عليها، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقا لأحكام هذا القانون . ويلتزم علي الأخص بالآتي :

١ – إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها ، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها .....".

٢– نص المادة (٣٥) من اللائحة الأوربية رقم ٦٧٩ الصادرة في ٢٧ أبريل لسنة ٢٠١٦ بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية وحرية نقل هذه البيانات.

فالمادة السابقة ألزمت الشخص المسؤول عن عملية معالجة البيانات الشخصية بإجراء تقييم تأثيري قبل القيام بأي عملية معالجة؛ وذلك من أجل بيان ما إذا كان من المرجح أن تؤثر معالجة محددة وخاصة بنوعية بفئة محددة من البيانات الشخصية باستخدام التكنولوجيا الحديثة بصورة خطرة على حقوق الأشخاص الطبيعيين وحرياتهم على بياناتهم من عدمه [١].

ووضحت المادة المذكورة، البيانات التي يجب أن يتضمنها التقييم وهي: وصف منهجي لعمليات المعالجة المعنية أو المقصودة، والمصلحة التي يرمي المعالج إلى تحقيقها، وتوضيح مدى ضرورة وتناسب عمليات المعالجة مع الهدف منها، وتقييم المخاطر المتعلقة بحقوق وحريات أصحاب البيانات محل المعالجة، والتدابير المتخذة لمواجهة تلك المخاطر والضمانات والتدابير والإجراءات الأمنية التي تكفل حماية هذه البيانات، وإثبات الامتثال لهذه الأمور

[1] - Art 35 of Regulation (EU) 2016/679 :" 1- Where a type of processing in particular using new technologies , and taking into account the nature , scope , context and purposes of the processing , is likely to result in a high risk to the rights and freedoms of natural persons , the controller shall , prior to the processing …".

مع الأخذ في الاعتبار حقوق ومصالح أصحاب البيانات وغيرهم من الأشخاص المعنيين.

وقد ألزم المشرع الأوربي معالج البيانات الشخصية في بعض الحالات بوجوب إجراء التقييم التأثيري، كما إذا كانت المعالجة الآلية تستطيل الجوانب الشخصية للأشخاص الطبيعيين بما في ذلك التنميط [١]، أو إذا كانت المعالجة تتم على نطاق كبير للبيانات الشخصية ذات الطابع الحساس أو البيانات المتعلقة بالإدانات الجنائية والجرائم [٢]. وكذلك لزوم قيام المعالج بالحصول على موافقة أصحاب البيانات أو من يمثلهم بخصوص عملية المعالجة بما لا يخل بحماية المصالح التجارية أو المصالح العامة أو أمن المعالجات [٣].

---

[١] – والتنميط هو أي صورة من صورة المعالجة الآلية للبيانات الشخصية التي تتألف من استخدام البيانات الشخصية من أجل تقييم بعض الجوانب الشخصية ذات الصلة بالشخص الطبيعي، وخصوصاً التحليل والتنبؤ بالجوانب المتعلقة بأداء الشخص الطبيعي في العمل والوضع الاقتصادي والوضع الصحي والرغبات الشخصية..... المادة الرابعة من اللائحة الأوربية رقم ٦٧٩ المؤرخة في ٢٧ أبريل سنة ٢٠١٦.

[2] - Art 35 of Regulation (EU) 2016/679 :" A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of : a- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing , including profiling ; b- processing on a large scale of special categories of data referred …… or of personal data relating to criminal convictions and offences ……".

[3] - Art 35 of Regulation (EU) 2016/679 :" 9- Where appropriate , the controller shall seek the views of data subjects or their representatives on the intended processing , without prejudice to the protection of commercial or public interests or the security of processing operations …..".

وفي هذا الصدد، أرسى المشرع الأوربي أمرين وازن من خلالهما بين ضرورة إجراء التقييم التأثيري من عدمه، وبين التأكيد على تطور هذا الالتزام إذا وُجد ما يستدعي ذلك، وهما:

أ- ألزم المشرع الأوربي السلطة أو الهيئة المنوط بها الإشراف على عمليات المعالجات، أن تضع وتنشر قائمة تبين فيها أنواع المعالجات التي ينطبق عليها الالتزام بأداء التقييم التأثيري، وتلك التي لا تستلزم مثل هذا الإجراء[١].

فليس كل عمليات المعالجة تتضمن قدر كبير من الخطورة بما يؤثر على حقوق أصحابها بالسلب، بمعنى أنه إذا كانت وسائل الأمان متحققة ومؤكدة ولن يؤثر إجراء التقييم على الحماية القانونية المرجوة لهذه البيانات، فلا داعي لإجرائه في هذه الحالة.

ب- يجب على المعالج عند الاقتضاء أن يراجع التقييم الذي أجراه على عملية معالجة البيانات الشخصية من ذي قبل، إذا تبين أن هناك تغيير في المخاطر التي تكتنف عملية المعالجة [٢].

---

[1] - Art 35 of Regulation (EU) 2016/679 :" 4- The supervisory authority shall estabhish and make public a list of the kind of processing operations which are subject to requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. 5- The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisopry authority shall communicate those lists to the Board ".

[2] - Art 35 of Regulation (EU) 2016/679 :" 11- Where necessary , the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represent by

ويرجع ذلك إلى أن وسائل تهديد أمن البيانات ومعالجتها، تتسم بالجدة والابتكار والتغيير من حين إلى آخر، لذلك يجب على المعالج مسايرة مثل هذه المستحدثات عن طريق مراجعة التقييم الذي أجراه سابقاً.

وترتيباً على ما تقدم، فإن المسؤول عن عملية معالجة البيانات الشخصية أو عن حمايتها، يُعدَ مرتكباً لخطأٍ مدني يستوجب مسؤوليته، إذا لم يجر التقييم التأثيري قبل إجراء عملية المعالجة. أو إذا أجرى التقييم دون أن يتضمن البيانات اللازمة لذلك والتي سبق ذكرها. وكذلك إذا لم يجر التقييم في الحالات التي يتوجب عليه فيها فعل ذلك عندما تمتد المعالجة الآلية إلى الجوانب الشخصية لصاحبها أو كانت ماسة ببياناته الحساسة أو كانت متعلقة بالإدانات الجنائية. وكذلك إذا لم يضع وينشر معالجات البيانات التي تستوجب إجراء التقييم التأثيري وتلك التي لا تستوجبه. وأخيراً إذا لم يراجع التقييم الذي أجراه في حالة ما إذا تبين له وجود مخاطر جديدة مستجدة تحيط بعملية المعالجة.

المبحث الثاني

الخطأ المدني الناشئ عن الإهمال في تأمين البيانات الشخصية

– تقسيم:

يلتزم معالج البيانات الشخصية بتأمين تلك البيانات بكل الوسائل التي تكفل حمايتها وعدم تعرضها للانتهاك أو الاختراق من قبل الغير ممن يُحظر عليهم الاطلاع عليها– ويشترك معه المتحكم والمسؤول عن حماية هذه البيانات في القانون المصري –. ويلتزم كذلك بالمحافظة على سرية هذه البيانات، وأن يراعي الضوابط القانونية المقررة في حالة نقل البيانات المعالجة إلى دولة خارج الاتحاد الأوربي أو دولة خارج جمهورية مصر العربية.

---

processing opereations ….".

وعلى ذلك، يكون المعالج مقصراً في أداء التزامه في هذا الشأن، إذا أهمل في تأمين البيانات الشخصية المعالجة، إو إذا لم يحافظ على سريتها، أو نقلها خارج الاتحاد الأوربي أو خارج جمهورية مصر العربية دون مراعاة ضوابط هذا النقل. لذلك، سنتناول هذا المبحث من خلال المطلبين الآتيين:

المطلب الأول: المقصود بإهمال المعالج في تأمين البيانات الشخصية.

المطلب الثاني: الخطأ المدني الناشئ عن إخلال المعالج بالالتزامات المتفرعة عن الالتزام بتأمين البيانات الشخصية.

المطلب الأول

المقصود بإهمال المعالج في تأمين البيانات الشخصية

سنتعرض في هذا المطلب للإقرار التشريعي لالتزام المعالج بتأمين البيانات الشخصية (أولاً)، وماهية هذا الالتزام (ثانياً)، وطبيعته (ثالثاً). وذلك على النحو التالي:

أولاً: الإقرار التشريعي لالتزام المعالج بتأمين البيانات الشخصية:

نظراً لأهمية التزام المعالج بتأمين البيانات الشخصية، فقد نص على هذا الالتزام بصورة صريحة كل من المشرع الفرنسي، والمشرع المصري، والمشرع الأوربي:

أ- إقرار المشرع الفرنسي: أقر المشرع الفرنسي التزام المعالج بتأمين البيانات الشخصية في المادة (٣٤) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، التي نصت على أنه:" يجب على الشخص المسؤول عن إجراء عملية المعالجة، أن يتخذ كل الاحتياطات المطلوبة للحفاظ على أمن البيانات، لاسيما منع تشويهها أو اتلافها أو الولوج إليها من غير المسموح لهم

بذلك، وذلك من منظور طبيعة البيانات وما يحيط بها من مخاطر بسبب عملية المعالجة " [١].

ب– إقرار المشرع المصري: لقد أولى المشرع المصري أهمية كبيرة لمسألة حماية أمن البيانات الشخصية [٢] سواء عند جمعها أو حفظها أو نقلها أو معالجتها؛ إيماناً منه بأهمية وخطورة هذه البيانات بالنسبة لصاحبها. وجاء ذلك خلال العديد من النصوص القانونية في القانون رقم ١٥١ لسنة ٢٠٢٠. وألقى – أي المشرع المصري – بهذا الالتزام على عاتق أي شخص يكون له دور في مجال هذه البيانات، أي على عاتق المتحكم والمعالج والمسؤول عن الحماية.

فجاء النص في المادة رقم (٢/٣) على أنه:" يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية .... ٢ – أن تكون صحيحة وسليمة ومؤمنة .....". وجاء النص أيضاً في المادة رقم (٦/٤) على أنه:" مع مراعاة أحكام المادة (١٢) من هذا القانون، يلتزم المتحكم بما

1- Art 34, loi n° 78 – 17 (Modifié par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004) :" Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8".

٢ – عرف المشرع المصري أمن البيانات الشخصية بأنه :" إجراءات وعمليات تقنية وتنظيمية من شأنها الحفاظ علي خصوصية البيانات الشخصية وسريتها وسلامتها ووحدتها وتكاملها فيما بينها.....". المادة رقم (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

يأتي..... ٦ – اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظا علي سريتها ، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قِبَل أي إجراء غير مشروع .....".

ونص المشرع المصري أيضاً في المادة (٧/٥) من ذات القانون على أنه:" مع مراعاة أحكام المادة (١٢) من هذا القانون، يلتزم معالج البيانات الشخصية بما يأتي .... ٧ – حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك وما عليها من بيانات شخصية .....". وكذلك النص في المادة (٤/٩) من ذات القانون على أنه:" يكون مسئول حماية البيانات الشخصية مسئولاً عن تنفيذ أحكام القانون ولائحته التنفيذية وقرارات المركز، ومراقبة الإجراءات المعمول بها داخل كيانه الإشراف عليها، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقا لأحكام هذا القانون . ويلتزم علي الأخص بالآتي ..... ٤ – إخطار المركز في حال وجود أي خرق أو انتهاك للبيانات الشخصية لديه .....".

وأخيراً أكد المشرع المصري على أهمية هذا الالتزام، بالنص على ذلك في المادة (١٣) من ذات القانون، والتي جاء بها :" بالإضافة إلي الالتزامات الواردة بالمادة (٩) من هذا القانون، يلتزم مسئول حماية البيانات الشخصية وتابعوه لدى المتحكم أو المعالج باتباع واستيفاء السياسات والإجراءات التأمينية اللازمة لعدم خرق البيانات الشخصية الحساسة أو انتهاكها ".

٣– إقرار المشرع الأوربي: أقر المشرع الأوربي التزام المعالج بتأمين البيانات الشخصية في المادة (٣٢) من اللائحة الأوربية رقم ٢٠١٦/٦٧٩ بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية وحرية نقل هذه البيانات، التي نصت على أنه:" يجب على المراقب أو المعالج، اتخاذ الخطوات اللازمة لضمان منع أي شخص طبيعي يعمل تحت سلطة المراقب أو

المعالج، من الوصول إلى البيانات التي تمت معالجتها، إلا بناءً على تعليمات من المراقب ما لم يكن مطلوباً منه القيام بذلك " [١].

ثانياً: ماهية التزام المعالج بتأمين البيانات الشخصية:

يعني التزام المعالج بتأمين البيانات الشخصية المعالجة، أن يبذل كل ما في وسعه للمحافظة على أمن هذه البيانات ومنع تعرضها للانتهاك أو الاختراق بقدر المستطاع وبأي وسيلة يراها هو مناسبة لتحقيق هذا الغرض، وذلك في ضوء خبرته ومعرفته بوسائل الأمان الإلكتروني. ويُعدَّ هذا الالتزام، من الالتزامات المهنية الموضوعية الملقاة على عاتق المعالج، والذي يلتزم به سواء في مرحلة جمع البيانات أو معالجتها.

وعلى ذلك يلتزم المعالج، بتوفير سبل الأمان المناسبة واللازمة للمحافظة على أمن البيانات الشخصية. وتوفير هذه السبل يكون من صميم عمل المعالج، وله مطلق الحرية في اختيار هذه السبل، والتي يعد من أبرزها:

أ- خاصية تشفير البيانات الشخصية: والتشفير هو عبارة عن مناهج لحط البيانات من خلال لوغاريثمات أو خوارزميات، بحيث لا يمكن قراءتها عن طريق أي طرف ثالث متطفل، بقصد حجب البيانات محل التشفير عن التداول العام [٢]. فوظيفة التشفير تتمثل في تخزين البيانات الشخصية في ملف حاسب آمن أو نقلها عبر قناة إلكترونية آمنة.

---

[1] - Art 35 of Regulation (EU) 2016/679 :" The controller and processor shall take steps to ensure that any natural person actin under the authority of the controller or the the processor who has access to personal data does not process them except on instruction from the contoroller , unless he or she is required to do ….".

[٢] – د/ وليد السيد سليم، مرجع سابق، ص ١٧٢.

وتُعرف البيانات أو المعلومات المُراد إخفاؤها " بالنص الأصلي "، وتُعرف عملية الإخفاء ذاتها " بالتشفير "، ويُطلق على النص الأصلي المشفر اسم "النص المشفر أو بيان التشفير "، ويُطلق على مجموعة القواعد المستخدمة في عملية تشفير النص الأصلي " بخوارزمية التشفير". وتعتمد هذه الأخيرة على مفتاح التشفير الذي يمثل مدخلاً لها، بالإضافة إلى الرسالة أو البيان الشخصي. ولكي يتمكن المتلقي أو من له حق الوصول إلى البيانات الشخصية المشفرة، الاطلاع على تلك البيانات أو استرجاع الرسالة أو البيان المشفر من خلال النص المشفر، يجب أن يتوافر لديه خوارزمية فك التشفير التي عند استخدامها مع مفتاح فك التشفير المناسب، تسترجع الأصلي من النص المشفر[١].

٢- حماية البيانات الشخصية عن طريق كلمات السر: وهي عبارة كلمات مرور لا تكون بحوزة إلا من يحق لهم الولوج إلى البيانات الشخصية والاطلاع عليها اطلاعاً مشروعاً. وعادة ما يتم تخزين أسماء المستخدمين وكلمات المرور في جداول، ويُحفظ الجدول بشكل دائم على ملف موجود على اسطوانة أو أي برنامج معلوماتي آمن. وغالباً ما تُحفظ جداول كلمات المرور جنباً إلى جنب مع جداول تتضمن حقوق المستخدمين فيما يتعلق بملفاتهم. ويجب ألا تكون جداول كلمات المرور مشفرة على نحو لا يمكن تعديله؛ وذلك لتجنب امكانية الاطلاع على محتوياتها [٢].

٣- حماية البيانات الشخصية عن طريق خاصية التوثيق: والتوثيق هو طريقة مفادها المحافظة على سرية البيانات عند استخدام الحاسب أو الأنظمة المعلوماتية. ويتم استخدامها عند مجرد التفكير في الدخول إلى البريد الإلكتروني

---

[١] – د/ فريد بايبر، علم التشفيرا، دار المحرر الأدبي، بدون سنة نشر، ص ١٥.

[٢] – د/ عبد العال الديربي، الجرائم الإلكترونية، دار المنهل، سنة ٢٠١٢، ص ١٩٤.

أو المدونة. وعلامة التوثيق هي نموذج يتيح للمستخدم أو صاحب البيانات الشخصية، الدخــول للتــطبيقات والمــلفات والمجلدات ونظام الحاسب بالكامل، ويكون لهذا المستخدم الصلاحية الكاملة والامتيازات حتى الخروج من النظام، كل ذلك بمجرد التسجيل [١].

وهناك صور أخرى لحماية أمن البيانات الشخصية، كخاصية النسخ الاحتياطي [٢]، وإجراءات إخفاء الهوية أو تجهيليها. وخواص التعرف على بصمة العين وبصمة الأصابع والتعرف على الوجه والتعرف على الصوت، مع اشتراط وجود التأمين الكافي لتلك الخواص. كما أن المعالج يلتزم بالبعد بهذه البيانات عن مصدر الخطر منذ البداية، كعدم وضع المعدات والتجهيزات المستعملة في عملية معالجة البيانات في ظروف أو أماكن تمكن من الوصول إليها ممن يُحظر عليهم مثل هذا الوصول وإجمالاً، يلتزم المعالج بالمحافظة على أمان البيانات المعالجة بأي وسيلة يراها مناسبة لذلك.

وتطبيقاً لما تقدم، قضت محكمة النقض الفرنسية بالتزام المسؤول عن إجراءات معالجة البيانات الشخصية، بتأمين هذه البيانات بما يراه ملائماً من الوسائل، بهدف منع الأشخاص غير المسموح لهم الوصول إلى البيانات الشخصية المعالجة أو الاطلاع عليها [٣].

وقضت ذات المحكمة أيضاً، بنفس الالتزام مقررةً التزام الشخص المسؤول عن عمليات معالجات البيانات الشخصية باتخاذ سائر الاحتياطات المطلوبة

---

[١] – د/ وليد السيد سليم، المرجع السابق، ص ١٧٤.

[٢] – وهي وسيلة تمكن الشخص من استعادة قواعد بياناته في حالة ما إذا تعرضت للسرقة أو التلف أو التدمير بفعل فيروس معين، كخاصية النسخ التي يوفرها تطبيق واتس آب لمستخدميه.

[3] - Cass. Crim , 30 octobre 2001 , n°: 99-82136.

واللازمة لأمان البيانات الشخصية، وذلك بالنظر إلى طبيعة هذه البيانات والمخاطر التي تكتنف عملية معالجتها [١].

وقضت أيضاً محكمة النقض الفرنسية في حكم حديث لها، بأن مزود الخدمة (المسؤول عن معالجة البيانات الشخصية) يلتزم باتخاذ التدابير اللازمة للمحافظة على أمان البيانات المعالجة من الاستخدام غير المصرح به، سواء عن طريق الاحتيال أو عن طريق القصد أو كان بسبب الإهمال الجسيم، مالم يكن الإخلال بتلك الحماية يرجع إلى فعل صاحب البيانات [٢].

ومن الناحية العملية، يصعب حصر الوسائل التي بها يتحقق عنصر الأمان للبيانات الشخصية المعالجة؛ لأنها مسألة متطورة وذات طابع نسبي تختلف من تقني إلى آخر، وتعتمد على القدرات الخاصة الذكائية لكل شخص في القدرة على مواجهة مصادر الخطر على هذه البيانات.

ثالثاً: طبيعة التزام المعالج بتأمين البيانات الشخصية:

يقتضي تحديد طبيعة التزام المعالج بتأمين البيانات محل المعالجة، بيان ما إذا كان هو التزام بتحقيق نتيجة أم أنه التزام ببذل عناية. فالمعروف أن الالتزام بتحقيق نتيجة، لا يكون إلا إذا حقق المدين (معالج البيانات الشخصية في هذا الشأن) النتيجة المبتغاة من الالتزام (تأمين البيانات الشخصية في هذا الصدد). أما الالتزام ببذل عناية، فيكفي فيه فقط أن يبذل المدين عناية الشخص المعتاد حتى وإن لم تتحقق النتيجة المطلوبة.

ومن التحديد السابق الخاص بالمقصود بالتزام المعالج بتأمين البيانات المعالجة، نجد أنه التزام ببذل عناية وليس التزام بتحقيق نتيجة. حيث يلتزم

---

[1] - Cass. Civ , 18 octobre 2016 , n° 15-15042.

[2] - Cass . com , 28 mars 2018 , n°: 16- 20.018.

بتوفير الأمان لهذه البيانات من منظور بذل عناية الشخص المعتاد من نفس المهنة إذا وُضع في نفس ظروف المعالج.

وما يؤيد هذه الطبيعة، هو أن الوسائل التكنولوجية الحديثة التي باتت تمثل تهديداً واضحاً لأمن البيانات الشخصية، أصبحت كثيرة جداً ومتنوعة. وأصبح هذا الأمر بمثابة مهنة لبعض الأشخاص ممن يبدعون ويتفننون في تلك الوسائل التي تمكنهم من اختراق قواعد البيانات الشخصية.

فعلى الرغم من المزايا الإيجابية الكثيرة التي حققتها الثورة التكنولوجية في حياتنا المعاصرة من حيث اعتبارها ضرورة لا غنى عنها، إلا أنها في ذات الوقت أداة متاحة للإخلال بالأمن والحقوق والحريات والخصوصية [١].

فشيوع النقل الرقمي للبيانات سهَّل عمليات استراق السمع والتجسس الإلكتروني، ومن هنا جاءت المخاطر التي تهدد الخصوصية الفردية، ويتمثل ذلك في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية البيانات الشخصية، وما نتج عن ذلك من امكانية استخدام تلك الشبكات والوصول إلى البيانات بصورة غير مشروعة [٢].

فمخاطر التقنيات التكنولوجية الحديثة استطالت عمليات معالجة البيانات الشخصية التي تتم على شبكات الحواسيب المربوطة ببعضها البعض والتي تتيح

---

[١] – د/ بدر خالد الخليفة؛ د/ سعيد عبد اللطيف اسماعيل، حماية الأمن القومي وأمن المعلومات والاتصالات والإنترنت ضد الإرهاب والجريمة المنظمة والاختراق والتجسس والمراقبة من المنظور الحقوقي والأمني والإستراتيجي، بحث منشور في مجلة كلية القانون الكويتية العالمية، العدد العاشر، يونيو ٢٠١٥، ص ١٨٢.

[٢] – د/ مصطفى موسى، مخاطر تهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية، بحث منشور في مجلة كلية القانون الكويتية العالمية، العدد العاشر، السنة الثالثة، يونيو ٢٠١٥، ص ٤٤٩.

تبادل المعلومات بين المراكز المتباعدة والمختلفة من حيث أغراض تخزين البيانات.

وهذا الأمر كان ولا زال محل اهتمام دولي واقليمي ووطني من أجل إقرار قواعد وإرساء مبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة في جمع البيانات وكفالة صحتها واتخاذ التدابير الأمنية اللازمة لمعالجتها وتخزينها ونقلها وإقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح طلب إلغاء البيانات ووجوب تحديد الغرض من جمعها واستخدامها وإقرار مبدأ مسؤولية القائمين على وظائف شبكات المعلومات والتواصل الاجتماعي لأي تجاوز أو مخالفة للمبادئ سواء الموضوعية أو الشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية[١].

وتُعتبر الأفعال التي تشكل اعتداءً على أمن البيانات الشخصية من الجرائم المعلوماتية [٢] التي يصعب حصرها تحت تقسيم محدد، غير أنه يمكن إبراز أهم تلك الاعتداءات والتي تتمثل في الأمور الآتية:

---

[١] – د/ مصطفى موسى، المرجع السابق، ص ٤٥٠، ٤٥١.

[٢] – الجريمة المعلوماتية هي كل سلوك إجرامي عمدي سواء كان إيجابياً أو سلبياً، يتم بمقتضاه الاعتداء بأية صورة من الصور على المعلومات أو البيانات المخزنة داخل الحاسب الآلي أو المخزنة داخل وسائط التخزين الملحقة بالحاسب الآلي أو التلاعب بهذه المعلومات بشكل يؤدي إلى حدوث جريمة على المعلومات المخزنة سواء على الحاسب أو الوسائط ..... د/عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً – دراسة مقارنة، دار النهضة العربية، سنة ٢٠١٠، ص ٥٩.

١- التجسس الإلكتروني: وهو الذي يحدث عن طريق عدة سبل تُستخدم لاختراق المواقع الإلكترونية أو اعتراضها من أجل سرقة بعض المعلومات والبيانات ذات الأهمية والخطورة لصاحبها أو لمن تخصة البيانات المعالجة.

والمشرع المصري تعرض صراحة في القانون رقم ١٧٥ لسنة ٢٠١٨[١] بشأن مكافحة جرائم تقنية المعلومات، لتحديد المقصود بمصطلحي اعتراض البيانات الشخصية واختراقها، وذلك في المادة الأولى من القانون المذكور. فعرف الاعتراض بأنه هو مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق.

وعرف المشرع المصري أيضاً في ذات المادة، الاختراق بأنه هو الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها.

كما أن المشرع المصري قد تعرض في المادة (١) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية، بتعريف خرق وانتهاك هذه البيانات بأنه:" كل دخول غير مرخص به إلي بيانات شخصية أو وصول غير مشروع لها، أو أي عملية غير مشروعة لنسخ أو إرسال أو توزيع أو تبادل أو نقل أو تداول يهدف إلي الكشف أو الإفصاح عن البيانات الشخصية أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها ..... ".

[١] – منشور بالجريدة الرسمية بالعدد ٣٢ مكرر(ج)، في ١٤ أغسطس سنة ٢٠١٨.

وغالباً ما يحدث اختراق قواعد البيانات الشخصية من قبل أشخاص هواة أو محترفون يُعرفون بالهاكرز [١]. وهذا الأخير نوعان، إما أن يكون هاكر آمن، وإما أن يكون هاكر غير آمن [٢]:

أ- الهاكر الآمن: ويحدث عن طريق الدخول غير المصرح به إلى نظم الحاسب بأي وسيلة، كالحصول بصورة غير قانونية على كلمة السر أو بواسطة التقاط موجات كهرومغناطيسية بحاسب خاص، وأحياناً يتم هذا الاختراق عن طريق رشوة المسؤولين عن معالجة البيانات الشخصية لتسهيل عملية الاختراق[٣].

وعلى الرغم من القدرة المؤكدة لهذا النوع من أنواع الهاكرز على اختراق قواعد البيانات الشخصية، إلا أنه هاكر غير مؤذ، أي لا يخترق بقصد الحاق الضرر أو الأذى بالمسؤول عن عملية معالجة البيانات الشخصية أو إيذاء صاحبها، ولكنه يخترق إشباعاً لدوافع الإثارة والمتعة والتحدي والشغف المعلوماتي. حيث يكون لدى بعض الأفراد غريزة في تحدي واختراق أجهزة

---

[١] – تنطبق كلمة الهاكر على الشخص الذي تكون لديه قدرات خاصة في مجال الحواسب الإلكترونية وأمن المعلومات. ويُطلق مصطلح الهاكرز على مجموعة من المبرمجين الأذكياء الذي يتحدون الأنظمة المعلوماتية المختلفة ويحاولون اقتحامها سواء كان ذلك بنية ارتكاب جريمة أو الحاق ضرر بصاحب البيانات المخترقة أو كان الاختراق محاولة منهم لإثبات قدراتهم الذاتية على تحدي تلك الأنظمة المعلوماتية واختراق أمنها..... د/ وليد السيد سليم، مرجع سابق، ص ٢٠٦.

[٢] – د/ عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت " الأحكام الموضوعية والجوانب الإجرائية "، دار النهضة العربية، سنة ٢٠٠٤، ص ٢٣٩، ٢٤٠.

[٣] – د/ مصطفى موسى، مرجع سابق، ص ٤٤٧.

الحاسب الآلي وقدرتها الرهيبة على حفظ المعلومات بأنظمتها الحمائية المختلفة، والشعور بلذة الانتصار على هذه الأجهزة [١].

وفي هذا النوع، لا توجد مسؤولية على معالج البيانات الشخصية في حالة حدوث اختراق لتلك البيانات، سواء كان ذلك بسبب تقصيره في تأمين النظام الحمائي للبيانات المعالجة أو كان الاختراق راجعاً لأسباب خارجة عن إرادته؛ وذلك لعدم وجود الضرر الموجب للمسؤولية في هذه الحالة. وإن كانت واقعة الاختراق في حد ذاتها تمثل اعتداءً على حماية تلك البيانات دون أن يتوقف ذلك على حدوث ضرر لصاحبها، والأمر هنا يتوقف على إرادة صاحب البيانات ذات الاختراق غير المصحوب بضرر، فيما يتعلق برفع دعوى المسؤولية المدنية.

ب- الهاكر غير الآمن: يُعرف هذا النوع أيضاً بالهاكر الخبيث، وفيه يقصد المخترق إلحاق الضرر والأذى بصاحب البيانات سواء بالاتلاف أو بالتخريب أو بالابتزاز [٢]. أي أنه يوضع في النظام المعلوماتي لتحقيق هدف غير مرخص به [٣].

ويستوي في هذا النوع الأسباب المؤدية إليه، أي سواء كان مرجعه السعي لتحقيق الأرباح المالية من قبل المخترق لاسيما وأن معظم الجرائم المعلوماتية تُرتكب لدوافع مالية، أو كان ذلك راجعاً إلى دوافع شخصية خاصة بالمعالج كشعوره بالحقد أو الضغينة تجاه صاحب البيانات فيتعمد الإهمال في تأمينها،

---

[١] – د/ عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص ١١٤، ١١٦؛ د/ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الطبعة الأولى، سنة ٢٠٠١، ص ٧٣.

[٢] – د/ عمر محمد أبو بكر بن يونس، مرجع سابق، ص ٢٤٠.

[٣] – د/ موسى مصطفى، مرجع سابق، ص ٤٤٢.

وأحياناً يكون مرجع هذا الإهمال تخفيض أجر المعالج أو احساسه بالإهمال والتهميش داخل المؤسسة التي يعمل بها، وأحياناً يكون مرجعه إلى مؤثرات خارجية كأن تمارس عملية الاختراق تحت تهديد أو ضغط يوقعه المخترق على إرادة المعالج وخصوصاً بشأن البيانات ذات الطابع المالي أو التجاري التي يغلب عليها طابع المنافسة والتجسس [١].

وفي هذا النوع من أنواع الهاكرز، تُثار مسؤولية المعالج المدنية لخطأه في تأمين البيانات إذا ثبت أنه لم يبذل العناية المطلوبة في تأمين تلك البيانات. وهنا تتحقق المسؤولية؛ لأن الضرر في هذه الحالة محقق ضد صاحب البيانات يستوي في ذلك تحقق الضرر بسبب الدوافع المالية أو الشخصية أو المؤثرات الخارجية للاختراق.

ولا يُعفى المعالج من المسؤولية في هذه الحالة إلا إذا ثبت أنه بذل العناية المطلوبة في تأمين البيانات الشخصية التي تم اختراقها، وأن هذا الأخير يرجع إلى أسباب لا دخل لإرادة المعالج فيها، وأن الاختراق كان سيحدث لو أن شخصاً غيره من المعالجين تولى مهمة تأمين البيانات المعالجة المخترقة.

٢- الفيروسات الإلكترونية: تعددت التعريفات الفقهية التي قيلت بشأن تعريف الفيروس الإلكتروني، غير أننا نرجح التعريف الذي قال به بعض المتخصصين في المجال المعلوماتي، بأنه:" برنامج يصممه بعض المتخصصين بهدف تخريبي مع إعطائه القدرة على ربط نفسه ببرامج أخرى، ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماماً " [٢].

---

[١] – د/ عبد الله حسين علي محمود، مرجع سابق، ص ٧١، ٧٤؛ د/ عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص ١٠٧، ١١٨، ١١٩، ١٢٠.

[٢] – د/ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، سنة ٢٠١١، ص ١٠٣.

وتتعدد أنواع الفيروسات الإلكترونية التي تمثل تهديداً لأمن البيانات الشخصية المعالجة، غير أن أشهر هذه الأنواع ما يلي:

أ- فيروس حصان طروادة: هو عبارة عن برنامج فيروسي لديه القدرة على الاختفاء في البرنامج الأصلي، وعندما يتم تشغيل البرنامج الأصلي ينشط الفيروس بصورة تلقائية ليبدأ نشاطه التدميري الذي قد يؤدي إلى إتلاف البرامج والبيانات، وقد يؤدي إلى تعديل أو تغيير البيانات والمعلومات، أو هلاك النظام بأكمله [١].

ب- فيروس الدودة الإلكترونية أو المعلوماتية: هو عبارة عن برنامج فيروسي ينقل نفسه من حاسب إلى آخر، ويستنسخ نفسه ويتكاثر داخل الذاكرة النشطة، التي تبدأ بمراقبة أي مسح بهدف العثور على مواطن الضعف فيها – أي في الذاكرة – ثم تنقل نفسها إلى الحاسبات الآلية الرقمية الأخرى [٢].

أي أنه برنامج له القدرة على تعطيل وإيقاف تشغيل النظام المعلوماتي بصورة تامة عن طريق نسخ نفسه عدة مرات وانتشاره عبر خطوط التوصيلات الإلكترونية، ويقوم بإصدار معلومات غير صحيحة تؤدي إلى ايقاف النظام المعلوماتي عن العمل. فهو فيروس يصيب جزء محدد من نظام المعالجة الآلية للبيانات، وهو الجزء الخاص بالتشغيل والذي يتكون من البرامج التي تتحكم في امكانيات الحاسب المسجل عليه البيانات الشخصية محل المعالجة [٣].

---

[١] – د/ موسى مصطفى، مرجع سابق، ص ٤٤٥؛ أ/ بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر العربي، سنة ٢٠٠٨، ص ٣٧٤.

[٢] – د/ مصطفى موسى، مرجع سابق، ص ٤٤٥.

[٣] – أ/ بلال أمين زين الدين، مرجع سابق، ص ٣٧٤، ٣٧٥.

ج- فيروس القنبلة المنطقية: وهو عبارة عن برنامج فيروسي أو جزء من برنامج، يُنفذ في وقت محدد أو على فترات زمنية منتظمة ويتم وضعه داخل النظام المعلوماتي بهدف تحديد ظروف أو حالة محتويات النظام من أجل تسهيل تنفيذ عمل غير مشروع [١]، أي اختراق قواعد البيانات الشخصية المعالجة.

وتكمن خطورة الاعتداء على البيانات الشخصية من خلال الفيروسات الإلكترونية، في الخصائص التي تتميز بها هذه الفيروسات من حيث تميزها بالطابع المعدي والانتقال بسرعة فائقة من جهاز إلى آخر والانتشار داخل الذاكرة والنسخ الذاتي السريع، وكذلك قدرة الفيروس على الاختفاء من مستخدم الجهاز الذي تكون مسجلة عليه البيانات الشخصية المعالجة بقصد التمويه عليه، وأيضاً قدرتها الكبيرة على اختراق النظام المعلوماتي واختراق كل سبل الحماية، وأخيراً قدرة الفيروس على تدمير النظام المعلوماتي بمسح البيانات المخزنة على وسائط التخزين أو على الأقل اصابة النظام بالبطء الشديد في التشغيل [٢].

وفي هذه الصورة من صور الاعتداء على أمن البيانات الشخصية، يكون المعالج مخلاً بالتزامه بالتأمين إذا لم يتخذ من الإجراءات ما يكون لازماً ومناسباً لدفع مخاطر الفيروسات السابقة. والحقيقة أنه لا توجد وسائل معينة يمكن اتباعها في هذا الشأن، غير أن المعالج يتعين عليه اتخاذ بعض التدابير وفقاً لخبرته، وعليه أن يطور من وسائل تأمين تلك البيانات بما يتماشى مع تطور المخاطر التي تحيط بأمن البيانات، وعليه أن يراجع نظم التشغيل الخاصة بأمن

---

[١] – د/ عبد الله حسين علي محمود، مرجع سابق، ص ١٢٢.

[٢] – د/ محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة، سنة ٢٠٠٣، ص ٢٩٢، ٢٩٣؛ د/ عزة محمود أحمد خليل، مشكلات المسئولية المدنية في مواجهة فيروس الحتسب، بدون ناشر، سنة ١٩٩٤، ص ٣٧ – ٤٠.

البيانات والملفات بصورة دورية بحثاً عن الفيروسات ومراجعة الأجهزة من وقت لآخر مسايرة لتطور هذه الفيروسات [١].

وهذا الأمر الأخير، أقرته اللائحة الأوربية رقم ٦٧٩/ ٢٠١٦ عندما ألزمت معالج البيانات الشخصية بمراجعة التقييم التأثيري الذي يجريه لمعرفة أثر عملية المعالجة على حماية البيانات محل هذه المعالجة، إذا تبين أن هناك تغيير في المخاطر التي تحيط بعملية بالمعالجة.

٣- تقنية الاسترجاع: ويُقصد بها تلك الوسيلة التي يستخدمها شخص ما قد يكون المسؤول عن عملية المعالجة أو شخص غيره، من أجل الحصول على معلومات أو بيانات موجودة في نظام معلوماتي بعد الانتهاء من تنفيذ عمل ما، وذلك من خلال البحث في سلات المهملات أو مناطق الذاكرة المغلقة والتي تُستخدم بواسطة الذاكرة المؤقتة لمعطيات الإدخال والإخراج، وهي لا تُمحى بعد إجراء حذفها. فالانتشار الواسع لأجهزة وشبكات الإنترنت قد سهل عملية الحفظ الفوري للبيانات وسهولة استرجاعها بعد حذفها.

وتمثل تقنية استرجاع المعلومات تهديداً خطيراً لأمن البيانات الشخصية وخصوصاً البيانات التي تكون موجودة أو محفوظة على هواتف الأفراد المحمولة، أو تلك التي تكون مسجلة على مواقع الإنترنت التي يتصفحونها أو يدخلون عليها ويسجلون عليها العديد من بياناتهم الشخصية، وخصوصاً الولوج إلى تلك المواقع من خلال هواتف الآندرويد التي يمكن من خلالها إعمال خاصية الاسترجاع بسهولة.

فالملفات التي يقوم الشخص بحذفها من على تلك الهواتف معتقداً عدم امكانية استرجاعها بعد الحذف، تكون قابلة للاسترجاع، كرسائل الواتس آب

---

[١] – د/ محمد حسين منصور، المرجع السابق، ص ٢٩٧.

والفيس بوك والرسائل النصية وأرقام الهواتف. ويرجع ذلك إلى أن النظام الحمائي بأجهزة الآندرويد لا يستطيع التغلب على خاصية الاسترجاع، وذلك على عكس أجهزة الآيفون التي تتميز بوجود نظام حمائي صارم للبيانات يصعب اختراقه أو الولوج إليه ممن لا يملك كلمة السر الخاصة بالتشفير الحمائي.

لذلك يجب أن تُزود أجهزة الآندرويد ما يمكن عن طريقة التغلب على خاصية الاسترجاع، أو على الأقل تطويرها وتزويدها بخصائص حمائية بحيث لا يجوز الاسترجاع إلا من خلال آلية محددة ولصاحب الهاتف فقط أو من يمكنه الاسترجاع من خلال الاطلاع على تلك الآلية بصورة مشروعة.

وفي هذه الصورة من صور الاعتداء، يكون المسؤول عن عملية المعالجة مخلاً بالتزامه بالمحافظة على أمن البيانات الشخصية المعالجة، إذا قام باسترجاع البيانات التي سبق له وأن عالجها وانتهى الغرض من معالجتها أو قام باسترجاعها بعد حذفها. ويكون مخلاً بالتزامه كذلك، إذا كان بوسعه التصدي لتقنية الاسترجاع لمنع الغير من العثور على تلك البيانات ولم يفعل ذلك، كل ذلك في إطار العناية المطلوبة منه.

وتتعدد الأضرار الناتجة عن الاعتداء على أمن البيانات الشخصية، كمحو هذه البيانات سواء كان ذلك بصورة كلية أو جزئية، أو سرقتها، أو إتلافها سواء كان ذلك بصورة كلية أو جزئية، وكذلك نسخ البيانات بصورة غير مشروعة، أو إدخال معلومات وهمية على البيانات الأصلية المعالجة، وأيضاً التلاعب في هذه البيانات. وإجمالاً كل ما يكون فيه ضرر لصاحب البيانات بسبب الاعتداء على بياناته، سواء وقع ذلك من المسؤول عن عملية المعالجة أو من قبل الغير [١].

[١] – يُنظر في ذلك تفصيلاً: م/ بهاء المري، شرح جرائم تقنية المعلومات " القانون رقم ١٧٥ لسنة ٢٠١٨ "، منشأة المعارف، سنة ٢٠١٩، ص ٦٩ وما بعدها.

وترتيباً على ما تقدم، تُثار المسؤولية المدنية للمسؤول عن عملية معالجة البيانات الشخصية، في كل صور الاعتداء السابقة على أمن تلك البيانات، سواء التي ذكرناها أو التي لم نذكرها. أي في كل فرض لا يكون فيه المسؤول قد بذل العناية المطلوبة للمحافظة على أمن البيانات التي عالجها، وذلك على حسب خبرته وكفاءته، وأيضاً على هدى خبرة وكفاءة من يعملون في نفس المجال وفقاً للمعيار المأخوذ به في الالتزام ببذل عناية.

والسؤال الذي يجب طرحه في الصدد، ما الذي يجب على المعالج فعله إذا حدث اختراق للبيانات الشخصية المعالجة بأي وسيلة اختراق؟

في هذا الصدد سنفرق بين موقف كل من المشرع الأوربي والمشرع الفرنسي والمشرع المصري، وذلك على النحو الآتي:

أولاً: موقف المشرع الأوربي:

أقرت اللائحة الأوربية رقم ٢٠١٦/٦٧٩ بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية، مبدأ اخطار الجهة الرقابية في حالة حدوث اختراق للبيانات الشخصية بأي وسيلة. وجاء ذلك في المادتين (٣٣، ٣٤) من اللائحة المذكورة، واللتين يُستفاد منهما وجود نوعين من الإخطار هما:

١- **الإخطار الفردي**: وهو الذي أقرته المادة (٣٣) من اللائحة، والتي بمقتضاها يلتزم المراقب أو المعالج بإخطار الجهة الرقابية بأي اختراق يحدث للبيانات الشخصية دون تأخير مبرر في موعد أقصاه ٧٢ ساعة من تاريخ العلم بواقعة الاختراق. وإذا تأخر المسؤول عن تقديم الإخطار في الموعد المحدد، وجب عليه تقديم أسباب التأخير. ويعتبر هذا الإخطار فردياً؛ تأسيساً على أنه

يقدم لجهة واحدة فقط وهي الجهة الرقابية المختصة فقط دون إخطار صاحب البيانات المخترقة [١].

ويجب أن يتضمن هذا الإخطار البيانات التي نصت عليها المادة (٣٣) والتي تتمثل في وصف طبيعة الاختراق الذي تعرضت له البيانات وذلك من خلال ذكر الفئات والعدد التقريبي لسجلات تلك البيانات، واسم ضابط حماية البيانات وتفاصيل الاتصال به أو أي جهة أخرى يمكن الحصول منها على مزيد من المعلومات، ووصف النتائج المحتملة لاختراق البيانات، والتدابير المتخذة أو المقترح اتخاذها من قبل المراقب لمواجهة هذا الاختراق أو التخفيف من آثاره السلبية المحتملة على الأقل [٢].

ومن أجل إحكام رقابة السلطة الرقابية المختصة على المراقب في تأمينه للبيانات الشخصية والتأكد من مدى التزامه بالتعليمات المنصوص عليها من

---

[1] - Art 33 of Regulation (EU) 2016/679 :" Notification of a personal data breach to the supervisory authority : In the case of a personal data breach , the controller shall without undue delay and where feasible , not later than 72 hours after having become aware of it , notify the personal data breach to the supervisory authority. Where the notification to the supervisory authority is not made within 72 hours , it shall be accompanied by reasons for the delay".

[2] - Art 33 of Regulation (EU) 2016/679 :" 4- The notification referred to in paragraph 1 shall at least: a- describe the nature of the personal data breach including where possible , the categories and approximate number of data subjects ……. b- communicate the name and contact details of the data protection officer ….. c- describe the likely consequences of the personal data breach …..d- describe the measures taken or proposed to be taken by the controller to address the personal data brrach , including , where appropriate . measures to mitigate its possible adverse effects ".

عدمه، يلتزم المراقب بتوثيق أي مخالفات تحدث للبيانات على أن يشمل ذلك الوقائع المتعلقة باختراق البيانات وآثار ذلك، والإجراءات الصحيحة المتخذة [١].

٢- الإخطار المزدوج: وهو الذي نصت عليه المادة (٣٤) من اللائحة الأوربية المذكورة. وهو مزدوجاً لكونه يتم من المراقب أو المعالج إلى الجهة الرقابية المختصة وصاحب البيانات المخترقة معاً، على عكس الإخطار الفردي.

ويحدث الإخطار المزدوج في الحالة التي يؤدي فيها اختراق البيانات الشخصية إلى إلحاق ضرر شديد وجسيم بحقوق وحريات الشخص المخترق بياناته على نحو يهدد خصوصيته تهديداً واضحاً وخطيراً. على أن يتم إخطار صاحب البيانات بلغة واضحة وبشكل يتضمن طبيعة هذا الاختراق والتدابير التي أُتخذت لمواجهته [٢].

واستثناءً على مبدأ التزام المراقب أو المعالج بالإخطار بواقعة الاختراق سواء كان الإخطار فردياً أو مزدوجاً، هناك حالات لا يلزم فيها هذا الإجراء، كحالة قيام المراقب بتنفيذ التدابير الحمائية المطلوبة أو المنصوص عليها سواء كانت تقنية أو تنظيمية كتشفير البيانات مثلاً، وحالة اتخاذ التدابير بصورة لاحقة

---

[1] - Art 33 of Regulation (EU) 2016/679 :" 5- The controller shall document any personal data breaches , comprising the facts relating to the personal data breach , its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article ".

[2] - Art 34 of Regulation (EU) 2016/679 :" Communication of a personal data breach to the data subject : 1- When the personaldata brrach is likely to result in a high risk to the rights and freedoms of natural persons , the controller shall communicate the personal data breach to the data subject without undue delay ".

على نحو يكفل عدم احتمال حدوث خطر كبير على حقوق وحريات صاحب البيانات وذلك في الفرض الذي تحدث فيه واقعة الاختراق بالفعل [١].

ثانياً: موقف المشرع الفرنسي:

تعرض المشرع الفرنسي لمسألة تأمين البيانات الشخصية على وجه العموم في المادة (٣٤) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، وتعرض بصفة خاصة لتلك الحماية بصدد البيانات الصحية الوطنية. حيث أنشأ المشرع الفرنسي لتأمين هذه البيانات لجنة تسمى ب" **لجنة تدقيق لنظام البيانات الصحية الوطنية** "، وذلك بمقتضى نص المادة (٦٥) من القانون المذكور [٢]. وسنتحدث عن هذه اللجنة من خلال النقاط الآتية:

---

[1] - Art 34 of Regulation (EU) 2016/679 :" 3- The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met : a- the controller has implemented appropriate technical and organizational protection measures , and those measures were applied to the personal data affected by the personal data breach , in particular those that render the personal data unintelligible to any person who is not authorized to access it , such as encryption . …. b- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize ….".

[2] - Art 65, loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 16) :" Dans le respect des missions et des pouvoirs de la Commission nationale de l'informatique et des libertés et aux fins de renforcer la bonne application des règles de sécurité et de protection des données, un comité d'audit du système national des données de santé est institué. Ce comité d'audit définit une stratégie d'audit puis une programmation, dont il informe la commission. Il fait réaliser des audits sur l'ensemble des systèmes réunissant, organisant ou mettant à disposition tout ou partie des données du système national des données de santé à des fins de recherche, d'étude ou d'évaluation ainsi que sur les systèmes composant le

système national des données de santé.

Le comité d'audit comprend des représentants des services des ministères chargés de la santé, de la sécurité sociale et de la solidarité, de la Caisse nationale d'assurance maladie, responsable du traitement du système national des données de santé, des autres producteurs de données du système national des données de santé, de l'Institut national des données de santé, ainsi qu'une personne représentant les acteurs privés du domaine de la santé. Des personnalités qualifiées peuvent y être désignées. Le président de la Commission nationale de l'informatique et des libertés, ou son représentant, y assiste en tant qu'observateur.

Les audits, dont le contenu est défini par le comité d'audit, sont réalisés par des prestataires sélectionnés selon des critères et modalités permettant de disposer de garanties attestant de leur compétence en matière d'audit de systèmes d'information et de leur indépendance à l'égard de l'entité auditée.

Le prestataire retenu soumet au président du comité d'audit la liste des personnes en charge de chaque audit et les informations permettant de garantir leurs compétences et leur indépendance.

Les missions d'audit s'exercent sur pièces et sur place. La procédure suivie inclut une phase contradictoire. La communication des données médicales individuelles ne peut se faire que sous l'autorité et en présence d'un médecin, s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé.

Pour chaque mission diligentée, des échanges ont lieu, si nécessaire, entre les personnes en charge des audits, le président du comité d'audit, le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique et le président de la Commission nationale de l'informatique et des libertés.

Si le comité d'audit a connaissance d'informations de nature à révéler des manquements graves en amont ou au cours d'un audit ou en cas d'opposition ou d'obstruction à l'audit, un signalement est adressé sans délai par le président du comité d'audit au président de la Commission nationale de l'informatique et des libertés.

Chaque mission diligentée établit un rapport relevant notamment les anomalies constatées et les manquements aux règles applicables aux systèmes d'information audités.

١-تعريف اللجنة: أنشئت هذه اللجنة تمشياً مع مهام وصلاحيات اللجنة الوطنية للمعلوماتية والحريات، ومن أجل تقرير التطبيق السليم لقواعد حماية البيانات وأمنها، فقد تم إنشاء لجنة تدقيق لنظام البيانات الصحية الوطنية، ومهمتها إجراء عمليات التدقيق على جميع الأنظمة التي تجمع أو تنظم أو توفر كا أو بعض نظم البيانات الصحية الوطنية لأغراض البحث أو الدراسة أو التقييم، وكذلك الأنظمة التي يتكون منها النظام الوطني للبيانات الصحية.

٢- تشكيل اللجنة: تضم لجنة التدقيق ممثلين عن الوزارات المسؤولة عن الصحة والضمان الاجتماعي والتضامن والصندوق الوطني للتأمين الصحي،

Si la mission constate, à l'issue de l'audit, de graves manquements, elle en informe sans délai le président du comité d'audit, qui informe sans délai le président de la Commission nationale de l'informatique et des libertés et le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique.

En cas d'urgence, le directeur général de la Caisse nationale d'assurance maladie peut suspendre temporairement l'accès au système national des données de santé avant le terme de l'audit s'il dispose d'éléments suffisamment préoccupants concernant des manquements graves aux règles précitées. Il doit en informer immédiatement le président du comité et le président de la commission. Le rétablissement de l'accès ne peut se faire qu'avec l'accord de ce dernier au regard des mesures correctives prises par l'entité auditée. Ces dispositions sont sans préjudice des prérogatives propres de la Commission nationale de l'informatique et des libertés.

Le rapport définitif de chaque mission est transmis au comité d'audit, au président de la Commission nationale de l'informatique et des libertés et au responsable du traitement audité.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise la composition du comité et définit ses règles de fonctionnement ainsi que les modalités de l'audit.

والمسؤول عن معالجة البيانات الصحية الوطنية، ومنتجي نظم البيانات الصحية الوطنية في المعهد الوطني للبيانات الصحية، وكذلك الشخص الذي يمثل الجهات الفاعلة في مجال الصحة، ويمكن تعيين الشخصية المؤهلة، ويحضر رئيس اللجنة الوطنية للمعلوماتية والحريات أو ممثله بصفة مراقب.

٣- كيفية مباشرة لجنة التدقيق لعملها: يدور الإطار المهني لتلك اللجنة في الخطوات الآتية:

أ- يتم إجراء التدقيق عن طريق تحديد محتوى هذه العمليات من قبل لجنة التدقيق بواسطة مزودي الخدمات الذين يتم اختيارهم وفقاً للمعايير والإجراءات التي توفر ضمانات كفاءتهم في نظم المعلومات المراجعة واستقلالهم عن الكيان المراجع.

ب- يقدم مزود الخدمة المختار إلى رئيس لجنة التدقيق، قائمة بالأشخاص المسؤولين عن كل تدقيق، والمعلومات اللازمة لضمان كفاءتهم واستقلالهم.

ج- توجد مهمام التدقيق على موقع لجنة التدقيق، وكذلك الإجراءات التي تتضمن نوعاً من التناقض كعدم جواز الاتصال بالبيانات الطبية الفردية إلا تحت إشراف الطبيب وبحضوره وذلك بالنسبة إلى المعلومات الواردة في المعالجة واللازمة لأغراض الطب الوقائي والبحوث الطبية والتشخيص الطبي وإدارة المعالجة أو إدارة الخدمات الصحية.

د- في حالة اللزوم، فإنه تُجرى في كل مهمة مطلوبة عمليات تبادل بين الأشخاص المسؤولين عن عمليات التدقيق ورئيس لجنة التدقيق والشخص المسؤول عن المعالجة المذكورة في المادة (١/١٤٦١) من قانون الصحة وكذلك رئيس اللجنة الوطنية للمعلوماتية والحريات.

هـ – إذا توافر لدى لجنة التدقيق علم بالمعلومات التي من المحتمل أن تبين أوجه قصور خطيرة في عملية التدقيق سواء قبله أو بعده، أو كانت هناك حالة معارضة أو عرقلة لإجرائه، فإنه يتم إرسال تقرير دون تأخير من قبل المراجع أو رئيس لجنة التدقيق إلى رئيس اللجنة الوطنية للمعلوماتية والحريات. ويجب في كل مهمة إعداد تقرير بالعيوب التي تم ملاحظتها والانتهاكات للقواعد المطبقة على نظم المعلومات المراجعة، وذلك أثناء إجراء التدقيق.

و– إذا وجدت لجنة التدقيق بعد إجراء التدقيق، أوجه قصور خطيرة، فإن عليها أن تبلغ دون تأخير رئيس لجنة التدقيق، الذي يلتزم من جانبه دون تأخير تبليغ كل من رئيس اللجنة الوطنية للمعلوماتية والحريات والمسؤول عن عمليات المعالجة المذكورة في المادة (١/١٤٦١) من قانون الصحة العامة.

ح– في حالة الاستعجال، يجوز للمدير العام للصندوق الوطني للتأمين الصحي أن يعطل بصورة مؤقتة الوصول إلى نظام البيانات الصحية الوطنية قبل انتهاء التدقيق إذا كان لديه مخاوف جدية مقلقة بدرجة كافية بشأن القواعد المذكورة عاليه. ويجب عليه على الفور إبلاغ رئيس لجنة التدقيق ورئيس اللجنة الوطنية للمعلوماتية والحريات، ولا يجوز استعادة الوصول إلى النظم التي تم تعطيلها إلا بموافقة رئيس اللجنة الوطنية للمعلوماتية والحريات من أجل الوقوف على التدابير التصحيحية التي أخذتها اللجنة المدققة، مع عدم الإخلال بصلاحيات اللجنة الوطنية للمعلوماتية والحريات في هذا الشأن.

ثالثاً: موقف المشرع المصري (الالتزام بالإخطار والإبلاغ):

حرصاً من المشرع المصري على حماية أمن البيانات الشخصية، فقد ألزم كل من المتحكم والمعالج بإبلاغ مركز حماية البيانات الشخصية بأي خرق أو انتهاك لهذه البيانات خلال اثنتين وسبعين ساعة من وقت علم أياً منهما بوجود

الخرق أو الانتهاك. وفي حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فوريا، وعلي المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فورًا، كما يلتزم بموافاة المركز خلال اثنتين وسبعين ساعة من تاريخ علمه بما يأتي :

١ – وصف طبيعة الخرق أو الانتهاك، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها.

٢ – بيانات مسئول حماية البيانات الشخصية لديه.

٣ – الآثار المحتملة لحادث الخرق أو الانتهاك.

٤ – وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية.

٥ – توثيق أي خرق أو انتهاك للبيانات الشخصية، والإجراءات التصحيحية المتخذة لمواجهته.

٦ – أي وثائق أو معلومات أو بيانات يطلبها المركز. وفي جميع الأحوال يجب علي المتحكم والمعالج، بحسب الأحوال، إخطار الشخص المعني بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات [١].

وختاماً لما بدأناه في هذا الصدد، نذكر بأن صور الاعتداء على البيانات الشخصية بالعرض السابق بيانه، تنطبق فقط على حالة المعالجة الإلكترونية لتلك البيانات دون المعالجة اليدوية أو الورقية. فالمعالجة الأولى تقتضي جمع وتخزين وحفظ البيانات عبر وسيط إلكتروني أياً كان نوعه مما يجعلها عرضة

[١] – المادة (٧) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

للاختراق، أما المعالجة الثانية فتتميز بقدر كبير من الأمان في معالجتها حيث يكفي أن توضع في مكان آمن بعيد عن العبث بها أو امكانية سرقتها.

المطلب الثاني

الخطأ المدني الناشئ عن إخلال المعالج بالالتزامات المتفرعة عن التزامه بتأمين البيانات الشخصية

ذكرنا منذ قليل ماهية وضوابط خطأ المعالج المدني الناشئ عن إخلاله بالتزامه بتأمين البيانات الشخصية التي يعالجها. غير أنه يتفرع عن ذلك حالات أخرى للخطأ المدني حال مخالفة المعالج لالتزامه بسرية البيانات التي يعالجها (فرع أول)، وكذلك مخالفته لضوابط ضوابط نقل هذه البيانات خارج الاتحاد الأوربي (فرع ثان).

الفرع الأول

الخطأ المدني الناشئ عن عدم المحافظة على سرية البيانات الشخصية

وسنتعرض لالتزام المعالج بالمحافظة على سرية البيانات الشخصية من خلال بيان المقصود بهذا الالتزام (أولاً)، وإقرار المشرع الفرنسي له (ثانياً)، وإقرار المشرع المصري له (ثالثاً). وذلك على النحو الآتي:

أولاً: المقصود بالالتزام بسرية البيانات الشخصية:

الالتزام بسرية البيانات الشخصية، يعني ضرورة التزام معالج هذه البيانات، بعدم إتيان أي أمر يكون من شأنه إفشاء أو الإفصاح عن تلك البيانات

التي يكون مطلع عليها بمقتضى وظيفته أو تحويلها أو الإعلان عنها أو نشرها أو تسريبها، وذلك لأي غرض من الأغراض سواء بمقابل أو بدون مقابل.

ولا يسري الالتزام بالسرية على المسؤول عن عملية المعالجة فقط أي المعالج الأصلي، بل يسري أيضاً على المعالج من الباطن، وكذلك أي شخص يُفوض أو يُناب للقيام بعمل من الأعمال الداخلة في عملية المعالجة، على نحو يمكّنه من الاطلاع على كل أو بعض البيانات الشخصية المعالجة.

ويتسم هذا الالتزام بصفة العمومية، أي أن المعالج أو المتحكم يلتزم به في كل المراحل، سواء عند جمع البيانات التي ستخضع للمعالجة أو عند معالجتها بالفعل أو بعد الانتهاء من معالجتها، على نحو يضمن في الأخير عدم وجود تهديد لصاحب البيانات بخصوص بياناته المعالجة ومنعاً لأساليب الابتزاز المالي التي قد يتعرض لها صاحب البيانات.

وإذا كان الالتزام بتأمين البيانات الشخصية هو التزام ببذل عناية، فإن الالتزام بسرية تلك البيانات هو التزام بتحقيق نتيجة؛ لأن أمر الحفاظ على هذه السرية يكون بيد المعالج أو المتحكم أو غيرهما ممن يطلعوا على البيانات اطلاعاً مشروعاً بحكم اشتراكهم في عملية المعالجة. وهنا يكون المعالج مسؤول عن إخلاله بهذا الالتزام إذا هو أفشى أو نشر أو حول أو أعلن عن البيانات التي يعالجها.

وتتمثل الحكمة من وجود الالتزام بسرية البيانات الشخصية، في تحقيق مصلحة المجتمع، والحفاظ على النظام العام [١]:

[١] – د/ معتز نزيه المهدي، الالتزام بالسرية والمسئولية المدنية " دراسة مقارنة "، دار النهضة العربية، سنة ٢٠٠٧، ص ٣٣، ٣٤.

أ- تحقق سرية البيانات الشخصية مصلحة المجتمع: فهذه المصلحة تقتضي المحافظة على سرية البيانات الشخصية منعاً لحدوث الفوضى بين أبناء المجتمع وألا تكون بيانات كل شخص في متناول الجميع بدون حاكم أو رابط ، وعدم زعزعة الاستقرار القانوني الذي تطمح إليه كل المجتمعات بنظمها القانونية المختلفة.

ب- تحقق سرية البيانات الشخصية متطلبات النظام العام: فالنظام العام يهدف في كل الأنظمة القانونية إلى حماية المصالح الأساسية لكل مجتمع أياً كان نوع هذه المصالح. ولا شك أن من ضمن هذه المصالح، صون سرية خصوصية الأفراد بصفة عامة وسرية بياناتهم الشخصية بصفة خاصة.

كما أن الالتزام بالسرية يجد مصدره في القواعد الأخلاقية التي تهتم بتحقيق الثقة بين الأشخاص؛ سعياً لتحقيق المثل العليا في المجتمع، وهو أمر من صميم مستلزمات النظام العام في أي دولة وفي أي نظام قانوني. بالإضافة إلى أن ذلك سيعود بالنفع على الأفراد من خلال انتشار الثقة المتبادلة بينهم وبين الدولة والأنظمة القانونية.

ثانياً- الإقرار التشريعي للالتزام بالسرية في القانون الفرنسي:

لقد سبق الذكر أن المادة (٣٤) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، قد أقرت التزام المعالج بتأمين البيانات الشخصية، وذات المادة أيضاً أقرت التزام المعالج بالمحافظة على سرية تلك البيانات.

غير أنه لا يعد تعارضاً مع الالتزام بسرية البيانات الشخصية ولا تهديداً أو انتهاكاً لها، ما أقرته المادة (٤٤) من القانون المذكور، من أن اطلاع الوكلاء المعتمدين والمفوضين من قبل اللجنة الوطنية للمعلوماتية والحريات على

البيانات المعالجة؛ لأن هؤلاء الأشخاص يمتد إليهم الالتزام بالسرية ولا يعد تعرضهم لهذه البيانات انتهاكاً لسريتها.

فهؤلاء الوكلاء المفوضون، يجب تزويدهم بجميع المستندات اللازمة لانجاز مهامهم أياً كانت الوسيلة في ذلك، ويحق لهم أخذ نسخة منها، ويحق لهم أيضاً جمع أي معلومات تفيدهم في القيام بما عُهد إليهم من مهام بأي وسيلة كالوصول إلى برامج الحاسب والبيانات المخزنة عليها.

ويُستثنى من ذلك، السرية المهنية التي تطبق على العلاقة بين المحامي وموكله، وكذلك سرية مصادر المعالجات الصحفية، والسرية الطبية. ففي هذه الأخيرة – أي السرية الطبية – لا يتعلق الاستثناء إلا بالسرية الفردية التي تكون بين الطبيب ومريضه، والتي لا يصح إجراؤها إلا بمعرفة الطبيب المعالج فقط ، أما معالجة البيانات التي تكون من لوازم الطب الوقائي أو البحوث الطبية أو التشخيص الطبي أو إدارة المعالجة أو إدارة الخدمات الصحية، فهي يصح إجراؤها من قبل الوكلاء المفوضين أو المعتمدين [١].

[1] - Art 65, loi n° 78 – 17 (Modifié par LOI n°2018-493 du 20 juin 2018 - art. 5) :" I.-Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en oeuvre d'un traitement de données à caractère personnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le procureur de la République territorialement compétent en est préalablement informé.

III. - Pour l'exercice des missions relevant de la Commission nationale de l'informatique et des libertés en application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et de la présente loi, les membres et agents mentionnés au premier alinéa du I du présent article peuvent demander communication de tous documents nécessaires à l'accomplissement

de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical.

Le secret médical est opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. La communication des données médicales individuelles incluses dans cette catégorie de traitement ne peut alors se faire que sous l'autorité et en présence d'un médecin.

En dehors des contrôles sur place et sur convocation, ils peuvent procéder à toute constatation utile ; ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Pour le contrôle de services de communication au public en ligne, les membres et agents mentionnés au premier alinéa du I peuvent réaliser toute opération en ligne nécessaire à leur mission sous une identité d'emprunt. À peine de nullité, leurs actes ne peuvent constituer une incitation à commettre une infraction. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées conformément au troisième alinéa du présent III. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise les conditions dans lesquelles ces membres et agents procèdent dans ces cas à leurs constatations.

Les membres et agents mentionnés au premier alinéa du I

ثالثاً– الإقرار التشريعي للالتزام بالسرية في القانون المصري:

لقد نص المشرع المصري صراحة على التزام المعالج بسرية البيانات الشخصية في المادة (٢/ أولاً / ٢) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، التي نصت على أن :" أولاً– مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات الصادر بالقانون رقم ١٠ لسنة ٢٠٠٣، يلتزم مقدمو الخدمة بما يأتي :..... 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 لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها .....".

كما نص المشرع المصري أيضاً على ضرورة سرية البيانات الشخصية في المادة رقم (٦/٤) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية، التي نصت على أنه:" مع مراعاة أحكام المادة (١٢) من هذا القانون، يلتزم المتحكم بما يأتي ..... ٦ – اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظا علي سريتها ، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قِبَل أي إجراء غير مشروع .....".

---

peuvent, à la demande du président de la commission, être assistés par des experts.

Il est dressé procès-verbal des vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation……".

فالسرية ما هي إلا انعكاس للحياة الخاصة أو الحق في الخصوصية، وكلاهما مصون وله حرمته التي لا يجوز انتهاكها أو التعدي عليها. وسرية البيانات الشخصية ما هي إلا مظهر من مظاهر الحق في الخصوصية المتعددة التي لا يجوز النفاذ إليها أو اقتحامها أو محاولة الاطلاع عليها سواء بصورة كلية أو جزئية.

وهذا المعنى أكدته المحكمة الدستورية العليا في حكم لها أصدرته سنة ١٩٩٥، وقضت فيه بأن :" ثمة مناطق من الحياه الخاصه لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي – دوماً ولاعتبار مشروع – ألا يقتحمها أحد ضماناً لسريتها، وصوناً لحرمتها، ودفعاً لمحاوله التلصص عليها، أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حداً مذهلاً، وكان لتنامي قدراتها على الاختراق أثر بعيد على الناس جميعهم وبياناتهم الشخصية التي غدا الاطلاع عليها وتجميعها نهباً لأعينها ولآذانها، وكثيراً ما ألحق النفاذ إليها الحرج والضرر بأصحابها، وهذه المناطق من خواص الحياة ودخائلها، تصون مصلحتين قد تبدوان منفصلتين، إلا أنها تتكاملان، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التي تكون – بالنظر إلى خصائصها وآثارها – أكثر اتصالاً بمصيره وتأثيراً في أوضاع الحياة التي اختار أنماطها، وتبلور هذه المناطق جميعها – التي يلوذ الفرد بها مطمئناً لحرمتها ليهجع إليها بعيداً عن أشكال الرقابة وأدواتها – الحق في أن تكون للحياة الخاصة تخومها بما يرعى الروابط الحميمة في نطاقها، ولئن كانت بعض الوثائق الدستورية لا تقدر هذا الحق بنص صريح فيها، إلا أن البعض يعتبره من

أشمل الحقوق وأوسعها، وهو كذلك أعمقها اتصالاً بالقيم التي تدعو إليها الأمم المتحضرة" [١].

وإذا كان التزام المعالج بسرية البيانات الشخصية، من الالتزامات المهنية الموضوعية الملقاة على عاتقة، ويُعمل به بصورة مطلقة من الناحية الشخصية أي يلتزم به المعالج الأصلي أو المعالج من الباطن أو أحد الموظفين التابعين لأي منهما [٢]، إلا أنه ليس مطلقاً من الناحية الموضوعية حيث يجوز الاطلاع عليها وفقاً لاعتبارات معينة وشروط محددة، كالاطلاع لدوافع أمنية أو وجود أمر مسبب من إحدى الجهات القضائية المختصة.

وترتيباً على ما تقدم، فإن المعالج يكون مخلاً بالتزامه بسرية البيانات الشخصية ومن ثم يكون مرتكباً لخطأٍ مدني، إذا هو أفشى أو أفصح أو أعلن أو نشر أو سرب بعض أو كل البيانات الشخصية التي يلتزم بمعالجتها للغير ممن لا يحق لهم الاطلاع على هذه البيانات، ما لم يكن هذا الاطلاع مشروعاً. والغير هنا هو كل شخص غير المعالج سواء الأصلي أو من الباطن، والموظفين المفوضين في المساهمة في عملية المعالجة، ومتلقي

---

[١] – المحكمة الدستورية العليا، جلسة ١٩٩٥/٣/١٨، القضية رقم ٢٣ لسنة ١٦ ق، مجموعة المبادئ التي قررتها المحكمة الدستورية العليا في أربعين عاماً ١٩٦٩ – ٢٠٠٩، الجزء السادس، ص ٥٦٧.

[٢] – وفي ذلك نصت المادة (٢/ رابعاً) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، على أنه " يلتزم مقدمو خدمات تقنية المعلومات ووكلاؤهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويُحظر على غيرهم القيام بذلك ".

البيانات، وصاحب هذه البيانات. يستوي في ذلك أن يكون الإخلال قبل المعالجة أو أثناءها أو بعدها [١].

الفرع الثاني

الخطأ المدني الناشئ عن الإخلال بضوابط نقل البيانات الشخصية خارج الحدود

إن مسألة نقل البيانات الشخصية خارج حدود الإقليمية للدول التي تُعالج فيها هذه البيانات، يحتوي على قدر كبير من المخاطرة والمساس بالأمن العام والمصالح الحيوية لتلك الدول. لذلك وجب إحاطة مسألة نقل البيانات بالضمانات التي توفر حماية أمنية كافية ومطمئنة لأصحابها. فهذا الاشتراط امتداد طبيعي لالتزام المعالج بتأمين الشخصية.

ونص على ضمانات نقل البيانات الشخصية خارج الحدود، كل من المشرع الأوربي والمشرع الفرنسي والمشرع المصري:

*** أقرت اللائحة الأوربية** رقم ٢٠١٦/٦٧٩ في المادة (٤٤) منها، أنه لا يجوز نقل البيانات الشخصية إلى دول غير دول الاتحاد الأوربي أو إلى منظمات دولية، إلا إذا وفر القائم بعملية المعالجة أياً ما كان، الضمانات المناسبة لتحقيق أمن هذه البيانات.

*** تعرض المشرع الفرنسي** لمسألة نقل البيانات الشخصية لدولة أو دول خارج الاتحاد الأوربي، مبيناً القاعدة العامة في ذلك والاستثناءات التي ترد

---

[١] – يُنظر في ذلك عموماً: د/ أحمد شوقي محمد عبد الرحمن، حقوق الغير المرتبطة بالعقد في القانون المدني والفقه والقضاء المصري والفرنسي، بدون ناشر، سنة ٢٠١٤، ص ٣ وما بعدها.

عليها، وذلك في المادتين (٦٨، ٦٩) من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحرية. وذلك على التوضيح الآتي:

أولاً- القاعدة العامة: نص المشرع الفرنسي في المادة (٦٨) من القانون المذكور [١]، على أنه لا يجوز للمسؤول عن عملية معالجة البيانات الشخصية أن ينقل هذه البيانات إلى دولة لا تنتمي إلى الاتحاد الأوربي إلا إذا كانت تلك الدولة تضمن مستوى كاف من حماية الخصوصية والحريات والحقوق الأساسية للأفراد عند معالجة تلك البيانات.

ويقع على عاتق المعالج تقدير مدى كفاية هذه الحماية في هذه الدول من أجل التحقيق الأمان اللازم للبيانات محل النقل. ويتحدد ذلك في إطار العديد من الضوابط التي وضعتها المادة (٦٨)، كالأحكام السارية في تلك الدولة، والتدابير الأمنية المطبقة لحماية البيانات الشخصية فيها، والخصائص المحددة لعملية المعالجة، والغرض من المعالجة ومدتها، وطبيعة البيانات المعالجة وأصلها ووجهتها.

---

[1]- Art 68, loi n° 78 – 17 (Créé par Loi n°2004-801 du 6 août 2004 - art. 12 JORF 7 août 2004) :" Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées ".

والحقيقة أن ترك تقدير توافر وسائل الأمان الواجب توافرها حال نقل البيانات الشخصية خاج الاتحاد الأوربي لمطلق تقدير المعالج في ضوء الاعتبارات السابقة، هو أمر ينتابه عدم الوضوح والتساهل نوعاً ما في توفير الحماية الكافية لنقل هذه البيانات. فمن الأفضل أن يوجد بجانب ذلك عدة ضوابط أخرى أكثر دقة ووضوحاً؛ ومنها [١]:

– إصدار مراسيم من وقت لآخر تحدد الدول التي توفر الضمانات الكافية لأمن البيانات ومن ثم يجوز النقل إليها وتلك التي لا توفرها ومن ثم لا يجوز النقل إليها.

– يُفضل أن تصدر اللجنة الوطنية للمعلوماتية والحريات تقارير توضح فيها الدول التي توفر الضمانات المناسبة وتلك التي لا توفرها صراحة لمدى إجازة عملية النقل من عدمها، وذلك من خلال الاعتماد على الضوابط الواردة في المادة (٦٨) للتأكد من مدى ملائمة الوسائل الحمائية في تلك الأنظمة القانونية.

– يفضل أن يكون مستوى حماية البيانات في الدولة التي سوف تُنقل إليها لا يقل عن مستوى الحماية الذي قرره كل من المشرع الفرنسي في القانون رقم ٧٨–١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات، واللائحة الأوربية رقم ٢٠١٦/٦٧٩ بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية وحرية نقل هذه البيانات.

<u>ثانياً– الاستثناءات الواردة على القاعدة السابقة</u>: أجاز المشرع الفرنسي نقل البيانات الشخصية إلى دولة خارج الاتحاد الأوربي على الرغم من عدم توافر الضمانات الكافية لتحقيق أمن هذه البيانات وذلك بمقتضى نص المادة (٦٩)

[١] – د/ سامح عبد الواحد التهامي، مرجع سابق، ص ٢٤٠، ٢٤١.

من القانون رقم ٧٨-١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات [١]، وذلك في الحالات الآتية:

---

[1] - Art 68, loi n° 78 – 17 (Créé par Loi n°2004-801 du 6 août 2004 - art. 12 JORF 7 août 2004):" Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :

1° A la sauvegarde de la vie de cette personne ;

2° A la sauvegarde de l'intérêt public ;

3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Il peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés ou, s'il s'agit d'un traitement mentionné au I ou au II de l'article 26, par décret en Conseil d'Etat pris après avis motivé et publié de la commission, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

La Commission nationale de l'informatique et des libertés porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres Etats membres de la Communauté européenne les décisions d'autorisation de transfert de données à

*** الحالة الأولى:** إذا وافق صاحب البيانات على نقلها دون تطلب توافر التدابير الأمنية التي نصت عليها المادة (٦٨) سالفة الذكر. ويجب أن تكون هذه الموافقة صريحة، حيث لا تكفي الموافقة الضمنية، وذلك على عكس موافقة صاحب البيانات بمعالجة بياناته حيث سبق وأن بينًا أنه تكفي لذلك الموافقة الصريحة أو الضمنية وفقاً للأصل العام. وتتمثل الحكمة من هذا الاستثناء في أن الحماية المقررة للبيانات الشخصية، إنما تتقرر للمصلحة الخاصة لصاحبها والذي يحق له التنازل عن هذه الحماية بموجب موافقته الصريحة.

ويجب ملاحظة أن هذه الموافقة تصدر من صاحب البيانات أو من له السلطة القانونية في ذلك. وتطبيقاً لذلك، قضت محكمة النقض الفرنسية بعدم مشروعية نقل الملفات التي تحتوي على بيانات شخصية، عندما قامت إحدى الشركات بـــتسليم عـــناوين البريد الإلـكتروني لعملائها وموظفيها لشركة أخرى؛ وذلك تأسيساً على أن تلك المعاملات تم إبرامها من قبل وكيل البائع الذي ليس لديه سلطة في ذلك [١].

*** الحالة الثانية:** إذا كان نقل البيانات الشخصية يمثل ضرورة في الحالات الآتية:

أ- إذا كان الغرض من نقل البيانات، حماية حياة صاحب هذه البيانات.

ب- إذا كان نقل البيانات ضروري لحماية المصلحة العامة.

ج- إذا كان في نقل البيانات احترام للالتزامات التي تسمح بإثبات حق أمام القضاء أو ممارسته أو الدفاع عنه.

---

caractère personnel qu'elle prend au titre de l'alinéa precedent ".

[1] - Cass . com , 29 avril 2014 , n°: 13 – 12.145 , R C D , 2014 , p. 639.

د- إذا كان نقل البيانات من أجل التشاور في ظل الظروف العادية بشأن السجل العام الذي هو بحكم الأحكام التشريعية أو التنظيمية يكون مخصص للمعلومات العامة ومفتوح للتشاور مع أي شخص تكون له مصلحة مشروعة.

هـ – إذا كان نقل البيانات من أجل تنفيذ عقد تم إبرامه بين المسؤول عن معالجة البيانات والشخص صاحب هذه البيانات، أو من أجل التدابير السابقة للعقد بناءً على طلب صاحب البيانات.

و- إذا كان نقل البيانات من أجل إبرام عقد أو تنفيذ عقد مبرم أو يتم إبرامه، ويتعلق بموضوع البيانات بين المسؤول عن عملية المعالجة والغير.

*** الحالة الثالثة:** يُستثنى من حكم المادة (٦٨) سالفة الذكر، حالة صدور قرار من اللجنة الوطنية للمعلوماتية والحريات يسمح لمعالج البيانات بنقلها. وكذلك تُستثنى عمليات نقل البيانات الخاصة بأمن الدولة أو الدفاع أو الأمن العام، وكذلك البيانات التي يكون الهدف من معالجتها منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو معاقبة مرتكبيها أو تنفيذ الإدانات الجنائية أو التدابير الأمنية، كل ذلك بموجب مرسوم يصدر من المجلس الدستوري بعد رأي مسبب ومنشور من اللجنة الوطنية للمعلوماتية والحريات، شريطة أن تضمن المعالجة مستوى كاف من حماية الخصوصية والحقوق والحريات الأساسية للأشخاص وخصوصاً الشروط التعاقدية أو القواعد الداخلية المعمول بها.

وفي حالة نقل البيانات بقرار من اللجنة الوطنية للمعلوماتية والحريات، فإن هذه اللجنة تقوم بإبلاغ لجنة الاتحاد الأوربي بقرارات الإذن بنقل البيانات الشخصية.

*** وبالنسبة لموقف المشرع المصري** من مسألة نقل البيانات الشخصية خارج حدود جمهورية مصر العربية، نجد أنه قد وضع لذلك قاعدة عامة واستثناءات عليها:

أ- القاعدة العامة: ونص عليها المشرع في المادة (١٤) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية، التي نصت على أنه:" يحظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلي دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوي من الحماية لا يقل عن المستوي المنصوص عليه في هذا القانون، وبترخيص أو تصريح من المركز. وتحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها ".

ب- الاستثناءات الواردة على القاعدة العامة: وجاء النص عليها في المادة (١٥) من القانون المذكور، والتي جاء بها أنه يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه، نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلي دولة لا يتوافر فيها مستوي الحماية المشار إليها في المادة السابقة، وذلك في الحالات الآتية :

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

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

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

٤ – تنفيذ إجراء خاص بتعاون قضائي دولي.

٥ – وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة.

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

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

وترتيباً على ما تقدم، يكون المعالج مخلاً بالتزامه في حالة نقل البيانات الشخصية إلى دولة خارج الحدود، ومن ثم يكون مرتكباً لخطأٍ مدني، إذا هو سمح بالنقل دون التأكد من وجود مستوى كافٍ من الأمان المعلوماتي يحفظ خصوصية الفرد وحقوقه وحرياته الأساسية على بياناته، وذلك من خلال تقديره لمعايير النقل التي أوردتها المادة (٦٨) من قانون المعلوماتية والحريات بالنسبة للمشرع الفرنسي، والواردة في المادة (١٤) من القانون رقم ١٥١ لسنة ٢٠٢٠ بالنسبة للمشرع المصري.

فيكون المعالج أو المتحكم مخلاً بالتزامه إذا سمح بنقل البيانات الشخصية على الرغم من أن الأحكام السارية في البلد المنقول إليها هذه البيانات لا توفر المستوى الملائم لحمايتها، أو إذا اتضح ذلك للمعالج من التدابير الأمنية التي تطبقها هذه الدولة وأنها دون المستوى المطلوب، أو كان واضحاً له من الغرض من المعالجة ومدة هذه المعالجة وطبيعة البيانات وأصلها ووجهتها أن هذه الدولة لا توفر الأمان المطلوب للبيانات محل النقل.

غير أن نقل البيانات الشخصية في بعض الحالات الاستثنائية، لا يشكل خطأ من جانب المعالج. كما إذا تم النقل بموجب الموافقة الصريحة لصاحب البيانات، أو كان النقل حمايةً لحياته أو لتحقيق المصلحة العامة أو من أجل

إثبات حق أمام القضاء أو ممارسته أو الدفاع عنه، أو كان النقل متعلق بالبيانات المتاحة للجمهور ونُقلت إلى شخص له مصلحة مشروعة في النقل، أو نُقلت بمناسبة تنفيذ عقد أُبرم بين المعالج وصاحب البيانات أو عقد أُبرم أو سيتم إبرامه بين المعالج وشخص من الغير يخص بياناته – أي بيانات الشخص المعني –، وكذلك حالة ما إذا كانت اللجنة الوطنية للمعلوماتية والحريات هي التي أعطت الإذن بنقل البيانات في الحالات التي قررتها المادة (٦٩) من قانون المعلوماتية والحريات، أو إذا توافرت حالة من الحالات المنصوص عليها في المادة (١٥) من القانون رقم ١٥١ لسنة ٢٠٢٠.

الـخـاتـمـة

سنتعرض بمشيئة الله تعالي لخاتمة البحث المعنون بالخطأ المدني الناشئ عن الإخلال بالحماية القانونية للبيانات الشخصية ، من خلال بيان نتائج البحث (أولاً)، ثم التوصيات التي انتهينا إليها (ثانياً). وذلك على العرض التالي:

أولاً: نتائج البحث :

لقد أورد كل من المشرع الفرنسي والمشرع المصري والمشرع الأوربي، العديد من الضوابط اللازمة لمشروعية عمليتي جمع ومعالجة البيانات الشخصية، والتي يترتب على مخالفتها وجود خطأ مدني يستوجب المسؤولية المدنية، سواء بالنسبة للشخص المسؤول عن الجمع والمعالج أو بالنسبة لغيره كالمتحكم أو المسؤول عن حماية البيانات. ويتوافر هذا الخطأ في الحالات الآتية:

١- إذا تم تجمـيع البيانات االشخصية بدون موافقة صاحب هذه البيانات. أو إذا توافرت هذه الموافقة، إلا أن المسؤول عن عملية الجمع أو المعالجة قد استخدم البيانات مرة أخرى بالتعارض من الهدف من جمعها أو معالجتها، أياً كانت الوسيلة في ذلك، أي سواء تم الجمع عن طريق تقنية الكوكيز (Cookies) أو باستخدام بيانات النقر، أو عن طريق تقنية (R F I D)، أو عبر مواقع التواصل الاجتماعي، أو عن طريق تقنية دمج المعلومات (Data Fusion)، أو عن طريق تقنية فك تشفير الأنماط، أو عن طريق ممارسات التسويق الخادعة.

٢- إذا كانت عملية المعالجة غير مشروعة، أياً ما كان مظهر عدم المشروعية، سواء تمت المعالجة بصورة عشوائية بدون هدف محدد، أو كانت المعالجة غامضة أي تخلق لبساً في ذهن صاحب البيانات بشأن الهدف من

معالجة بياناته، وكذلك إذا كان الهدف من المعالجة غير مشروع وذلك بأن كانت البيانات محل الجمع أو المعالجة غير ملائمة أو غير دقيقة أو غير كافية أو غير مناسبة للجمع أو المعالجة أو كانت منعدمة الصلة بالهدف الذي من أجله تم جمع البيانات أو معالجتها.

٣- إذا لم يقم المسؤول عن عملية المعالجة بتنفيذ أي من الالتزامات الملقاة على عاتقه. كما إذا يعلم صاحب البيانات بهويته، أو لم يعلمه بالغرض من عملية المعالجة، أو إذا لم يخبره بمدى إلزامية أو اختيارية البيانات محل المعالجة، أو إذا لم يخبره بالعواقب المحتملة للخطأ في الإجابة على البيانات محل المعالجة، أو إذا لم يعلمه بالفئات المرسل إليهم البيانات المعالجة، أو إذا لم يعلمه بالحقوق المقررة له على بياناته، أو إذا لم يعلمه بالإجراءات المقترحة في حالة نقل بياناته إلى دولة ليست عضواً في الاتحاد الأوربي أو خارج جمهورية مصر العربية، وأخيراً إذا لم يعلمه بمدة حفظ بياناته المعالجة.

٤- إذا أُجريت عملية المعالجة رغم عدم علم صاحب البيانات الشخصية محل المعالجة أو رغم معارضته لذلك. ما لم تكن المعالجة تُجرى تنفيذاً لالتزام قانوني يقع على عاتق المعالج، أو كان الغرض منها الحفاظ على حياة الشخص المعني بمعالجة بياناته الشخصية، أو كان في إجراء المعالجة تنفيذاً لمهمة عامة يتولاها المسؤول عن المعالجة أو متلقيها، أو إذا كانت المعالجة تتم لتنفيذ عقد كان صاحب البيانات المعالجة طرفاً فيه، أو إذا كان الغرض من المعالجة يحقق مصلحة مشروعة للمسؤول عن المعالجة أو لمتلقي البيانات.

٥- إذا أُجريت معالجة للبيانات الشخصية ذات الطابع الحساس التي تمس الحياة الاجتماعية أو الصحية لصاحب البيانات أو معتقداته الدينية أو آرائه السياسية أو انتماءاته النقابية أو أصوله العرقية أو الجنسية بدون موافقته

الصريحة، ما لم يتعلق الأمر بحالة من الحالات المستثناة من ذلك على النحو الذي بينَّاه في موضعه.

٦- إذا قام المسؤول عن عملية المعالجة بمعالجة البيانات الشخصية المتعلقة بالجرائم والإدانات والتدابير الأمنية، يستوي في ذلك الإدانات المدنية والجنائية، وذلك بالنسبة للمشرع الفرنسي.

٧- إذا لم يحصل المسؤول عن عملية المعالجة على إجازة قانونية مسبقة من الجهة الإدارية المختصة. ما لم تكن عملية المعالجة متوقفة على الحصول على ترخيص وزاري أو ترخيص قضائي. وكذلك الحال، إذا لم يقم المعالج – أو المسؤول عن حماية البيانات الشخصية في القانون المصري – بإجراء تقييم تأثيري لعملية المعالجة على حماية البيانات الشخصية.

٨- إذا أهمل المسؤول عن عملية المعالجة – وكذلك المتحكم أو المسؤول عن حماية البيانات في القانون المصري – في تأمين البيانات محل المعالجة، من منظور التزامه ببذل العناية المطلوبة في تحقيق أمن البيانات وسلامتها بأي وسيلة تتراءى له. ويثور الخطأ المدني في حالة إخلاله ببذل العناية اللازمة لذلك في أي صورة يحدث فيها اختراق لسلامة وأمن البيانات المعالجة، سواء عن طريق التجسس الإلكتروني، أو الفيروسات الإلكترونية، أو عن طريق تقنية الاسترجاع. ويثور الخطأ المدني أيضاً، في حالة حدوث اختراق للبيانات الشخصية ولم يخطر المعالج الجهة الرقابية المختصة في الوقت المحدد.

٩- إذا لم يحافظ المسؤول عن عملية معالجة البيانات الشخصية – ومعه المتحكم في القانون المصري – ، على سرية البيانات التي يعالجها. وكذلك إذا لم يراع الضوابط اللازمة لمشروعية نقل البيانات الشخصية خارج الحدود

الإقليمية للدولة التي تُعالج فيها هذه البيانات، ما لم يتعلق الأمر بحالة من الحالات المستثناة من تلك الضوابط .

ثانياً: توصيات البحث:

١- نوصي بأن تكون مسألة الموافقة على معالجة البيانات الشخصية، موافقة صريحة وقاطعة الدلالة على قبول عملية المعالجة، ما لم يتعلق الأمر بحالة من الحالات المستثناة من الحصول على هذه الموافقة، وهذا بالنسبة للمشرع الفرنسي فقط دون المشرع المصري الذي اشترط هذه الموافقة بالفعل في المادة (٢) من القانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

٢- نوصي المعالجين والمتحكمين والمسؤولين عن حماية البيانات الشخصية، وكل من له دور في تأمين البيانات الشخصية، ببذل أقصى عناية ممكنة في حدود خبراتهم وكفائتهم وأمانتهم ونزاهتهم في تأمين هذه البيانات. ونوصيهم كذلك بضرورة مراجعة النظم التأمينية الخاصة بالبيانات الخاضعة للمعالجة بشكل دوري وعدم الاكتفاء أو الاعتماد على سبل حماية معينة بصورة ثابتة؛ وذلك بسبب تطور وسائل الاختراق بصورة شبه يومية وبطريقة مذهلة وذات خطورة كبيرة على أمن هذه البيانات.

٣- نوصي بتدريب وتوعية المعالجين والمتحكمين والمسؤولون عن حماية البيانات الشخصية، عن طريق عقد ندوات وورش عمل تدريبية لهم، ويُفضل أن تتم على نطاق كبير من أجل ضمان أكبر استفادة ممكنة من خبرات وأفكار التقنيين الفنيين في مجال سلامة البيانات الشخصية. ونوصي أن يتم تفعيل هذا الأمر على كافة المستويات، سواء الوطنية أو الإقليمية أو الدولية؛ وخصوصاً وأن الاعتداء على البيانات الشخصية من الجرائم المعلوماتية التي تتميز بالطابع

عبر الإقليمي الذي يتخطي حدود الدولة الواحدة، ولا مجال لمواجهة ذلك إلا بالتكاتف الدولي.

٤- نوصي بأن تلتزم مواقع المتاجر الإلكترونية بسرية البيانات الشخصية التي تتحصل عليها من الأفراد الذين يتعاملون معها، والالتزام بضوابط التسويق الإلكتروني المباشر التي نص عليها المشرع المصري في المادتين (١٧، ١٨) من القانون رقم ١٥١ لسنة ٢٠٢٠. حيث يجب ألا تكون هذه المعلومات بمثابة رصيد كبير وبخس للمتاجر الأخرى، ويتم تداولها بين المتاجر وبعضها البعض من أجل إرسال الإعلانات الدعائية بما يتوافق مع الميول الاستهلاكية للأشخاص المعنيين بهذه البيانات، والتي تُعرف عن طريق الأماكن التي يدلون فيها ببياناتهم الشخصية، وذلك حفاظاً على مصلحة المجتمع المتمثلة في خلق نوع من الثقة بين العميل والمتجر الإلكتروني الذي يتعامل معه، بالإضافة إلى المحافظة على النـظام العام الذي يعد من أهدافه الحفاظ على خصوصية الأفراد، ناهيك عن شعور الأفراد بالأمان على بياناتهم على نحو يزيد من قوتهم الشرائية لكثير من السلع بصورة إلكترونية دون خوف على سرية بياناتهم، بما يعود بالنفع على المصلحة العامة من الناحية الإقتصادية.

٥- نوصي بضرورة اهتمام الأفراد بقراءة سياسات الخصوصية التي تتواجد على المواقع التي يقوم الأفراد بزيارتها أو تصفحها، ويفصحون عليها عن الكثير من بياناتهم الشخصية، على نحو يهدد خصوصية وأمن هذه البيانات، لا سيما وأن الكثير من المواقع تتطلب الإفصاح عن الكثير من البيانات الشخصية ويتذرع القائمون على هذه المواقع بعدم حدوث انتهاك للبيانات تأسيساً على اطلاع الأفراد على سياسة الخصوصية لتلك المواقع وأنهم كانوا على علم بها عند إفصاحهم عن بياناتهم. وعملياً، نجد أن الكثير من الأفراد لا يهتمون بقراءة

بنود هذه السياسة؛ وذلك بسبب الاستعجال وعدم الاكتراث بقراءة هذه السياسة، وهو ما يضر بهم في الأخير.

٦- نوصي بأن توزع منشورات داخلية داخل كل جهة تتعامل مع البيانات الشخصية للأفراد أو تتحصل عليها بأي طريقة سواء بصورة مباشرة أو غير مباشرة، باحترام سرية هذه البيانات. وضرورة التأكيد على أن التعامل في هذه البيانات يدور فقط في إطار الغرض من جمعها أو معالجتها. كما يلزم فرض جزاءات داخلية على من ينتهك القواعد التي تتضمنها هذه المنشورات، ويجب تفعليل هذه الجزاءات بأقسى الطرق؛ وذلك إيماناً بأهمية وخطورة هذه البيانات بالنسبة لأصحابها ولمصلحة المجتمع ككل.

قائمة المراجع

أولاً:المراجع باللغة العربية:

أ- المراجع العامة:

- **أ/ عبد السلام عبد الجبار:** الدراسات السابقة، ورقة بحثية ضمن متطلبات الحصول على درجة الماجستير من كلية الدعوة وأصول الدين بالجامعة الإسلامية بالمدينة النبوية، سنة ١٤٣٢ – ١٤٣٣ هـ .

- **د/ أحمد أبو بكر الهوش:** الأرشفة الإلكترونية " الأسس النظرية والمعرفة العملية " ، دار حميثر للنشر والترجمة، سنة ٢٠١٨.

- **د/ أحمد شوقي محمد عبد الرحمن:** حقوق الغير المرتبطة بالعقد في القانون المدني والفقه والقضاء المصري والفرنسي، بدون ناشر، سنة ٢٠١٤.

- **د/ جيمس كيروز؛ د/ كيث روس:** شبكات الحاسب والإنترنت " أسس ومبادئ الشبكات والإنترنت "، ترجمة : د/ السيد محمد الألفي؛ د/ رضوان السعيد عبد العال، دار العبيكان، سنة ٢٠١١، الطبعة الرابعة.

- **د/ سامح عامر:** التميز الإداري في القرن الحادي والعشرين، الناشر : دار المنهل، سنة ٢٠١٣.

- **د/ عزة محمود أحمد خليل:** مشكلات المسئولية المدنية في مواجهة فيروس الحتسب، بدون ناشر، سنة ١٩٩٤.

- **د/ فريد بايبر:** علم التشفيرا، دار المحرر الأدبي، بدون سنة نشر.

- **د/ محمد حسين منصور:** المسئولية الإلكترونية، دار الجامعة الجديدة، سنة ٢٠٠٣.

- **د/ معتز نزيه المهدي:** الالتزام بالسرية والمسئولية المدنية " دراسة مقارنة "، دار النهضة العربية، سنة ٢٠٠٧.

ب- المراجع المتخصصة

- **أ/ بلال أمين زين الدين:** جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر العربي، سنة ٢٠٠٨.

- **د/ أيمن أحمد الدلوع:** المسئولية المدنية الناشئة عن الممارسات غير المشروعة عبر مواقع التواصل الاجتماعي، دار الجامعة الجديدة، سنة ٢٠١٨.

- **د/ عبد العال الديربي:** الجرائم الإلكترونية، دار المنهل، سنة ٢٠١٢.

– **د/ عبد العزيز بن محمد العبيد:** المسئولية الجنائية في الإعلانات التجارية، دراسة تأصيلية مقارنة، الناشر : دار المنهل، سنة ٢٠١٦.
– **د/ عبد الله حسين علي محمود:** سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الطبعة الأولى، سنة ٢٠٠١.
– **د/ عمر أبو الفتوح عبد العظيم الحمامي:** الحماية الجنائية للمعلومات المسجلة إلكترونياً – دراسة مقارنة، دار النهضة العربية، سنة ٢٠١٠.
– **د/ عمر محمد أبو بكر بن يونس:** الجرائم الناشئة عن استخدام الإنترنت " الأحكام الموضوعية والجوانب الإجرائية "، دار النهضة العربية، سنة ٢٠٠٤.
– **د/ محمد علي العريان:** الجرائم المعلوماتية، دار الجامعة الجديدة، سنة ٢٠١١.
– **د/ وليد السيد سليم:** ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، سنة ٢٠١٢.
– **م/ بهاء المري:** شرح جرائم تقنية المعلومات " القانون رقم ١٧٥ لسنة ٢٠١٨ "، منشأة المعارف، سنة ٢٠١٩.

ج– الأبحاث:

– **د/ بدر خالد الخليفة؛ د/ سعيد عبد اللطيف اسماعيل:** حماية الأمن القومي وأمن المعلومات والاتصالات والإنترنت ضد الأرهاب والجريمة المنظمة والاختراق والتجسس والمراقبة من المنظور الحقوقي والأمني والإستراتيجي، بحث منشور في مجلة كلية القانون الكويتية العالمية، العدد العاشر، يونيو ٢٠١٥.
– **د/ سامح عبد الواحد التهامي:** الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، القسم الأول، بحث منشور في مجلة الحقوق الكويتية، العدد الثالث، المجلد الخامس والثلاثون، سنة ٢٠١١.
– **د/ شريف خاطر:** حق الاطلاع على البيانات الشخصية في فرنسا، بحث منشور في مجلة القانون الكويتية العالمية، العدد التاسع، السنة الثالثة، مارس ٢٠١٥.
– **د/ مصطفى موسى:** مخاطر تهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية، بحث منشور في مجلة كلية القانون الكويتية العالمية، العدد العاشر، السنة الثالثة، يونيو ٢٠١٥.

ثانياً: المراجع الأجنبية:

أ– المؤلفات والرسائل العلمية:

- AVOINE (G.): Sécurité de la R F I D , Comprendre la technique sans être technician , in la secrete de l’individu

numérise , réflexions prospectives et internationals , sous la direction de LACOUR (S.) , L'Harmattan , 2008 .

- **Céline CASTETS – RENARD** : commerce électronique , Dalloz , Juillet 2016 (actualization : octobre 2018).

- Céline CASTETS-RENARD : La protection des données personnelles dans les relations internes à l'Union européenne – La protection des données personnelles en matière civile et commercial , Dalloz , Octobre 2018 (actualisation : Mai 2019).

- **CHASSI GNEUX (C.)** : L'encaclrement juridique du traitment des données personnelles sur les sites de commerce en ligne , Thése , Université Panthéon Assas , 2003 .

- **EVSOUSSAN (A.)**: In formatiqe et libertés , Edition francis Lefebvre , 2008 .

- Fabrice NAFTALSKL , OEUVRE COLLECTIVE Sous LA DIRECTION DEPHILIPPE – HENRI DU THEIL : Fonctionnement de l'association , partie 4 , 2016 (actualization : Avril 2019).

- Fanny Rogue : Capacité et consentement au traitement de données à caractère personnel et au contrat , AJ contrat 2019.

- **Fanny Rogue** : op. cit , p. 370 ؛ Hugues Ciray , Du contrôle d'un systéme de traitment automatisé de données personnelles , 2 juillet 2018 , Dalloz actualité , 2 juillet 2018.

- FERAL-SCHUHL : Cyber droit , le droit ā l'épreuve de l'internet , Dalloz , paris , 2000 .

- Fréderique CHOPIN : Cybercriminalité , Juillet 2013 (actualization : Avril 2018) , Dalloz.

- **LABOILE (X.) :** Aspects Juridique et éthiques du recueil des donnée médicales aux fins d'analyses épidémiologiques , Thése , Université de Bordeaux IV , 2000.

- **Matthieu Dary** : L'enjeu de la conformité ā la réglementation des données personnelles pour les collectivités territoriales , Nina Gosse , A J Colletivités terrtoriales , 2018 .

- Mike Puglia , Albert Puglia , V.Daniel Hunt : R F I D , AGuide to Radio Frequency identification , John Wiley , Sans , 2007.

ب- المقالات والتقارير والتعليقات:

− Appréciation de la légalité du décretcréant un traitement de la données personnelles relative aux étrangers faisant l'object d'une mesure d'éloignement , dit Elol – Conseil d'Etat 30 décembre 2009 , n°: 31 2051 31 760 , Recueil Lebon – Recueil des décisions du Conseil d'Etat , 2009.

- C N I L , Délibération 2006 – 103 , du 27 avril 2006.

- C N I L : 3éme rapport d'activité , 15 octobre 1981 – 15 octobre 1982 , La document Française , Paris , 1983 , p. 148.

- C N I L : 6 éme rapport d'activité , 1985 , La documentation Française , paris , 1986 , p. 95.

- C N I L : Délibération n°: 92 – 130 , du 24 november 1992 , portant avis sur la mise en oeuvre , par le minister de l'education nationale , d'un traitement automatisé d'informations nominatives dénommé scolarité….. www.legimonible.fr/cnil.

- C N I L : Délibération n°: 96 – 035 du 16 avril 1996 , relative ā la mission de verification sur place effectuée le 4 avril 1996 auprés de l'Institut Louis Harris …..

- C N I L : Internet et la collecte de données personnelles auprés des mineurs , rapport adopté le 21 juin 2001 , present par Mme Céile ALVERQNAT

- C N I L: Délibération , n°: 2006 – 048 , du 23 Février 2006.

- C N I L: Délibération , n°: 2019 – 001 , du 21 janvier 2019 : Delphine Castel , protection des données personnelles –

Réglementation – Des association Font condemner . Google ā un amende – juris association , 2019 , n°593 , p. 11 , Dalloz , 15 Février 2019.

- Christian GUERY , instruction preparation pouvoirs propres du juge d›instruction , juin 2018 (actualisation : juillet 2019) , Dalloz , N: 523.

- Le juge référé mesures utiles et la messagerie électronique du détenu – Conseil d'Etat , 5 mars 2018 , n°: 414859 , Recueil Lebon

- L'utilisation de cookies constitue un traitement de données – conseil d'Etat 6 juin 2018 – Le bon 2018 , Recueil Lebon – Recueil des decisions du conseil d'Etat 2018.

- M. Falala , Réponse ministérielle à question écrite n° 29894 , JOAN Q 19 octobre 2004 , p. 8112 .

- Moteur de recherché (Google) : responsabilité du traitement des données personnelles – cour de justice de l'Union européenne , 13mai 2014 , Recueil Dalloz , 2014.

- Nicolas Nalepa , La notion de responsible du traitement – version large , 25 juin 2018 , Dalloz actualité , 25 juin 2018.

- Réglment caropéen (UE) 2018 / 608 de la commission du la avril établissant les critéres technique applicables aux etiquettes électronique pour les équipements marins (JOUE n° l Loi , 20 avril 2018).

- Tiphaine Bessiére , Le collecte de données personnelles : Un cadre précis ā respecter , Jurisport 2011 , n° 111 , p. 22.

- Virginie GAUTRON , Fichiers de police – Fichiers princip alement destines aux missions de police judiciaire , Avril 2015 , (actualisation : mars 2019) , N : 149.

ج– الأحكام القضائية:

- Cass . com , 28 mars 2018 , n°: 16- 20.018.

- C J U E , gr . ch , 5 juin 2018 , aff. C- 210/ 16.
- Cass. Civ , 18 octobre 2016 , n° 15-15042.
- Cass.civ , chamber civile 1 , 7 octobre 2015 , No: 14-20370. Publié au bulletin , 2016 , n°: 837 , 1re civ , n°: 335.
– Conseil d'Etat , 12 mars 2014 , n°: 354629 , Recueil Lebon , 2014
- C J U E , 13 mai 2014 , Google Spain , aff C-131/ 12 .
- Cass. Civ , chamber civile 1 , 19 november 2014 , No: 13-25156.
- Conceil d'Etat , 11 mars 2013 . n°: 332886.
- Conseil d'Etat , 30 décembre 2009 , n°: 306173 , Recueil Lebon: 535.
- Cass Crim , 14 mars 2006 , n° 05 – 83 . 423 . Dalloz , 2007 . Pan . 404 , obs . Garé.
- Cass . soc , 6 Avril 2004 , n°: 01 – 45 . 227 , Dalloz . 2004 , 2736.
- conseil d'Etat , 28 juillet 2004 , n°: 26-2851 , CNIL . 25 éme rapport d›activité 2004 , p. 78.
- C J U E , 6 november 2003 , Lindquist , aff : c- 101/ 01 , EU : C : 2003 , 596.
- Cass. Crim , 30 octobre 2001 , n°: 99-82136.
- Cour d'apple de paris , 31 mai 1995.
- Cour d'apple de paris , 31 mai 1995.

د- المواقع الإلكترونية:

- http:// www. Cnil . fr.
- https : // books . google . com . eg.
- https : // en. m.wikipedia.org/ Wikipedia/ Data – Fusion.
- www. Al-Hayat. Com
- www.dalloz.fr
- www.legifrance.gouv.fr/.