دراسة نقدية

لقانون حماية البيانات الشخصية

رقم (١٥١) لسنة ٢٠٢٠

تتضمن الدراسة توصيات ورشة العمل المنعقدة
بكلية القانون بالجامعة البريطانية في مصر
يوم الاثنين الموافق ١٢ أكتوبر ٢٠٢٠

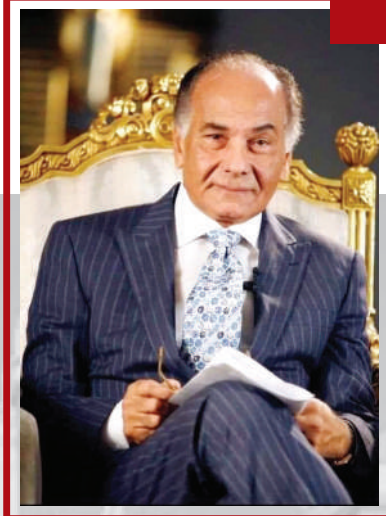
إعداد
مركز بحوث القانون والتكنولوجيا

إشراف
أ.د حسن عبد الحميد
عميد كلية القانون بالجامعة البريطانية
مُدير مركز بحوث القانون والتكنولوجيا

بالتعاون مع مكتب اندرسن للمحاماة

إهـداء إلى روح

الأستاذ/ محمد فريد خميس



فما مات من نبلت شمائله

فهو حي لدي التاريخ إمام

رجل الصناعة العظيم والأب الروحي للجامعة البريطانيـة واسـاس نشأتها.. من استلهمنا عبر مدرسـته فن القيـادة والإدارة.. ومن عشقـه لعمله معنى الاخلاص والإرادة.. ذلك الرمز الركين من رموز العطاء الوطني الشاهدة.

المحتويـــــات

فريق اعداد الدراسة «بمركز بحوث القانون والتكنولوجيا»

والمشاركون فى ورشة العمل

"دراسة نقدية لقانون حماية البيانات الشخصية"

تم النشر تحت رعاية:

الاستاذة/ فريدة خميس

رئيس مجلس أمناء الجامعة البريطانية في مصر

يوم الاثنين
الموافق ١٢ أكتوبر ٢٠٢٠
عبر تطبيق Zoom

الإشراف العام على الدراسة ورئاسة ورشة العمل:

أ.د. حسن عبد الحميد

عميد كلية القانون بالجامعة البريطانية
ومدير مركز بحوث القانون والتكنولوجيا.

المشاركون

في الورشة من الهيئات القضائية والجهات العلمية والخبراء:

محكمة النقض:

القاضي / محمد حسن عبد اللطيف

نائب رئيس محكمة النقض
رئيس إدارة العلاقات الدولية بالمحكمة

القاضي .د/ محمد عصام الترساوي

نائب رئيس محكمة النقض
عضو مركز معلومات المحكمة

القاضي / شريف الشيتاني

المحامي العام الأول بالنيابة العامة لدي محكمة النقض
عضو إدارة العلاقات الدولية بالمحكمة

القاضي / محمد عبد الله عمر

عضو المكتب الفني لمحكمة النقض
عضو إدارة العلاقات الدولية بالمحكمة

القاضي / محمد حسين مقرب

عضو المكتب الفني لمحكمة النقض
عضو مركز معلومات المحكمة

الجهات العلمية والخبراء:

القاضي/ على يونـس

المستشار الإقليمي بمكتب الأمم المتحدة المعنى بالمخدرات والجريمة

الدكتور/ محمد حجازي

رئيس لجنة التشريعات السابق بوزارة الاتصالات وتكنولوجيا المعلومات.

الأستاذ /أحمد الشرقاوي

الشريك بمكتب الشرقاوي وسرحان.

الأستاذ/ محمد عبد الجواد

الشريك بمكتب أديسيرو.

الدكتور/ محمد الديجوى

مدرس بقسم المالية العامة بكلية الحقوق جامعة القاهرة.

الدكتور أحمد عاطف أحمد

أستاذ الدراسات الدينية بجامعة كاليفورنيا سانتا باربرا.

الدكتور/ أحمد ضبش

مدرس الشريعة الإسلامية.

المستشار/ عبد المحسن شيحة

القاضي بمجلس الدولة

المستشار/ محمد الرفاعي

القاضي بمجلس الدولة.

المستشار/ محمد جميل

القاضي والمحاضر بالأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

المهندس/ وليد صابر

مسئول إنفاذ القانون السابق بشركة أوبر.

المهندس/ أسامة المصري

مسئول حماية البيانات فودافون مصر.

الأستاذة/ منة أبو ذكري

المحامية بمكتب الشرقاوي وسرحان.

فريق اعداد الدراسة وتنظيم وإدارة ورشة العمل بكلية القانون بالجامعة البريطانية:

الأستاذ الدكتور/ تامر الدمياطى

أستاذ القانون المدنى المساعد ونائب
مدير مركز بحوث القانون والتكنولوجيا

الدكتور/ محمد الجندى

خبير النيابة العامة للتحول الرقمي
ومستشار مدير مركز بحوث القانون
والتكنولوجيا

دكتور/ مروه زين

مدرس القانون الدولي الخاص
ومدير البرامج البحثية بالمركز.

دكتور/ كريم أبو العزم

مدرس القانون العام
ومسئول وحدة الامتحانات.

أ./ مها عمر

المدرس المساعد بالكلية.

أ./ عبد الرحمن جمال

المدرس المساعد بالكلية.

أ./ فرح صيام

المدرس المساعد بالكلية.

أ./ أحمد فؤاد

المدرس المساعد بالكلية.

فريق اعداد الدراسة وتنظيم وإدارة ورشة العمل بكلية القانون بالجامعة البريطانية:

أ. عبد الجابر أحمد

المدرس المساعد المنتدب بالكلية.

أ./ رانا سامى

المدرس المساعد بالكلية.

أ. محمد السيد

المسئول الإدراى
بمركز بحوث القانون والتكنولوجيا.

المشاركون بالحضور بكلية القانون

الأستاذ/ أحمد عبد الجواد

المدرس المساعد بكلية القانون.

الأستاذة/ مها عياد

المدرس المساعد بكلية القانون.

CLETs
Centre for Law & Emerging Technologies

تقديـــم

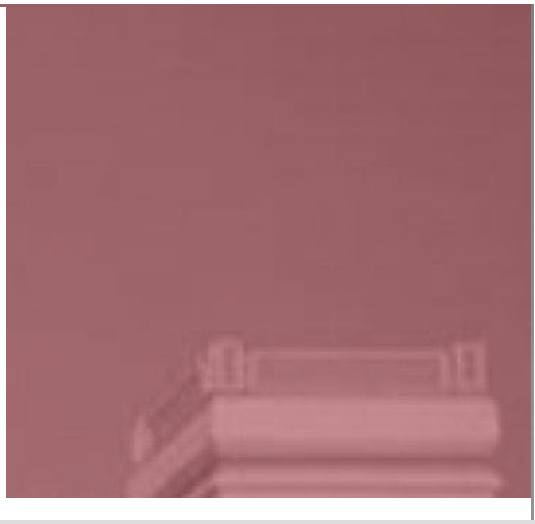
الأستاذ الدكتور/ حسن عبد الحميد

عميد كلية القانون بالجامعة البريطانية

يسعدني أن أقدم لرجال القانون، في مصر والعالم العربي، هذه الدراسة التي تمثل الإصدار العلمي الأول لمركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية في مصر. وهي دراسة قائمة علي مجهود بحثي قام به أعضاء المركز من أعضاء هيئة التدريس ومعاونيهم، وكذلك هي قائمة علي النقاش الجاد والمثمر الذي أنتجته ورشة العمل التي قام بتنظيمها المركز بتاريخ الإثنين الموافق ١٢ أكتوبر ٢٠٢٠، والتي شرفت بمشاركة كوكبة من رجال القانون في مصر، قضاة ومحامين، بالإضافة للمتخصصين في مجال تقنية المعلومات، وغيرهم ممن لهم علاقة مباشرة بقانون حماية البيانات الشخصية وما يثيره من إشكاليات جديدة بالنسبة للمجتمع المصري والعالم.

وقد نُظمت هذه الورشة في إطار ما نطلق عليه اسم "سلسلة الندوات العلمية للمركز"، والتي تحاول تقديم دراسات جادة لكل التشريعات واللوائح الصادرة في مجال القانون والتكنولوجيا، وذلك في إطار رؤية المركز التي تقوم علي أن الواقع الجديد الذي خلقته التكنولوجيا يحتاج إلى حلول قانونية مبتكرة توازن بين مصالح متعددة متنازعة ومعقدة في كثير من الأحيان. فالمشكلات التي تثيرها التكنولوجيا الناشئة، والمتجددة والمتطورة يوماً بعد يوم تحتاج لحلول قانونية غير تقليدية، فهي مشكلات غير تقليدية تحتاج لابتكار حلول جديدة دون التوقف فقط عند محاولة إنزال الحلول التقليدية على المعطيات الجديدة. هذا التطور يجبر رجال القانون على "العودة" للمنطق القانوني القائم على الافتراضات، والذي يطلق عليه بعض الفقهاء المسلمين "علم الهبهبة" (هب أن ـــ) والذي أدي لابتكار حلول لمشاكل مفترضة لم تحدث في الواقع. فعلي سبيل المثال: يثار حالياً النقاش - بمناسبة الذكاء الاصطناعي - حول مدي إمكانية الاعتراف بشخصية قانونية للإنسان الآلي (الروبوت)؟ وغيرها من المسائل الجديدة تماما بالنسبه لرجال القانون.





في الحقيقة، إن الحياة الرقمية يترتب عليها العديد من المشكلات المتعلقة بالوجود القانوني في هذه الحياة الافتراضية. ومن جهة أخري، فإذا كان القانون، فيما سبق، يحركه الاقتصاد والسياسة، فإن القانون في زمن الحياة الرقمية يحركه أيضاً الاقتصاد والسياسة. فليس خافياً على أحد أن اقتصاديات العالم الافتراضي قد وصلت لأرقام تجاوزت بكثير كل التوقعات. إن من بين أهم مصادر الثروة في الحياة الرقمية "تجارة المعلومات"، ويدخل في هذه التجارة، علي وجه الخصوص، التجارة المتعلقة بالبيانات الشخصية. ليس هذا فحسب، فالبيانات الشخصية تستعمل كذلك سياسياً وعسكرياً وأمنياً. وحينما أصبح إستغلال البيانات الشخصية " ظاهرة" بالمعني الحقيقي لمصطلح " ظاهرة" في علم الاجتماع القانوني، وارتبط بها العديد من الأنشطة الإنسانية، كان لزاماً على القانون التدخل لضبط هذه الظاهرة من خلال التشريع.

لذلك فإن حماية (أو بالأحرى) تنظيم استخدام البيانات الشخصية يرتبط بشكل وثيق بحماية الحق الدستوري في الخصوصية، ومن ثم فإن التشريعات التي تنظم استخدام البيانات الشخصية هي من القوانين المكملة للدستور: فهل يتفق قانون حماية البيانات الشخصية الجديد في مصر مع الدستور؟ وهل يحفظ فعلاً الحق في الخصوصية؟

صدر قانون حماية البيانات الشخصية في مصر بعد إصدار قانون مكافحة الجرائم الإلكترونية، وهناك العديد من القوانين الواجب إصدارها لتنظيم الحياة الرقمية، فهل توجد رؤية متكاملة لدى المشرع المصري في هذا الشأن؟ وهل يوجد تعارض بين القانونين؟ وهل يمكن ضمان عدم تعارض هذا القانون مع غيره من القوانين الواجب إصدارها في المستقبل؟ ألم يكن من الأفضل إصدار قانون واحد لتنظيم الاقتصاد الرقمي أو "الحياة الرقمية" يشتمل على كل هذه التفاصيل ويبنى على رؤية متكاملة لمصر في هذا المجال، ولا يقتصر على مجرد ردود أفعال لالتزامات دولية تفرض على مصر فتضطر لإصدار قانون اليوم وآخر غداً؟

إن قانون حماية البيانات الشخصية رقم ١٥١ الصادر في ١٥ يوليو ٢٠٢٠، يرتبط ارتباطًا وثيقًا بالدفاع عن الحق في الخصوصية، ويمكن اعتباره وسيلة من وسائل العودة لحماية الخصوصية بعد أن تعرضت لانتهاكات عديدة بفعل التقدم التكنولوجي والحرب ضد الإرهاب. لذلك فإن التأصيل الفلسفي لهذا القانون يرتبط، بصورة جوهرية، بمعرفة الحق في الخصوصية، باعتباره أحد أهم الحقوق التي نشأت في العصر الحديث، والذي لو فهمناه جيدا كان من السهل علينا أن نفهم قانون حماية البيانات الشخصية ونستطيع أيضاً أن ننقده نقداً إيجابياً يخدم المشرع في المستقبل.

فمن بين المباديء التي قامت عليها الحداثة القانونية والتي تمثل أساسا للقانون في العصر الحديث، التفرقة بين الشأن العام والشأن الخاص، والذي ترتب عليها التفرقة بين القانون العام والقانون الخاص، وأدت إلي ظهور مفهوم الحياة الخاصة بكل أبعادها المعروفة في نظرية القانون في العصر الحديث.

ويعتبر الحق في الخصوصية من بين الحقوق الأكثر إشكالية. ففي ظل غياب أي توافق حول أساس نظري واضح لمفهوم الخصوصية، لا يكاد يوجد رابط، معتمد، بين مختلف القضايا والموضوعات، التي يتم إدراجها تحت هذا الحق. فدعاوى الخصوصية تستخدم للدفاع عن حقوق تبدو متباعدة تمامًا، مثل الحق في عدم التعرض لمراقبة المكالمات الهاتفية، والحق في الإجهاض، والحق في معرفة ما تحتفظ به شركة الاتصالات من بيانات شخصية لعملائها. وبالتالي فإن غياب الأساس النظري الواضح للحق في الخصوصية يؤدي لتعرضه لمخاطر متعددة في عهد التوسع الهائل لاستخدام شبكة الإنترنت وتطور تطبيقاتها، وفي ظل تصاعد الحرب ضد الإرهاب حول العالم.

ومن جانب آخر، يعتبر الحق في الخصوصية حقًا نسبيًا، سواء من حيث الزمان أو المكان، وذلك لارتباطه بالثقافة السائدة في مجتمع بعينه وزمن بعينه. فأكثر من أي حق آخر، يعتمد الحق في الخصوصية على تصورات الناس عن حدود خصوصيتهم ومدى تقديرهم لقيمتها في حياتهم، وتختلف هذه التصورات، بقدر كبير، من مكان إلى مكان، كما تختلف بمرور الزمن، ونتيجة لتغير أنماط الحياة اليومية. فتصور ذلك الحق نسبي من حيث المكان في الزمان الواحد، ونسبي من حيث الزمان في المكان الواحد.

وفي ظل تسارع التغيرات الاجتماعية في العقود الأخيرة -وبدرجة أكبر في السنوات الأخيرة نتيجة الاستعمال الكبير والواسع لوسائل التواصل الرقمية في الحياة اليومية- تشهد تصورات الناس عن الخصوصية اضطرابًا كبيرًا. وذلك لأن هذه التصورات غير قادرة على التعامل مع مواقف جديدة يفرضها الواقع اليومي. خاصة أن هذه المواقف لا تخضع للأنماط التقليدية التي ما زالت أغلب التصورات السائدة للخصوصية تعتمد عليها.

في ظل هذه العوامل، تزداد الحاجة إلى بناء مفهوم نظري متماسك للحق في الخصوصية. وفي هذا الصدد احتدم الجدل حول مفهوم الخصوصية في النصف الثاني من القرن العشرين. ويمكن التمييز بين مدرستين من المدارس الفقهية التي تتناول مفهوم الحق في الخصوصية. المدرسة الأولى هي المدرسة الوصفية التي تحدد على سبيل الحصر ما ينبغي عمليًا حمايته بوصفه خاصًا. أما الثانية فهي المدرسة المعيارية التي تدافع عن الخصوصية كقيمة، وتحاول أن تضع للحق في الخصوصية تعريفًا يمكن أن يندرج تحته بعد ذلك كل الأمور المستجدة التي تمثل نوعا من الخصوصية.

ويجب الاعتراف بأن بناء مفهوم متماسك للحق في الخصوصية في العصر الحالي يمثل مشكلة حقيقية، نظرًا لعدم اهتمام رجال القانون بالتأصيل الفلسفي، الذي لا غني عنه لضبط المفاهيم. ففي حالة الاحتياج لمفاهيم مجردة لابد من الاستعانة بالتأصيل الفلسفي. ونحن اليوم في أشد الحاجة لخلق مفاهيم جديدة، خصوصًا ونحن نواجه واقعًا جديدًا يستحيل معه استخدام الآليات التقليدية للممارسة

القانونية، وبالتالي تفقد المفاهيم التقليدية للفكر القانوني جدواها.

وعلي الرغم من تناول الفلسفة الإغريقية لمسألة التفرقة بين الشأن العام والشأن الخاص، من خلال التمييز بين المدينة والمنزل، وربط الرجال بالأولى، والنساء والأطفال (والعبيد) بالثانية، إلا أن المفهوم الحقيقي للحق في الخصوصية يرتبط بالفلسفة الحديثة، وخصوصا فلسفات العقد الاجتماعي التي تمثل الأساس الفلسفي للغة القانون في العصر الحديث. فعلى سبيل المثال، ترى فلسفة جون لوك John Locke، أن معيار التمييز بين الشأن العام والشأن الخاص يكمن في ممارسة الحق في الملكية. فالنطاق الذي يحق للفرد أن يمارس فيه حرية كاملة للتصرف في مكوناته، بينما لا يكون لغيره مثل هذا الحق، هو الشأن الخاص للفرد، ويمتد هذا النطاق إلى كل ما يملكه الفرد. في حين أن جون ستيوارت ميل John Stuart Mill يرى أن هذا المعيار يكمن في مبدأ "رفع الأذى"، حيث يرى أنه لا يحق للسلطة التدخل في شئون الأفراد، إلا بغرض حماية الأخرين من الأذى. ومن ثم فإن المجال الخاص يتعلق بكل أفعال وممارسات الفرد التي لا يمكن إثبات أن ينشأ عنها أذى يلحق بغيره.

ولكن ظهور مفهوم محدد للحق في الخصوصية بناءً على هذه التفرقة بين الشأن العام والشأن الخاص ارتبط باستخدام الصور الفوتوغرافية في الصحافة في نهاية القرن التاسع عشر إضافة إلى تصاعد رواج الصحف بين الطبقات الوسطى والشعبية في الولايات المتحدة بصفة خاصة، مما أدى إلى خلق مناخ ملائم لإبراز الحاجة إلى تطوير مفهوم قانوني للحق في الخصوصية. وهذا العصر هو عصر نشأة ما سمي بالصحف الصفراء والتي اهتمت بنقل صور تفصيلية لأروقة حياة النخبة وما يدور فيها وحولها من شائعات وقصص وفضائح.

ونتيجة ازدياد عدد القضايا في هذا الخصوص، والتي نظرتها المحاكم الأمريكية، استطاع الفقهاء وضع تصور - ليس لمفهوم الحق في الخصوصية - ولكن لما قد يعتبر انتهاكا لهذا الحق، مثل: التطفل على خلوة أو عزلة الشخص، أو التدخل في شئونه الشخصية، أو الفضح العلني لحقائق خاصة محرجة عن الشخص، أو النشر العلني الذي يضع الشخص في صورة زائفة في أعين الرأي العام، أو الاستخدام دون إذن لإسم أو صورة شخص لتحقيق مصالح شخص أخر. ويهدف هذا الحق، بصفة عامة، إلى: الحماية من التطفل على منزل وشخص المواطن، وضمان الاستقلالية وهي حق الشخص في اتخاذ قرارات مصيرية شخصية دون تدخل من غيره، وحماية حق الفرد في منع نشر معلومات شخصية عنه.

وعلى الرغم من ذلك، ما زال مفهوم الحق في الخصوصية يحتاج إلى دراسات عميقة تستطيع الوقوف على كل التطورات التي تلحق به يومًا بعد يوم في ظل التسارع التكنولوجي الذي نعيش فيه والذي يخلق كل يوم أدوات جديدة تساهم فيما يمكن اعتباره حقًا في الخصوصية. فهل يُقصد بالخصوصية التحكم في المعلومات الشخصية حصرًا؟ هل الخصوصية هي أحد وجوه الكرامة الإنسانية؟ أم أنها تتعلق بفكرة الحميمية؟

وبصفة عامة، يمكن القول بأن المعلومات الشخصية هي "الحقائق" التي يفضل أغلب الناس إبقائها سرًا ولا يرغبون في نشرها، والمتعلقة مثلا بحالتهم الصحية، أو دخلهم، أو وزنهم، أو توجههم الجنسي.

عمومًا يعتبر قانون حماية البيانات الشخصية (وإن كنت أفضل تسميته قانون تنظيم استخدام البيانات الشخصية) من القوانين الهامة التي تسعى لاستعادة الحق في الخصوصية بعد تعرضه لسلسلة من الانتهاكات في الأحقاب الأخيرة.

والدراسة التي بين يدي القارئ تنقسم إلى أربعة محاور، يسبقهم محور تمهيدي يُلقي نظرة عامة على قانون حماية البيانات الشخصية، ويتعرض المحور الأول للإطار المفاهيمي لقانون حماية البيانات الشخصية، مبيناً المصطلحات الأساسية التي يقوم بُنيان القانون عليها، ويشير المحور الثاني إلى حقوق الشخص المعني بالبيانات وشروط المعالجة، بينما يبين المحور الثالث التزامات أطراف معالجة وحماية البيانات (المتحكم والمعالج)، وأخيراً نختتم الدراسة بالمحور الرابع المعني بوسائل إنفاذ قانون حماية البيانات الشخصية. كذلك وجدنا أنه من المفيد لأغراض هذه الدراسة، إضافة بعض الملاحق الهامة لخدمة الباحثين فى هذا المجال، على النحو الوارد فى محتويات الدراسة.

ولا يسعني في النهاية إلا أن أتوجه بالشكر الخالص لفريق العمل بمركز بحوث القانون والتكنولوجيا، لما بذلوه من جهد صادق لتنظيم وإخراج هذا العمل، كما أتوجه بخالص الشكر وعظيم التقدير للأستاذ/ ماهر ميلاد إسكندر الشريك الإداري لشركة أندرسن العالمية للمحاماة، على دعمه الكريم في طباعة هذا العمل، الذي يعد الأول من نوعه، والذي سوف يتبعه بمشيئة الله أعمال أخرى تثري المكتبة العربية في هذا المجال.

القاهرة - مدينة الشروق

٢٠٢١/٢/٢٥

المقدمة

■ مدخل تعريفى بموضوع الدراسة:

يُعد الحق فى الخصوصية The right to privacy **(أو الحق فى حرمة الحياة الخاصة) من أكثر الحقوق ارتباطاً بالشخصية القانونية للإنسان[١] وأشدها تعلقاً بالكرامة، وهو مؤشر على تحضر الأمم ورقيها، وذلك لجمعه بين الجوانب المادية والمعنوية لشخصية الإنسان وعلاقته الوثيقة وتداخله الشديد بالحقوق والحريات الأخرى، إضافة إلى خضوعه لقواعد الدين والأخلاق والأعراف السائدة فى المجتمع، وتأثره بطبيعة النظام السياسى الذى يحكم الدولة والتطورات التكنولوجية التى فرضها التقدم العلمى.**

وتتعدد مظاهر هذا الحق[٢] وتتنوع سبل حمايته، وتحرص المجتمعات على احترامه، فاعتبرته حقاً مستقلاً قائماً بذاته، ولم تكتف بسن القوانين لحمايته بل سعت إلى ترسيخه في الأذهان، وما زال يحظى باهتمام كبير من جانب الهيئات والمنظمات الدولية والدساتير والنظم القانونية[٣].

وتقتضى خصوصية البيانات تنظيم عملية جمع البيانات والمعلومات الشخصية ومعالجتها واستخدامها ونقلها، على نحو يكفل سريتها خصوصاً فى ظل المخاطر المتزايدة للكشف عنها وإساءة استخدامها بفعل الحاسب الآلى وشبكة الانترنت[٤] والتطور المتعاظم للبلوك تشين وأنظمة الذكاء الاصطناعى.

ويعتبر الحق فى حماية البيانات الشخصية وصونها وعدم إفشائها للغير، من أهم وأعظم صور الحق فى الخصوصية[٥] أو حرمة الحياة الخاصة، فالحفاظ على أسرار الإنسان هو جوهر وأساس ضمانة حرية الخصوصية ضد انتهاك الغير، وهنا يظهر دور القواعد القانونية التى تؤطر وتحكم وتنظم مسائل هذه الحماية، من خلال ما تسنه من تشريعات تكفل ضمان عدم المساس بها أو إفشائها.

---

١ – يقصد بالخصوصية لغةً: حالة الخصوص، والخصوص نقيض العموم، ويقال خصه بالشيء يخُصّه خَصّاً وخُصوصاً وخَصُوصِيّةً، وأخصته: أي أفرده دون غيره. ويقال: اختصّ فلانٌ بالأمر وتخصّصَ له إذا انفرد. ابن منظور: لسان العرب، الجزء الرابع، بيروت – لبنان، دار إحياء التراث العربي، ١٩٩٩، ص ١٠٩.

٢ – يرى البعض أن أبعاد الحق في الخصوصية تتمثل فى أربع فئات وهى: خصوصية الشخص، خصوصية سلوكه، خصوصية بياناته، خصوصية اتصالاته. انظر:

Shraddha Kulhari: Building-Blocks of a Data Protection Revolution, The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, Chapter III: Data Protection, Privacy and Identity: A Complex Triad, Germany, Nomos - Munich Intellectual Property Law Center (MIPLC), 2018, p. 23.

٣ – لمزيد من التفصيل فى شأن حماية الحق فى الخصوصية، انظر:

د. حسام الدين الأهواني، الحق في احترام الحياة الخاصة، القاهرة، دار النهضة العربية، ١٩٧٨م، ص ٨؛ د. أحمد فتحي سرور، الحماية الدستورية للحقوق والحريات، القاهرة، دار الشروق، ٢٠٠٠م، ص ٣٣ وما بعدها؛ د. محمد عبد المحسن المقاطع: حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، الكويت: دار السلاسل، ١٩٩٢م، ص ٩٦؛ د. محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية (الحق في الخصوصية المعلوماتية)، مجلة كلية القانون الكويتية العالمية، العدد التاسع، السنة الثالثة، مارس ٢٠١٥، ص ١٠٥.

Alan F. Westin, Privacy And Freedom, Washington and Lee Law Review, Volume 25, Issue 1, 1968, p. 166

٤ – د. محمود عبد الرحمن: التطورات الحديثة لمفهوم الحق فى الخصوصية، مرجع سابق، ص ١٠٦.

Gary T. Marx, Murky Conceptual Waters: The Public and the Private, Ethics and Information Technology, Volume 3, 2001, pp. 157-159.

٥ – د. شريف يوسف خاطر: حق الاطلاع على البيانات الشخصية في فرنسا، مجلة كلية القانون الكويتية العالمية، السنة الثالثة، العدد التاسع، مارس ٢٠١٥م، ص ٢٨١، ص ٢٨٢–٢٨٣.

وقد أولت التشريعات الدولية المختلفة اهتماماً متعاظماً لحماية حق الأفراد في الخصوصية نظراً لاعتماد أنماط الحياة المعاصرة باطراد على البنى التكنولوجية في مختلف أوجه الإدارة والإتصال، ما نتج عنه تعاظماً في كمية البيانات التي تحوذها الدولة والمؤسسات الخاصة، ما استدعى أن ينظر المشرع بوجه العناية إلى الكيفية التي يتم بها جمع، وحفظ، ومعالجة البيانات التي يمكن أن تحتوي على معلومات خاصة بالأفراد؛ وما قد ينتج عن إساءة استخدامها من انتهاك لخصوصيتهم، وذلك في حاجة ملحة تضمن خصوصية المواطنين؛ بحيث يجرم جمع البيانات الشخصية بطرق غير مشروعة، ومعالجتها بطرق تدليسية، ونقلها عبر الحدود الجغرافية، ويجرم إفشاءها؛ ما قد يعرض المواطنين لانتهاك حرمة حياتهم الخاصة وحقهم في الخصوصية[٦].

■ التنظيم التشريعى الأوروبي لحماية البيانات الشخصية:

يرجع الفضل فى حماية الخصوصية على الصعيد الدولى لجهود المنظمات الدولية والإقليمية، والتي كان لها الأثر البيّن في صياغة النظام القانوني لخصوصية البيانات الشخصية[٧]، غير أن القانون الأوروبي احتل الريادة في هذا الصدد وذلك من خلال اللائحة العامة لحماية البيانات General Data Protection Regulation (GDPR)[٨] بالاتحاد الأوروبي، والتي تمثل قانونًا نموذجيًا للعديد من التشريعات الوطنية داخل الاتحاد الأوروبي وخارجه[٩].

---

٦ – في يونيو عام ٢٠١٣ فجر إدوارد سنودن Edward Snowden، وهو متعاقد تقنى سابق مع وكالة الأمن القومي الأمريكى، فضيحة التنصت العالمى واختراق الخصوصية، حيث قام بتسريب وثائق سرية للغاية لوكالة الأمن القومي الأمريكي وشركائها الدوليين، ونشرتها جريدة الجارديان وجريدة الواشنطن بوست وغيرها من الصحف العالمية، والتى كشفت عن تدخلهم بصورة واسعة النطاق فى التنصت من خلال الانترنت، ومراقبة الهواتف على نطاق عالمي عبر برنامج التجسس بريسمPRISM . وقد أثارت هذه التسريبات النقاش بشأن القيود المفروضة على المراقبة الشاملة وعما إذا كانت قوانين الخصوصية تواكب التقدم التكنولوجي، وخاصة وأن القواعد الدولية لحقوق الإنسان والتي تحمي الحق في الخصوصية قد صيغت قبل ظهور الانترنت.

٧ – ونجد أهم جهود المنظمات الدولية والاقليمية فى مجال حماية لخصوصية البيانات الشخصية، واضحة فيما يلى:-

أ– الإعلان العالمى لحقوق الإنسان الصادر عام ١٩٤٨: حيث يرسخ الحق فى الخصوصية، بشكل واضح فى المادة ١٢ منه التى تنص على أن: "لا يجوز تعريض أي شخص للتدخل التعسفي في خصوصياته أو في شئونه الأسرية أو المنزلية أو في مراسلاته، ولا حتى إثارة حملات تستهدف شرفه وسمعته. ويمتلك كل إنسان الحق في الحصول على حماية القانون ضد مثل هذا التدخل أو تلك الهجمات.

ب – قرار الجمعية العامة للأمم المتحدة بشأن الحق فى الخصوصية فى العصر الرقمى عام ٢٠١٣: حيث اعتمدت الجمعية العامة في ٢٠ ديسمبر ٢٠١٣، بالإجماع، وبدون تصويت، القرار رقم (١٦٧/٦٨) بشأن الحق في الخصوصية في العصر الرقمي، ليدعم بقوة "احترام وحماية الحق في الخصوصية"، داعيا جميع الدول إلى اتخاذ التدابير اللازمة لوضع حد للأنشطة التي تنتهك هذا "المبدأ الأساسي للمجتمع الديمقراطي، ومعربة عن قلقها إزاء التأثير السلبي للمراقبة الإلكترونية واعتراض الاتصالات الرقمية وجمع البيانات الشخصية، على حقوق الإنسان.

ج – المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD) عام ١٩٨٠: وهى مجموعة قواعد لحماية الخصوصية ولضمان نقل البيانات ذات الطبيعة الشخصية عبر الحدود، وتبني مجلس المنظمة هذه القواعد وصدقت عليها العديد من الدول، وتعد تلك المبادئ إرشادية غير ملزمة بحيث لا يتم توقيع جزاءات علي الدول الأعضاء حال مخالفتها، ولكن لا يمكن أغفال أهمية ما أفرزته هذه المبادئ من قواعد تشريعية وإدارية تتعلق بالحصول علي البيانات عبر وسائل عادلة ومشروعة، واستخدامها في الاغراض المحددة سلفاً والتي تم على أساسها جمع البيانات وذلك بعد موافقة أصاحبها، هذا بالاضافة إلي مبدأ الوقاية الأمنية للبيانات الشخصية خلال مراحل الجمع والتخزين والنقل والمعالجة، ومبدأ مشاركة الأفراد بحيث يحق للمواطنين الاطلاع علي البيانات الخاصة بهم وأحقيتهم في تعديلها ومحوها.

د – توجيهات الاتحاد الأوروبي بشأن معالجة البيانات الشخصية: فقد سعي الاتحاد الأوروبي لتوحيد قواعد حماية الخصوصية اعتباراً من عام ١٩٧٦، حيث أصدر التعليمات رقم ٧٦/٤/٨ المتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات The protection of the individual against the technical evolution of informatics، والتعليمات ٧٩/٥/٨ المتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات The protection of the rights of the individual in the face of technical developments in data processing . كما ينص التوجيه الاوروبي رقم ٤٦/٩٥ في مادته السادسة علي المبادئ الأساسية لحماية البيانات حيث يقرر ضرورة مراعاة التعامل مع البيانات الشخصية وشروطها.

هـ – اتفاقية مجلس أوروبا: Council of Europe: وتعنى بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، وتعد تلك الاتفاقية ملزمة للدول الأطراف، وتتضمن عدة مبادئ تمثل الحدود الدنيا للقواعد التي يجب أن يتضمنها تشريع الدول الموقعة علي الإتفاقية، وتتشابه هذه المبادئ مع تلك التي تقررها المبادئ التوجيهية لمنظمة التعاون الأقتصادي والتنمية (OECD) .

٨ – هي مجموعة من القواعد المتعلقة بحماية البيانات تم وضعها من قبل الإتحاد الأوروبي تمت الموافقة عليها في ١٤ أبريل ٢٠١٦ من قِبل المفوضية الأوروبية، بغرض حماية حقوق جميع مواطني الدول الأعضاء فى الاتحاد الأوروبي وبياناتهم الشخصية، وقد جاءت هذه اللائحة لتحل محل التوجيه الأوروبى رقم 95/46/EC الصادر عن البرلمان الأوروبي بتاريخ ٢٤ أكتوبر ١٩٩٥ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية تداول البيانات، وقد دخلت حيز النفاذ في كافة الدول الأوروبية فى ٢٥ مايو ٢٠١٨. متاحة على الموقع التالى:

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

٩ – تجدر الإشارة إلى الأحكام المعنية بحماية البيانات الشخصية والسابقة على صدور هذه اللائحة كانت تصدر من الاتحاد الأوروبى فى صورة توجيهات (Directives)، بينما نلاحظ أن الأحكام الحديثة لتنظيم حماية البيانات الشخصية قد صدرت فى صورة لائحة (Regulation) ذات صفة إلزامية قانونية أكبر من التوجيهات على الدول الأعضاء كما أن لها تطبيق مباشر داخل الدول. وربما يستدل بذلك على رغبة الاتحاد الأوروبى فى توحيد حماية البيانات الشخصية والوقوف على أحكام موحدة بالنسبة لحماية البيانات الشخصية داخل الدول الأعضاء.

■ حماية خصوصية البيانات فى النظام القانونى المصري:

حظى الحق فى الخصوصية أو حرمة الحياة الخاصة بعناية خاصة في الدستور المصري الصادر عام ٢٠١٤،[١٠] فاعتبره حقاً من الحقوق الدستورية المطلقة، حيث نصت المادة ٥٧ منه على أن: "للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك".

ولم يقف عند هذا الحد، بل وفر الحماية ضد الاعتداد علي هذا الحق أو المساس به، فقررت المادة ٩٩ من الدستور أن: "كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر".

وفى سبيل التأكيد على أهمية حماية الحق فى الخصوصية، وهو ما ينصرف بالطبع للبيانات الشخصية، ذهبت **المحكمة الدستورية العليا** المصرية – فى حكمها الصادر بجلسة ١٥ نوفمبر ١٩٩٦[١١] – إلي أن هناك " ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي دوماً ألا يقتحمها أحد ضماناً لسريتها وصوناً لحرمتها، فلا يكون اختلاس بعض جوانبها مقبولاً. وهذه المناطق من خواص الحياة ودخائلها تصون مصلحتين تتكاملان فيما بينهما وإن بديتا منفصلتين، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها وحجبها عن الآخرين، وكذلك بما ينبغي أن يستقل به كل فرد من سلطة التقرير فيما يؤثر في مصيره. وتبلور هذه المناطق جميعها التي يلوذ الفرد بها، مطمئناً لحرمتها، وامتناع إخضاعها لأشكال الرقابة وأدواتها على اختلافها، الحق في أن تكون للحياة الخاصة تخومها، باعتبار أن صونها من العدوان أوثق اتصالاً بالقيم التي تدعو إليها الأمم المتحضرة، وأكفل للحرية الشخصية التي يجب أن يكون نهجها متواصلاً ليوائم مضمونها الآفاق الجديدة التي ترنو الجماعة إليها".

كذلك نجد صدى لحماية البيانات الشخصية في بعض القوانين المصرية ولكنها مجرد نصوص متفرقة تشير لسرية البيانات الشخصية وتجرم إفشاء البيانات، وتشدد العقوبة على مرتكبها لما لها من خطورة على المجتمع.

ففى قانون العقوبات، أفرد المشرع عقوبة خاصة لكل من يعتدى على حرمة الحياة الخاصة للمواطن وهى عقوبة الحبس لمدة لا تزيد على سنة (م ٣٠٩ مكرر عقوبات)[١٢]، كما يعاقب كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بطرق غير مشروعة أو كان بغير رضاء صاحب الشأن، كما يعاقب كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها لحمل شخص على القيام بعمل أو الامتناع عنه بالسجن مدة لا تزيد على خمس سنوات (م ٣٠٩ مكرر أ عقوبات).

كما شدد المشرع العقوبة على من يفشي سر خصوصي أؤتمن عليه بحكم وظيفته كالأطباء والجراحين أو الصيادلة والقوابل يعاقب بالحبس مدة لا تزيد علي ستة أشهر أو بغرامة (م ٣١٠ عقوبات).

وفى قانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤، تشير المادة ١٣ منه إلى أن" "تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتي تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين الملحقة سرية، ولا يجوز الاطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون ووفقا لأحكامه.

وتعتبر البيانات أو المعلومات أو الإحصائيات المجمعة التي تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين سرًا قوميًا، ولا يجوز الاطلاع عليها أو نشرها إلا لمصلحة قومية أو علمية وبإذن كتابي من مدير قطاع الأحوال المدنية أو من ينيبه وفقا للأوضاع والشروط التي يحددها القانون واللائحة التنفيذية"[١٣].

---

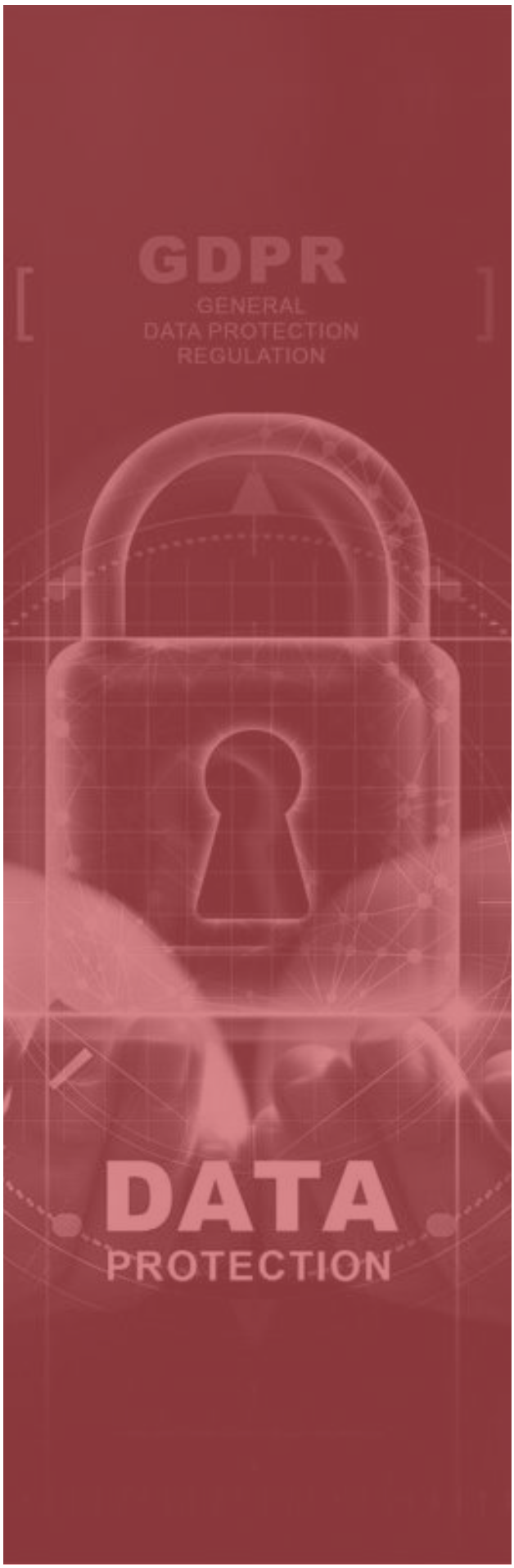
١٠ – الجريدة الرسمية، العدد (٣) مكرر (أ)، ١٨ يناير سنة ٢٠١٤م.

١١ – راجع: حكم المحكمة الدستورية العليا، القضية رقم ٥٦ لسنة ١٨ قضائية دستورية، جلسة ١٥ نوفمبر ١٩٩٦، أحكام المحكمة الدستورية العليا – الجزء الثامن من أول يوليو ١٩٩٦ حتى آخر يونيو ١٩٩٨ – ص ٩٢٨.

١٢ – نصت المادة ٣٠٩ مكرر من قانون العقوبات على أن: " يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه: (أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون. (ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً. ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويُحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما تحكم بمحو التسجيلات المتحصلة عنها أو إعدامها".

١٣ – وتضيف الفقرة الثانية من المادة ١٤٠ من هذا القانون أن: "ومع عدم الإخلال بالاستعلامات الواردة بهذا القانون ، يسرى الحظر المنصوص عليه في الفقرة الأولى من هذه المادة على جميع الأشخاص والجهات بما في ذلك الجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون، ويظل هذا الحظر قائماً حتى ولو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب" .



كما حرص **قانون البنك المركزى والجهاز المصرفى** الصادر عام ٢٠٢٠ على سرية بيانات وحسابات العملاء، حيث تنص المادة ١٤٠ منه على أن: "تكون جميع بيانات العملاء وحساباتهم وودائعهم وأماناتهم وخزائنهم في البنوك وكذلك المعاملات المتعلقة بها سرية، ولا يجوز الاطلاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر إلا بإذن كتابي من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصى لهم بكل هذه الأموال أو بعضها، أو من نائبه القانوني أو وكيله أو بناء على حكم قضائي أو حكم تحكيم[١٤].

وفى السياق نفسه، حرص **قانون الطفل** رقم ١٢ لسنة ١٩٩٦ المعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨، على حماية بيانات الطفل؛ حيث نصت المادة ١١٦ مكررًا (ب) من هذا القانون على أن: "مع عدم الإخلال بأى عقوبة أشد ينص عليها فى قانون آخر، يعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه كل من نشر أو أذاع بأحد أجهزة الإعلام أى معلومات أو بيانات، أو أى رسوم أو صور تتعلق بهوية الطفل حال عرض أمره على الجهات المعنية بالأطفال المعرضين للخطر أو المخالفين للقانون.»

كما اعتبر **قانون التوقيع الإلكترونى** رقم ١٥ لسنة ٢٠٠٤، بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التى تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكترونى "سرية"، وجرم إفشاء هذه البيانات واستخدامها فى غير الغرض الذى قدمت من أجله (م ٢١ من القانون)، وقرر توقيع عقوبة الحبس والغرامة التى لا تقل عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين لمن يخالف ذلك، وينشر حكم الإدانة فى جريدتين يوميتين واسعتي الانتشار وعلى شبكات المعلومات الإلكترونية المفتوحة علي نفقة المحكوم عليه (م ٢٣ من القانون).

ورغم هذا تبقى تلك النصوص القانونية متفرقة وجزئية، فتعالج بعض أوجه الخصوصية في مجالات محددة، ولا تشكل بأى حال نظام متكامل يتضمن أطراً عامة لحماية البيانات الشخصية، مما كان يستدعى إصدار قانون خاص ينظم طرق جمع البيانات بوسائل مشروعة، ويحدد كيفية معالجتها والحفاظ عليها، ويقرر مدد حفظها والغرض المحدد لها، وكذلك كيفية استخدام البيانات ومعالجتها وبيان حقوق صاحب البيانات، وتحديد العقوبات على مخالفة أحكامه وغيرها من الأحكام ذات الصلة.

١٤ – وفقًا للمادة ٧٦ من قانون الأحوال المدنية يُعاقب بالسجن المشدد كل من اخترق أو حاول اختراق سرية البيانات أو المعلومات أو الإحصاءات المجمعة بأية صورة من الصور. وتكون العقوبة السجن المؤبد إذا وقعت الجريمة في زمن الحرب.

■ إصدار قانون حماية البيانات الشخصية المصري – خطوة طال انتظارها:

أدرك المشرع المصري أن تنظيم وحماية البيانات الشخصية بات أمراً ملحاً وحيوياً وليس من قبيل الرفاهية القانونية، وعكف لمدة سنتين على إعداد قانون يعالج هذه المسألة حتى صدر قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ – الذى طال انتظاره – في ١٥ يوليو ٢٠٢٠ (الجريدة الرسمية – العدد ٢٨ مكرر (هـ) فى ٢٥ يولية ٢٠٢٠)[١٥]. وجاء القانون في ٤٩ مادة وبين أسطره العديد من التساؤلات والنقاط الجدلية.

وفي هذا الإطار نظم مركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية فى مصر ورشة عمل، فى الثانى عشر من أكتوبر ٢٠٢٠، بحضور لفيف من الخبراء والمتخصصين ورجال القانون والقضاء، لدراسة القانون الصادر مؤخراً بُغية اقتراح تصور فعال للائحة التنفيذية للقانون، وتلمس النقاط التى تحتاج إلى تعديل تشريعى لنصوص القانون.

> بات إصدار قانون خاص بحماية البيانات الشخصية ضرورة مُلحة وليس رفاهية تشريعية.

> تنظيم كلية القانون لورشة عمل حول قانون حماية البيانات الشخصية.

ولا جرم فى أن تحقيق هذا الغرض استتبع التعرض بالنقاش للظروف التي دفعت الجهات التشريعية لإصدار هذا القانون وكذلك فلسفته، وأيضًا نطاق القانون الجديد، وحقوق الشخص المعنى بالبيانات، وشروط معالجة البيانات، والالتزامات الواقعة على عاتق المتحكم ومعالج البيانات، إضافة إلى دور مركز حماية البيانات المزمع إطلاقه في ظل هذا القانون، ومتطلبات امتثال المؤسسات للقانون والعقوبات المترتبة على مخالفته، ونتناول هذه المسائل فى إطار مقارن مع اللائحة الأوروبية لحماية البيانات – قدر الإمكان – باعتبارها القواعد التى استهدى بها المشرع فى إعداد هذا القانون[١٦].

١٥ – حرصت الكثير من الدول على سن تشريعات ترمى إلى حماية البيانات الشخصية، وتعد فرنسا من أوائل الدول التى عنيت بالاهتمام بها وحمايتها، حيث أصدرت القانون رقم ١٧ لسنة ١٩٧٨ فى ٦ يناير ١٩٧٨ المتعلق بالمعلوماتية والملفات والحريات والذى تم تعديله حديثاً بموجب القانون رقم ٤٩٣ لسنة ٢٠١٨ الصادر فى ٢٠ يونيو ٢٠١٨ بشأن حماية البيانات الشخصية.

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF n°0141 du 21 juin 2018.

كما أصدرت دولة تونس القانون رقم ٦٣ لسنة ٢٠٠٤ الخاص بحماية المعطيات الشخصية، وأصدرت دولة المغرب قانون "حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي" في ٢٠٠٩.

١٦ – من المهم دراسة المناهج المختلفة للتشريعات التي تنظم البيانات الشخصية وما تنظمه من حقوق واشتراطات والتزامات تقع على عاتق الأطراف الرئيسية فى مجال حماية البيانات الشخصية، باختلاف مسمياتهم وتعريفاتهم، لبيان مدى ملائمتها مع المناخ العملي والمجتمعي فى الدولة.

■ خطة الدراسة:

ومن هذا المنطلق تم تقسيم محاور الدراسة النقدية لقانون حماية البيانات الشخصية المصري الجديد - محل ورشة العمل - على أربعة محاور، يسبقهم محور تمهيدى، وذلك على النحو التالى: -

المحور التمهيدى:

نظرة عامة على قانون حماية البيانات الشخصية

المحور الأول:

الإطار المفاهيمي لقانون حماية البيانات الشخصية

المحور الثانى:

حقوق الشخص المعنى بالبيانات وشروط المعالجة.

المحور الثالث:

التزامات أطراف معالجة وحماية البيانات

المحور الرابع:

وسائل إنفاذ قانون حماية البيانات الشخصية

■ ملاحق الدراسة:

١ - التعديلات المقترحة لمواد قانون حماية البيانات الشخصية والمقارنة مع اللائحة الأوروبية GDPR.

٢ - التشريعيات المصرية المنظمة لحماية البيانات الشخصية.

٣ - المواد التى أحال فيها قانون حماية البيانات إلى لائحته التنفيذية، مع المعايير التقنية المقترحة.

٤ - نماذج قوانين حماية البيانات الشخصية فى العالم.

٥ - نماذج من أهم قضايا حماية البيانات الشخصية فى العالم.

المحور التمهيدى

نظرة عامة على إصدار قانون حماية البيانات الشخصية
(خطوة تشريعية طال انتظارها)

■ تمهيد:

لقد أدت تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع بزوغ تكنولوجيا إنترنت الأشياء، والحوسبة السحابية، والذكاء الاصطناعي وغيرها، إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبوق، مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد[١٧].

> **أهمية إصدار قانون خاص بحماية البيانات الشخصية فى تحقيق التنمية الاقتصادية .**

ونظراً لاهتمام الدولة فى الوقت الحاضر بتشجيع الاستثمارات في مجال صناعة مراكز البيانات العملاقة، هادفةً لأن تصبح مصر ممرًا رقميًا عالميًا، ولما كان ذلك يتطلب وجود بيئة تشريعية مناسبة، فقد حرصت الحكومة وأعضاء مجلس النواب على إعداد وصياغة مشروع قانون حماية البيانات الشخصية بما يضمن خصوصية المواطنين والعمل علي تهيئة المناخ الاستثماري في مصر، وحتى يكون متسقاً مع اللائحة العامة لحماية البيانات GDPR الصادرة عن الاتحاد الأوروبي[١٨]، باعتبارها التغيير الأكثر أهمية في تنظيم خصوصية البيانات على المستوى العالمي خلال العشرين عاماً الماضية، ولتأثر الكيانات غير الأوروبية التى تستخدم خدمات الانترنت بأحكامها[١٩].

١٧ – راجع: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يولية ٢٠١٩، ص ٨ وما بعدها، متاح على الموقع التالى:
https://www.elwatannews.com/data/iframe/pdf/25021748.pdf

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

١٩ – فعلى سبيل المثال أعلنت شركة ميكروسوفت العملاقة عبر موقعها عن التزامها تجاه الامتثال للقانون العام لحماية البيانات (GDPR)، راجع الموقع التالى:
https://www.microsoft.com/ar-ww/trust-center/privacy/gdpr-overview

أولاً

مراحل سن وإصدار قانون حماية البيانات الشخصية

(أحد القوانين المكملة للدستور)[٢٠]:

مر إصدار قانون حماية البيانات الشخصية بمراحل عديدة، وبُذلت فى إعداده جهود مضنية، حتى خرج للنور بهذه الصورة النهائية، نبتة جديدة فى مضمار الصرح التشريعى المصري العريق، ويُمكن تلمس أبرز المحطات فى طريق إعداد القانون كالتالي:-

- بتاريخ الاثنين الموافق ٦ نوفمبر ٢٠١٧ أحال مجلس النواب إلى لجنة مشتركة من لجان الاتصالات وتكنولوجيا المعلومات والدفاع والأمن القومي والشئون الدستورية والتشريعية مشروع القانون المقدم من السيد النائب أشرف عمارة و(٦٠) نائباً آخرين (أكثر من عُشر عدد أعضاء المجلس) في ذات الموضوع وذلك لبحثه وإعداد تقرير عنه يُعرض على المجلس. وقد عقدت اللجنة اجتماعاً بتاريخ ٢٠ نوفمبر ٢٠١٧ وافقت عليه من حيث المبدأ واستمرت اللجنة في نظره في عدة اجتماعات أخري دون الانتهاء منه.

- تقدمت الحكومة بمشروع قانون بشأن "إصدار قانون حماية البيانات الشخصية "الذى أعدته وزارة الاتصالات وتكنولوجيا المعلومات"، وأحاله مجلس النواب بجلسته المعقودة يوم الأحد الموافق ١٠ مارس ٢٠١٩، إلى لجنة مشتركة من لجنة الاتصالات وتكنولوجيا المعلومات، ومكاتب لجان الشئون الدستورية والتشريعية، والخطة والموازنة، والدفاع والأمن القومي.

- بعد أن أطلعت اللجنة المشتركة على مشروعي القانونين ومذكرتيهما الإيضاحية، تبين لها أن مشروع القانون المقدم من الحكومة ومشروع القانون المُقدم من النواب متفقان من حيث المبدأ ولهذا رأت اللجنة اعتبار مشروع القانون المُقدم من الحكومة أساساً لدراستها وذلك إعمالاً لحكم المادة (١٨٦) من اللائحة الداخلية للمجلس.

- عقدت اللجنة المشتركة - اجتماعات عديدة - لنظر مشروع القانون المقدم من الحكومة، شارك فيها وزير الاتصالات وتكنولوجيا المعلومات وممثلى الوزارات المعنية (الاتصالات - الدفاع - الداخلية - الخارجية - العدل - الهجرة..)، وممثلى جهات الدولة ذات الصلة، وأجرت جلسات حوار مجتمعى حوله حضرها العديد من ممثلى الشركات العالمية والمحلية العاملة في مجال الاتصالات وتكنولوجيا المعلومات ومؤسسات المجتمع المدني والمؤسسات المصرفية والمالية.

- وقد استبان من ورشة العمل، قيام عدد من أساتذة القانون بالمشاركة في المراحل التمهيدية لصياغة ومناقشة مشروع القانون. ولكن كان غيابهم واضحاً عن مائدة مناقشات المراجعة النهائية لمشروع القانون فى اللجنة المشتركة (إلا من أستاذة واحدة فقط شاركت فى المناقشات)، واقتصرت المشاركة فى هذه المرحلة على المتخصصين فى مجال تكنولوجيا المعلومات والاتصالات والشركات العاملة فى هذا المجال، وهو ما ألقى بظلاله على بعض الصياغات فى القانون، **حيث أدت المناقشات والتعديلات التي اقترحتها الهيئات المختلفة إلى عدم تناسق الصياغة في عدد من المواضع**، فضلاً عن الحاجة لتكامله مع غيره من النصوص فى المنظومة التشريعية المصرية.

- وقد عُرض مشروع القانون على قسم التشريع بمجلس الدولة، وقد كان للقسم ما ارتآه من ملاحظات شكلية وموضوعية على مواد مشروع القانون بما تستقيم معها أحكامه على الأسس القانونية السليمة، وهو ما أخذته اللجنة بعين الاعتبار بتلافيها لكافة الملاحظات الواردة من مجلس الدولة.

- بتاريخ ١٦ يونيو ٢٠١٩ وافقت لجنة الاتصالات وتكنولوجيا المعلومات نهائياً على مشروع قانون حماية البيانات الشخصية بعد إجراء التعديلات عليه، وتم إرساله إلى مكتب المجلس.

- ناقش مجلس النواب مشروع القانون، وجرى التصويت عليه، وبجلسة الاثنين الموافق ٢٤ فبراير ٢٠٢٠، وافق نواب المجلس نهائياً على مشروع قانون حماية البيانات الشخصية المقدم من الحكومة، وذلك **بموافقة ثلثي أعضاء المجلس بوصفه من القوانين المكملة للدستور**[٢١].

- بتاريخ ١٥ يولية ٢٠٢٠ أصدر السيد رئيس الجمهورية القانون المذكور، ونشر فى الجريدة الرسمية (العدد ٢٨ مكرر هـ فى ١٥ يولية ٢٠٢٠)، على أن يُعمل به بعد مضى ثلاثة أشهر من اليوم التالى لتاريخ نشره.

٢٠ - فى هذا الصدد، راجع: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، ص ٨ وما بعدها.

٢١ - تنص المادة ١٢١ من الدستور المصرى الصادر عام ٢٠١٤ في فقرتها الرابعة على ما يلى:"كما تصدر القوانين المكملة للدستور بموافقة ثلثي عدد أعضاء المجلس. وتعد القوانين المنظمة للانتخابات الرئاسية، والنيابية، والمحلية، والاحزاب السياسية، والسلطة القضائية، والمتعلقة بالجهات و الهيئات القضائية، والمنظمة للحقوق والحريات الواردة في الدستور، مكملة له".

ثانياً

فلسفة وأهداف قانون حماية البيانات الشخصية

وأهم الأحكام التى يتضمنها

يُعد إصدار قانون حماية البيانات الشخصية المصري خطوة تشريعية بالغة الأهمية فى مضمار تأمين البيانات الشخصية للمواطنين، وخاصة مع خلو التشريعات القائمة من إطار قانونى ينظم حماية البيانات الشخصية المعالجة إلكترونياً أثناء جمعها أو تخزينها أو معالجتها.

ويعبر القانون عن صور حق الأشخاص في حماية بياناتهم الشخصية، ويُجرم جمع البيانات بطرق غير مشروعة أو بدون موافقة أصحابها، وتجريم معالجتها بطرق تدليسية أو غير مطابقة للأغراض المُصرح بها من قبل صاحب البيانات وتنظيم نقل ومعالجة البيانات عبر الحدود بما يعود بالنفع على المواطنين وعلى الاقتصاد القومي، بما يسهم في حماية الاستثمارات والأعمال، كما يتوافق مع المعايير الدولية في مجالات حماية البيانات الشخصية، وذلك من خلال القواعد والمعايير والاشتراطات التى يفرضها، ويباشر الإشراف عليها مركز حماية البيانات المنشأ لهذا الغرض.

ويشير تقرير اللجنة المشتركة بمجلس النواب حول مشروع القانون إلى أنه يتواكب مع المعيار العالمي الخاص بحماية البيانات الشخصية حالياً في العالم، وهو اللائحة العامة لحماية البيانات الشخصية (GDPR) باعتبارها القواعد الذهبية الموجودة في العالم لحماية البيانات الشخصية للمستخدمين، كما يهدف إلى العمل على حماية خصوصية البيانات بشأن المواطنين والمؤسسات المختلفة داخل وخارج الدولة ويضمن حماية الاستثمارات الوطنية لاسيما المتعاملة مع الاتحاد الأوروبي.

> **التوافق مع اللائحة الأوروبية العامة لحماية البيانات GDPR**

أشار البعض بورشة العمل إلى أنه لا توجد ضرورة لتطابق القانون المصري بصورة كاملة مع اللائحة الأوروبية لحماية البيانات الشخصية وذلك لوجود اختلافات عديدة بين كل من النظامين القانونيين فى شأن تطور التشريعات المنظمة لحماية البيانات الشخصية.

ومع ذلك يوجد اتفاق على أن مراعاة المشرع المصري لأحكام اللائحة وأخذها فى الاعتبار حال صياغة نصوص قانون حماية البيانات الشخصية، كان أمراً محموداً، نظراً لما يتميز به المشرع الأوروبي من تاريخ حافل فى هذا المجال، فضلاً عن أن نطاق التطبيق المكاني لهذه اللائحة لم يمنعها من اجتياز الحدود الجغرافية لتطبق فى العديد من دول العالم، لدرجة جعلت الشركات العالمية الكبرى تسرع وتهرول نحو الامتثال لأحكام هذه اللائحة (مثل ميكروسوفت وجوجل وغيرها).

ومن أهم النقاط التي يقوم عليها القانون هي وضع التزامات على المتحكم والمعالج في البيانات ليضمن تطبيق معايير حوكمة تكنولوجيا المعلومات داخل المؤسسات المختلفة ويحد من عمليات انتهاك خصوصية البيانات الشخصية.

كما تم صياغة القواعد القانونية وتنظيم الإجراءات المتعلقة بحماية البيانات والأنشطة المعلوماتية بما يحقق الالتزامات الدستورية الواردة في المواد (٢٨، ٣١، ٥٧) من الدستور المصري الصادر عام ٢٠١٤[٢٢].

٢٢ – النصوص الدستورية الحاكمة لمشروع القانون:

– المادة (٢٨) من الدستور تنص على أن: "الأنشطة الاقتصادية الإنتاجية والخدمية والمعلوماتية مقاومات أساسية للاقتصاد الوطني، وتلتزم الدولة بحمايتها، وزيادة تنافسيتها، وتوفير المُناخ الجاذب للاستثمار، وتعمل على زيادة الإنتاج، وتشجيع التصدير، وتنظيم الاستيراد. وتولي الدولة اهتماماً خاصاً بالمشروعات المتوسطة والصغيرة ومتناهية الصغر في كافة المجالات وتعمل على تنظيم القطاع غير الرسمي وتأهيله".

– المادة (٣١) من الدستور تنص على أن: "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون".

– المادة (٥٧) من الدستور، سالف الإشارة إليها، يجرى نصها على أن: "للحياة الخاصة حرمة وهي مصونة لا تُمس. وللمراسلات البريدية، والبرقية، والالكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة اشكالها، ولا يجوز تعطيلها او وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك".

١- فلسفة وأهداف إصدار قانون حماية البيانات الشخصية[٢٣]:

جاء مشروع القانون متوخيًا الأهداف الآتية:-

- ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً.
- وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين، ومكافحة انتهاك خصوصيتهم.
- تطبيق إطار معياري يتواكب مع التشريعات الدولية لحماية البيانات الشخصية للأفراد، وحرياتهم، واحترام خصوصيتهم.
- صياغة التزامات على كل من المتحكم في البيانات، ومعالج البيانات باعتبارهما من العناصر الفاعلة في مجالات التعامل في البيانات الشخصية، سواء عن طريق الجمع أو النقل أو التبادل أو التخزين أو التحليل أو المعالجة بأي صورة من الصور.
- إلزام المؤسسات والجهات والأفراد المتحكمين في البيانات الشخصية، والمعالجين لها بتعيين مسئول لحماية البيانات الشخصية داخل مؤسساتهم وجهاتهم، بما يسمح بضمان خصوصية بيانات الأفراد، واقتضاء حقوقهم المنصوص عليها في هذا القانون.
- تقنين وتنظيم أنشطة استخدام البيانات الشخصية في عمليات الإعلان والتسويق على الانترنت، وفى البيئة الرقمية بشكل عام.
- وضع إطار إجرائي لتنظيم عمليات نقل البيانات عبر الحدود وضمان حماية بيانات المواطنين وعدم نقلها أو مشاركتها مع دول لا تتمتع فيها البيانات بالحماية.
- تنظيم العمليات المعالجة إلكترونياً للبيانات الشخصية، وإصدار تراخيص لمن يقوم بها، وعلى الأخص فيما يتعلق بالبيانات الشخصية الحساسة "ذات الطابع الخاص".
- إنشاء مركز حماية البيانات الشخصية كهيئة عامة يكون مختصاً بتنظيم والإشراف على تنفيذ أحكام القانون.

٢٣ - راجع: تقرير اللجنة المشتركة حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، سالف الإشارة إليه، ص ص ٩، ١٠.

٢ - أهم الأحكام التى تضمنها القانون:

جاء القانون، كما وافق عليه مجلس النواب وصدر فى الجريدة الرسمية، في (٧) سبع مواد إصدار، و (٤٩) تسعة وأربعين مادة قانون على النحو التالي:

أ- مواد الإصدار:

المادة الأولى: من قانون الإصدار حددت نطاق سريان القانون من حيث طبيعة البيانات (المعالجة إلكترونياً) والأشخاص (الطبيعيين).

المادة الثانية: حددت نطاق تطبيق القانون من حيث المكان (النطاق الإقليمى للتطبيق)

المادة الثالثة: تضمنت الاستثناءات الواردة على نطاق سريان القانون (٦ حالات).

المادة الرابعة: تنص على اختصاص وزير الاتصالات وتكنولوجيا المعلومات بإصدار اللائحة التنفيذية (خلال ٦ أشهر من تاريخ العمل بالقانون).

المادة الخامسة: قررت اختصاص المحاكم الاقتصادية بنظر المنازعات المتعلقة بأى جرائم ترتكب بالمخالفة لأحكام هذا القانون.

المادة السادسة: ألزمت المخاطبين بأحكام هذا القانون بتوفيق أوضاعهم خلال سنة من تاريخ صدور اللائحة التنفيذية.

المادة السابعة: وهي المادة المتعلقة بنشر القانون في الجريدة الرسمية والعمل به بعد مُضي ثلاثة أشهر من اليوم التالي لتاريخ نشره.

ب - مواد القانون المرافق:

يحتوي على (٤٩) مادة، تندرج تحت (١٤) فصل، وتجرى أحكامه على النحو الآتي:

الفصل الأول تضمن المادة (١) بعنوان "**التعريفات**" الخاصة بالمصطلحات الواردة بالقانون؛ تفادياً للخلاف حول المقصود منها[٢٤].

وتناول **الفصل الثاني** بالمادتين (٢، ٣) **حقوق الشخص المعنى بالبيانات، وشروط جمع ومعالجة البيانات الشخصية.**

٢٤ - تتضمن الفصل الخاص بالتعريفات، عدد (١٨) تعريف للمصطلحات الآتية: (البيانات الشخصية - المعالجة - البيانات الشخصية الحساسة - الشخص المعنى بالبيانات - الحائز - المتحكم - المعالج - إتاحة البيانات الشخصية - أمن البيانات - خرق وانتهاك البيانات الشخصية - حركة البيانات الشخصية عبر الحدود - التسويق الإلكترونى - جهات الأمن القومى - المركز - الترخيص - التصريح - الاعتماد - الوزير المختص).

وأشار **الفصل الثالث** بالمواد (٤، ٥، ٦، ٧) إلى **التزامات المتحكم والمعالج**، كما تناول شروط المعالجة والالتزام بالإخطار والإبلاغ.

وتضمن **الفصل الرابع** بالمادتين (٨، ٩) **مسئول حماية البيانات الشخصية**، من حيث تعيينه والتزاماته.

ونظم **الفصل الخامس** بالمادتين (١٠، ١١) **إجراءات إتاحة البيانات الشخصية**، ومنح الدليل الرقمي المستمد من البيانات حجية في الإثبات.

وتضمن **الفصل السادس** بالمادتين (١٢، ١٣) أحكام **البيانات الشخصية الحساسة.**

ونظم **الفصل السابع** في المواد (١٤، ١٥، ١٦) أحكام حركة **البيانات الشخصية عبر الحدود.**

وجاء **الفصل الثامن** بالمادتين (١٧، ١٨) لينظم أحكام **التسويق الإلكتروني المباشر.**

وأفرد **الفصل التاسع** المواد (من ١٩ إلى ٢٥) **لمركز حماية البيانات الشخصية**؛ من حيث إنشاء المركز وأحكامه واختصاصاته.

وتضمن **الفصل العاشر التراخيص والتصاريح** والاعتمادات، مبيناً **أنواعهم** وإجراءات إصدارهم وتعديل شروطهم وإلغائهم والجزاءات الإدارية بالمواد (من ٢٦ إلى ٣٠).

وبين **الفصل الحادي عشر موازنة مركز حماية البيانات الشخصية وموارده المالية** بالمادة (٣١).

وتضمن **الباب الثاني عشر** أحكام تقديم **الطلبات والشكاوى** بالمادتين (٣٢، ٣٣).

ونظم **الباب الثالث عشر الضبطية القضائية** بالمادة (٣٤).

وأخيراً تعرض **الفصل الرابع عشر** بالمواد (من ٣٥ إلى ٤٩) أحكام **الجرائم والعقوبات**، والصلح والتصالح عليها.

ثالثاً

نطاق تطبيق قانون حماية البيانات الشخصية

حدَّد القانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية نطاق تطبيقه على سبيل الحصر، مستبعداً مجالات متعددة من هذا النطاق، سواء ما تعلق منها بطبيعة المعالجة وصورها أو الأشخاص محل الحماية القانونية، كما حدد نطاق تطبيقه من حيث المكان ومن حيث الزمان، وأورد قائمة موسعة للبيانات الشخصية المستبعدة من تطبيق أحكامه.

١ – من حيث طبيعة البيانات الشخصية وصورها:

أشارت المادة الأولى من قانون الإصدار على أن "يُعمل بأحكام هذا القانون والقانون والمُرافق فى شأن حماية البيانات الشخصية **المعالجة إلكترونياً جزئياً أو كليًا** لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة **للأشخاص الطبيعيين**".

(أ) اقتصار الحماية على البيانات المعالجة إلكترونياً:

يقتصر تطبيق القانون على البيانات المعالجة إلكترونياً فقط، ولا يمتد نطاقه إلى معالجة البيانات المكتوبة أو المخزنة ورقياً بصورة كاملة، إذ يمتد تطبيق القانون للبيانات المعالجة الكترونياً بصورة جزئية، وهوتعبير ينصرف بطبيعة الحال للبيانات المأخوذة ورقياً ثم يجرى معالجتها الكترونياً.

وقد سار المشرع المصري على درب اللائحة العامة لحماية البيانات (الأوروبية) التى نصت فى المادة ١/٢ منها على ما يلى: "تنطبق هذه اللائحة على معالجة البيانات الشخصية كليًا أو جزئيًا بوسائل آلية وعلى المعالجة بخلاف الوسائل الآلية للبيانات الشخصية التي تشكل جزءًا من نظام حفظ الملفات أو يُقصد بها أن تشكل جزءًا من نظام حفظ الملفات".

وجدير بالذكر أن بعض التشريعات لم تفرق بين المعالجة الإلكترونية (الآلية) وغير الإلكترونية (اليدوية)، طالما انصبت على بيانات ذات طابع شخصى، نظراً لوحدة الوظائف والأهداف، وإن اختلف أسلوبها من الجهة التقنية، فلا عبرة للطريقة التى تتم بها معالجة البيانات الواردة أو المزمع وردوها فى ملفات ورقية أو أجندة شخصية أو حتى صورة، سواء تمت المعالجة بطريقة آلية أو غير آلية، كلياً أو جزئياً، وكلتا الطريقتين تمتد إليهما الحماية القانونية على نحو ما أكده القانون الفرنسي بشأن المعلوماتية والملفات والحريات رقم ١٧ لسنة ١٩٧٨ والمُعدّل بالقانون رقم (٤٩٣) لسنة ٢٠١٨ بشأن حماية البيانات الشخصية(م٢)[٢٥]، وما أخذ به أيضاً القانون المغربي (م١/٢)[٢٦].

(ب) الأشخاص المخاطبون بالقانون: سريان القانون على بيانات الشخص الطبيعي:

ينحصر نطاق تطبيق القانون فى بيانات الأشخاص الطبيعيين، وهو ما يعنى استبعاد البيانات الخاصة بالشخص الاعتباري العام أو الخاص، وهو منطق غريب، لا يوجد له تبرير، إذ منح المشرع الشخص الاعتباري شخصية قانونية، ونص على تمتعه بجميع الحقوق إلا ما كان منها ملازماً لشخصية الإنسان الطبيعية وذلك فى الحدود التى قررها القانون (المادة ١/٥٣ مدنى)، وباتت بيانات الأشخاص الاعتبارية تحظى بأهمية بالغة فى الوقت الحاضر قد تفوق أهمية بيانات الشخص الطبيعى، وهو ما يحتاج لإفراد حماية خاصة بها.

ومن المسلم به، أن الشخصية الطبيعية للإنسان تبدأ بتمام ولادته حياً، فيجب إذن أن تكون ولادته تامة، وأن يكون قد ولد حياً، وتنتهى الشخصية بالموت (المادة ٢٩ مدنى)، وما بين الولادة والموت يوجد الشخص الطبيعى، ويتمتع بأهلية الوجوب، وهى صلاحيته لأن تكون له حقوق وعليه واجبات[٢٧]، فضلاً عن أهلية الأداء ومناطها التمييز والإدراك[٢٨].

٢٥ – وضع القانون الفرنسي رقم ٤٩٣ لسنة ٢٠١٨ أحكاماً تهدف لتطويع قواعد القانون الفرنسي مع لائحة (الاتحاد الأوروبي) العامة لحماية البيانات رقم ٦٧٩/ ٢٠١٦ (GDPR)، والتوجيه الأوروبي رقم ٦٨٠/ ٢٠١٦، ومعدلاً قانون المعلوماتية والملفات والحريات رقم ١٧ لسنة ١٩٧٨ فيما يتعلق بحماية البيانات الشخصية. كما صدر المرسوم رقم ١١٢٥ لسنة ٢٠١٨ الصادر فى ١٢ ديسمبر ٢٠١٨ لتطبيق أحكام هذا القانون.

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n°0288 du 13 décembre 2018.

وتنص المادة ٢ من القانون رقم ١٧ لسنة ١٩٧٨ بشأن المعلوماتية والحريات المعدل بالمرسوم رقم ١١٢٥ لسنة ٢٠١٨، على أن: "ينطبق هذا القانون على المعالجة الآلية للبيانات الشخصية كلياً أو جزئياً، وكذلك على المعالجة غير الآلية للبيانات الشخصية الواردة أو المطلوب ظهورها في الملفات، عندما يستوفي المسئول الشروط المنصوص عليها في المادة ٣ من هذا القانون، باستثناء المعالجة التي يقوم بها الأشخاص الطبيعيون لممارسة الأنشطة الشخصية أو المحلية البحتة".

٢٦ – تنص المادة ٢ /١ من القانون المغربى المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي (الصادر فى ١٨ فبراير ٢٠٠٩) على أنه: " يطبق هذا القانون على المعالجة الآلية الكلية أو الجزئية للمعطيات ذات الطابع الشخصي وكذا على المعالجة غير الآلية للمعطيات ذات الطابع الشخصي الواردة أو المرتقب ورودها في ملفات يدوية".

٢٧ – تناول القانون المدنى المصرى فى الفصل الثانى (الأشخاص) منه، أحكام "الشخص الطبيعى، فى المواد من ٢٩ إلى ٥١ مدنى، كما تناول أحكام الشخص الاعتبارى فى المواد من ٥٢ إلى ٥٣ مدنى.

٢٨ – راجع: مجموعة الأعمال التحضيرية للقانون المدنى المصرى: الجزء الأول: الباب التمهيدى أحكام عامة وزارة العدل، مطبعة دار الكتاب العربى، ص ٢٩ وما بعدها.

٢ - البيانات الشخصية المُستبعدة من نطاق القانون: توسع غير محمود:

أشارت المادة الثالثة من القانون إلى طائفة من البيانات الشخصية، وإن كانت تعد شخصية أى خاصة بالأشخاص الطبيعيين، ومُعالجة إلكترونياً كلياً أو جزئياً، ولكن لا يسري عليها أحكام قانون حماية البيانات الشخصية، ولا تتمتع بالحماية، وذلك بُغية تحقيق أهداف ومرامي متنوعة، فتقتصر الحماية على البيانات الشخصية التى تتم فى إطار مهنى أو تجاري، ويخرج من نطاقها البيانات التى تتم معالجتها فى سياق أو إطار شخصي أو منزلي بحت[٢٩]، أو تناولها لأغراض إعلامية بحتة، أو ما يرتبط منها بالحفاظ على الأمن القومى وأغراض منع الجرائم أو ضبط مرتكبيها أو تنفيذ العقوبات وأعمال السلطة القضائية[٣٠].

ويجري نص المادة الثالثة على أن: "لا تسرى أحكام القانون المرافق على ما يلى:

١ - البيانات الشخصية التى يحتفظ بها الاشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي.

وهو استبعاد يتسق مع منطق الأمور، إذ يكمن الهدف من التنظيم القانوني فى حماية بيانات الأشخاص من تعرضها لانتهاك واستغلال من جانب الغير، أما في هذه الحالة فمن غير المتصور أن يكون الاستخدام الشخصي محلاً لانتهاك الخصوصية والاستغلال.

٢ - البيانات الشخصية التى تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني.

٣ - البيانات الشخصية التى تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخدم فى أغراض أخرى وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام.

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

٥ - البيانات الشخصية لدى جهات الأمن القومى وما تقدره لاعتبارات أخرى. ويجب على المركز، بناء على طلب من جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم اظهار أو إتاحة أو تداول البيانات الشخصية خلال مدة زمنية محددة، وفقا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به.

٢٩ - راجع: المادة ٢/ ج من اللائحة العامة لحماية البيانات الشخصية (GDPR).

٣٠ - راجع: المادة ٢/ د من اللائحة العامة لحماية البيانات الشخصية (GDPR).

٦ - **البيانات الشخصية لدى البنك المركزى المصري والجهات الخاضعة لرقابته وإشرافه** عدا شركات تحويل الأموال وشركات الصرافة، على أن يراعى فى شأنهما القواعد المقررة من البنك المركزى المصري بشأن التعامل مع البيانات الشخصية[٣١]".

> **حدوث اختلاف فى وجهات النظر حول استبعاد البيانات لدى البنك المركزى عند مناقشة مشروع القانون**

ويُلاحظ على مسلك المشرع المصري **توسعه بشكل كبير** فى استبعاد طائفة كبيرة من البيانات الشخصية من نطاق الحماية التى يضفيها هذا القانون الجديد على البيانات، رغم حاجتها لإضفاء الحماية عليها، ودون مبرر أو علة، ومن ذلك البيانات الشخصية لدى البنك المركزى، والبيانات المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية ولدى جهات الأمن القومى، حيث كان من الأولى وضعها تحت مظلة الحماية وفق ضوابط تراعى خصوصيتها، وليس استبعادها على إطلاقها.

ومن جهة أخرى، تفتح هذه المادة الباب واسعاً لاستبعاد البيانات لدى جهات الأمن القومى (المتعددة)، بالإضافة إلى "ما تقدره هذه الجهات لاعتبارات أخرى"، أي اعتبارات خلاف الأمن القومى وهي بالطبع كثيرة!

> **التوسع فى البيانات المستبعدة من نطاق تطبيق القانون أفرغه - لحد ما - من مضمونه!**

٣١ - يُشار إلى سابقة رفض لجنة الاتصالات وتكنولوجيا المعلومات بمجلس النواب ووزارة الاتصالات طلب البنك المركزي باستثنائه والجهات التابعة له من مشروع قانون "حماية البيانات الشخصية"، تأسيساً على أن القطاع المصرفي في العالم يخضع لحماية مضافة للبيانات لأنها بطبيعتها بيانات حساسة، وأن فلسفة مشروع القانون تكمن فى تنظيم حماية البيانات وليس وضع سرية على البيانات. وتعليقاً على ذلك صرح البعض - ممن شاركوا فى إعداد مشروع القانون - بأن هذا الاستثناء يُفرغ القانون من مضمونه ويجعله بلا قيمة ويمثل عدم استيعاب لفلسفة حماية البيانات الشخصية التي تعد حقًا أصيلاً للمواطن. ولكن ظهر القانون فى النهاية بعد مناقشته فى المجلس متضمنا هذا الاستثناء! راجع بوابة جريدة الأهرام، بتاريخ ٢٠١٩/٦/١٧ على الموقع التالى:
http://gate.ahram.org.eg/News/2224851.aspx

٣ - نطاق تطبيق القانون من حيث المكان ومن حيث الزمان:

لكل قاعدة قانونية نطاقين، الأول هو النطاق المكاني والثاني هو النطاق الزماني، وقد حددت المادة الثانية من القانون نطاق تطبيقه المكاني ثم الزماني.

نطاق التطبيق من حيث المكان:

جاءت المادة الأولى من قانون الإصدار تفيد العمل بأحكام هذا القانون والقانون المرافق فى شأن حماية البيانات الشخصية المعالجة إلكترونياً جزئياً أو كلياً لدى أى حائز أو متحكم أو معالج لها، وذلك بالنسبة للأشخاص الطبيعيين، ولكنها لم تحدد مجال انطباقها من حيث المكان، وهو مسلك غريب، فالنظر لهذا النص على إطلاقه من شأنه أن ينصرف لكافة البيانات لدى أي متحكم فى أي مكان خارج مصر، وهو أمر لا يستقيم ولا يسوغ قبوله.

وفى المقابل، تشير المادة الثانية من قانون الإصدار إلى سريان أحكام هذا القانون على كل من **ارتكب إحدى الجرائم** المنصوص عليها في القانون المرافق متى كان **الجانى**:

- من المصريين داخل الجمهورية أو خارجها.

- أو كان من غير المصريين المقيمين داخل الجمهورية.

وجاء ذلك أخذاً بكل من مبدأي إقليمة القوانين وشخصية القوانين مجتمعين، حيث يمتد أثر تطبيق القانون للمصريين المقيمين بالخارج أخذاً بمبدأ شخصية القوانين، كما يطبق القانون على جميع المقيمين في جمهورية مصر العربية سواء من المصريين أو الأجانب، أخذاً بمبدأ الإقليمية.

فمن ناحية تحرص هذه الفقرة على إبراز مبدأ إقليمية القانون La territorialité des lois، على نحو ما أخذ به قانون العقوبات المصري بحسب الأصل[٣٢]، وهو يرتبط بحق الدولة فى السيادة على كل إقليمها، وعلى كل من يوجد وكل ما يقع على هذا الإقليم، وهو ما يعنى سريان قانون الدولة على كل نشاط يجري على هذا الإقليم، وعلى كل شخص داخل حدود هذا الإقليم.

ومن ناحية أخرى، توجد بعض الاستثناءات على هذا المبدأ، حيث يطبق قانون الدولة على جميع الأشخاص الذين يحملون جنسيتها، فى أي مكان يوجدون، حتى ولو وجدوا خارج إقليم دولتهم، وهذا هو ما يعرف بمبدأ شخصية القوانين La personalité des lois، وهو حق يفتقر إلى الفعالية في كل حالة يصطدم فيها بحق دولة أخرى فى السيادة على إقليمها، ولهذا نجد أن قانون العقوبات ينطبق انطباقاً إقليمياً كقاعدة أساسية، مع وجود استثناءات ترجع إلى مبدأ الشخصية أو إلى غيره من المبادئ القانونية[٣٣].

كما ينطبق قانون حماية البيانات الشخصية أيضاً متى كان **الجانى**:

- من غير المصريين خارج الجمهورية إذا كان الفعل معاقبًا عليه في الدولة التى وقع فيها تحت أي وصف قانوني، وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية.

أشار القانون إلى سريان أحكامه على غير المصري فى الخارج فى هذه الحالة على أساس الصلة بين الشخص (مصري أو أجنبي مقيم فى مصر) والبيانات محل الجريمة[٣٤].

ويعني ذلك أن المشرع اعتد فى هذه الصورة بالجنسية المصرية للشخص المعنى بالبيانات أو محل إقامته فى مصر، بصرف النظر عن مكان وقوع الجريمة، وأياً كان محل تواجد الجانى. وقد تثور مشكلة تنازع القوانين وخاصة فى حالة الاعتداء على بيانات لمصريين، من الخارج، ومما يزيد هذه المسألة تعقيداً أن النص اشترط للتجريم أن يكون الفعل معاقبًا عليه في الدولة التى وقع فيها، فعلى افتراض وقوع اعتداء على بيانات **شخص مصري**، مقيم فى ألمانيا مثلاً، من قبل شخص ألمانى مقيم فى ألمانيا، فكيف يتسنى فى هذه الحالة معاقبة الأجنبي المقيم خارج مصر، إذ يخضع بطبيعة الحال للقانون الألماني، وفقاً لمبدأ الإقليمية.

تعقيب: يُلاحظ أن السمة الغالبة على هذا القانون، وحسبما صرح المشرع نواحي كثيرة منه، وخاصة فى مواد الإصدار وهي قبلة القانون، أنه **يُصنف ضمن طائفة القوانين العقابية**، إذ يُركز على انطباقه فى حالة ارتكاب الجرائم الواردة فيه، رغم أنه من المفروض أن يكون قانون حمائي فى المقام الأول هدفه الوقاية أو المنع، إلى جانب الزجر والردع، عبر تنظيم دقيق لمظاهر حماية البيانات الشخصية.

وقد راعت المادة الثالثة من لائحة الاتحاد الأوروبي GDPR، المعنية بالنطاق الإقليمى لتطبيق أحكامها، الأخذ بمعيار موطن المعالج أو المتحكم فى البيانات بصرف النظر عما إذا كانت المعالجة تتم فى الاتحاد الأوروبي أم لا، كما تنطبق اللائحة على البيانات المتداولة داخل الاتحاد رغم وجود المعالج أو

٣٢ - نصت المادة الأولى من قانون العقوبات المصرى على أن: "تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه". ويستفاد من هذا النص أن قانون العقوبات المصرى ينطبق على كل جريمة ترتكب فى مصر سواء كان مرتكبها مصرياً أو غير مصرى.

٣٣ - راجع: د. سمير عبد السيد تناغو: النظرية العامة للقانون، منشأة المعارف، الإسكندرية، ١٩٧٣، ص ص ٦٣٥، ٦٣٦.

٣٤ - تعد هذه القاعدة من بين الاستثناءات على مبدأ إقليمية القانون، وقد سبق وأن أخذ بها المشرع فمد نطاق سريان قانون العقوبات المصرى إلى كل من ارتكب خارج مصر فعلاً يجعله فاعلاً أو شريكاً فى جريمة وقعت كلها أو بعضها فى مصر (م ٢ من قانون العقوبات).

المتحكم خارج الاتحاد متى تعلقت أنشطة المعالجة بعرض سلع أو خدمات لأصحاب هذه البيانات داخل الاتحاد، أو يوجد فى مكان ينطبق فيه قانون الدول الأعضاء بموجب القانون الدولي العام (م ٣ من اللائحة الأوروبية)

٤- الاختصاص القضائي:

نصت المادة الخامسة على أن المحاكم الاقتصادية تختص بنظر الجرائم التى ترتكب بالمخالفة لأحكام القانون المرافق.

بيد أن القانون لم يبين الاختصاص القضائي بالمنازعات الناشئة عن هذا القانون، وهى لا تعد من قبيل الجرائم، أياً كان نوعها، وخاصة المنازعات المدنية أو التجارية، كالاعتراض على عمليات الجمع والمعالجة، أو المطالبة بالتعويض وغيرها، ومن ثم من المفروض أن تخضع أيضاً لاختصاص المحاكم الاقتصادية.

وقد أوصت المناقشات بالورشة بضرورة تعديل القانون لجعل الاختصاص للمحاكم الاقتصادية في كافة المنازعات الناشئة عن تطبيق أحكام هذا القانون (وليس الجرائم فقط).

٥ - مبادئ حماية البيانات:

لم يحدد القانون الجديد، على خلاف الحال مع اللائحة الأوروبية لحماية البيانات (الفصل الثانى منه)[٣٥]، سلسلة من المبادئ لحماية البيانات التي يجب على المؤسسات المعنية الالتزام بها، والتي تشمل (من بين جملة أمور أخرى) مفاهيم مألوفة مثل مبادئ القانونية والإنصاف والشفافية والخصوصية.

وتفرض اللائحة الأوروبية التزامًا صريحًا على وحدات التحكم والمعالجة بإنشاء برنامج خاص لإثبات الخضوع للقانون، ويعتمد مدى تعقيد البرنامج ومستوى التفاصيل فيه جزئيًا على حجم المؤسسة المعنية ومواردها إضافة إلى المخاطر التي تفرضها المعالجة على أصحاب البيانات. ومع ذلك، يجب أن يثبت البرنامج أن المبادئ الأساسية للقانون جزء لا يتجزأ من المؤسسة.

٦- نشر القانون ونفاذه وإصدار اللائحة التنفيذية:

نصت المادة السابعة من القانون على أن يُنشر فى الجريدة الرسمية (وقد نُشر فى العدد ٢٨ مكرر هـ فى ١٥ يولية ٢٠٢٠)، ولكنها لم تنص على الأثر الفورى لسريانه، نظراً لما له من تأثير على قطاعات عريضة فى المجتمع المصري، ويحتاج للتريث فى تطبيقه، ولهذا نصت على أن يُعمل به بعد مضي ثلاثة أشهر من اليوم التالي لتاريخ نشره، أي بعد مضى ثلاثة أشهر من تاريخ ١٦ يولية ٢٠٢٠ (اليوم التالى للنشر)، ومن ثم يدخل هذا القانون حيز النفاذ اعتباراً من ١٦ أكتوبر ٢٠٢٠.

ووفقاً للمادة الرابعة من القانون يُصدر الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات اللائحة التنفيذية للقانون المرافق **خلال** ستة أشهر من تاريخ العمل بذلك القانون.

وحيث من المقرر أن هذا القانون بدأ العمل به بعد مضى ثلاثة شهور، أى فى أكتوبر الجارى، فإن اللائحة يجب أن تصدر بحد أقصى فى منتصف أبريل ٢٠٢١.

ويلتزم المخاطبون بأحكام هذا القانون بتوفيق أوضاعهم طبقًا لأحكام القانون المرافق ولائحته التنفيذية، وذلك خلال سنة من تاريخ صدور اللائحة التنفيذية (المادة ٦ من القانون).

> **ضرورة صدور اللائحة التنفيذية للقانون خلال منتصف شهر أبريل ٢٠٢١.**

٣٥ - راجع: الفصل الثانى من اللائحة العامة لحماية البيانات GDPR بعنوان "المبادئ"، المادة ٥ "المبادى المتعلقة بمعالجة البيانات، و المادة ٦ "قانونية التجهيز".

المحور الأول

الإطار المفاهيمي
لقانون حماية البيانات الشخصية

■ تمهيد:

لا جرم أن التعرض للمفاهيم الواردة فى قانون حماية البيانات الشخصية وتوضيحها وسبر أغوارها، يعتبر من الأمور الضرورية في هذا السياق، قبل الخوض فى تناول أحكام هذا القانون، إذ يؤدي اتسام بعض المفاهيم بالغموض إلى فهمها وتناولها بشكل خاطئ مما يؤثر بشكل كبير على الأهداف والمرامي والآثار التى يرغب المشرع فى ترتيبها من خلال أحكام القانون.

وقد أوردت المادة الأولى من قانون حماية البيانات عدد (١٨) تعريفاً لعدد من المفاهيم والمصطلحات المختلفة، منها ما هو متعلق بعملية الحماية وأطرافها ومنها ما هو متعلق بالجهات القائمة على تنفيذ القانون.

ونود الإشارة إلى أن الدراسة سوف تقتصر على بحث بعض المفاهيم الجوهرية اللازمة لبيان أحكام القانون، فقط، دون البعض الآخر، كما سيتم إيضاح بعض المفاهيم الأخرى التي لم ترد بهذا القانون ولكنها تتصل به إلى حد كبير.

لذلك سوف يتم التعرض لأهم المفاهيم الواردة بقانون حماية البيانات الشخصية (البيانات الشخصية، معالجة البيانات الشخصية) ومن قبلها المفاهيم المرتبطة وذلك على النحو التالي:-

أولاً - مفهوم البيانات الشخصية.

ثانياً - مفهوم معالجة البيانات الشخصية وتحديد أطرافها.

أولاً

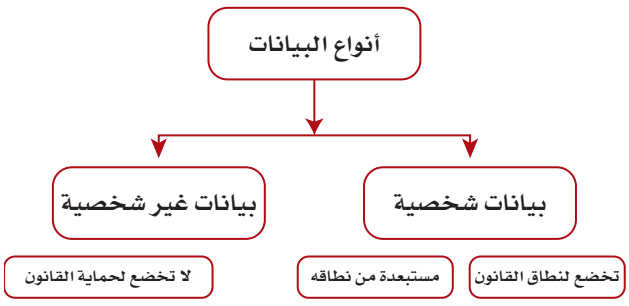
مفهوم البيانات الشخصية

من أجل الوقوف على تعريف واضح ودقيق لمفهوم البيانات الشخصية لابد أولاً التفرقة بين البيانات الشخصية المشمولة بالحماية القانونية وغيرها من البيانات غير المشمولة بهذه الحماية، ليس هذا فحسب وإنما يجب أيضاً تحديد البيانات غير الشخصية وذلك للتفرقة بينها وبين البيانات سالفة الذكر.

ولاشك أن تصدى القوانين الوطنية لتقديم تعريفات محددة للبيانات الشخصية، من شأنه تيسير مهمة القائمين على أعمال جمع ومعالجة البيانات[٣٦].

وفى هذا الصدد، تجدر الإشارة إلى تعدد أنواع البيانات الشخصية، فهى لا تقع تحت حصر، وتختلف بحسب النظر إليها، فمنها بيانات شخصية تخضع لتطبيق القانون، ومنها بيانات غير شخصية تخرج من نطاق هذه الحماية.

كما أشرنا فى المحور التمهيدى إلى أن القانون استبعد طائفة من البيانات الشخصية من نطاق تطبيقه، ومنها البيانات التى تتم معالجتها فى سياق أو إطار شخصي أو تناولها لأغراض إعلامية بحتة، أو ما يرتبط منها بالحفاظ على الأمن القومي والبيانات لدى البنك المركزي.



ومن هنا نتناول تعريف البيانات الشخصية التى ينطبق عليها القانون، ثم نتعرض للبيانات غير الشخصية المستبعدة من نطاق الحماية القانونية، وأخيراً نشير إلى البيانات غير الشخصية والمستبعدة بالطبع من نطاق الحماية القانونية للبيانات، ونخصص لكل مسألة منها فقرة مستقلة.

١ - تعريف البيانات الشخصية

تصدى المشرع المصري لتعريف البيانات الشخصية فى القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات حين نص فى المادة الأولى منه على أنه يقصد بالبيانات الشخصية: "أى بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين أي بيانات أخرى"[٣٧].

ثم ما لبث أن عاد المشرع المصري وقام بتعريف البيانات الشخصية في المادة الأولى من قانون حماية البيانات الشخصية، بأنها "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى، كالاسم أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الانترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية".

وبقراءة النص المصري بشكل متعمق يظهر أنه قد اقتصر على البيانات المتعلقة بالأشخاص الطبيعيين فقط، كما تضمن التعريف للبيانات الشخصية بعض الأمثلة التى تبين هوية الشخص مثل الاسم أو الصورة أو الصوت ..... وكل الأمثلة التي وردت بهذه المادة بالنسبة للبيانات الشخصية إنما أتت على سبيل المثال وليس على سبيل الحصر، وهذا يعني أن أية بيانات أخرى من الممكن أن يتم اعتبارها بيانات شخصية طالما تعلقت بشخص طبيعي محدد أو من الممكن تحديده.

أما إذا كانت هذه البيانات غير متعلقة بشخص محدد ولا توجد أية إمكانية لتحديده بشكل مباشر أو غير مباشر، فإنه بمفهوم المخالفة لنص المادة في تعريفها للبيانات الشخصية لا يمكن اعتبار هذه البيانات بيانات شخصية، وذلك لأن المشرع قد اشترط أنه لابد أن تكون البيانات متعلقة بشخص محدد أو يمكن تحديده لاعتبارها بيانات شخصية.

كما تعرف المادة ٤ من اللائحة الأوروبية (GDPR) "البيانات الشخصية Personal data" بأنها "تعني أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد (صاحب البيانات)؛ والشخص الطبيعي هو الشخص الذى يمكن تحديد هويته بشكل مباشر أو غير مباشر، بوجه خاص بالرجوع إلى محدد للهوية (مُعرف شخصي an identifier) مثل الاسم أو رقم الضمان

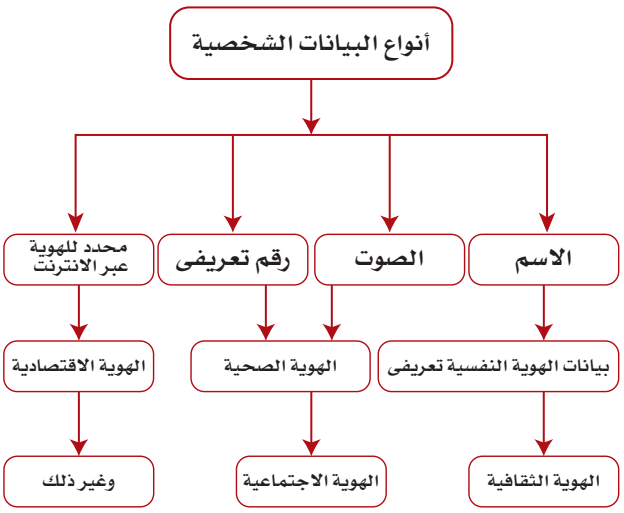
36 - Stephen Allison, The Concept of Personal Data under the Data Protection Regime, Edinburgh Student Law Review, Volume 1, Issue 1, 2009, p. 2.

٣٧ – الجريدة الرسمية – العدد ٣٢ مكرر (ج) فى أغسطس سنة ٢٠١٨.

الاجتماعي identification number أو بيانات الموقع أو المعرّف عبر الإنترنت (عنوان IP أو عنوان البريد الإلكتروني) أو لواحد أو أكثر من العوامل الخاصة بالهوية البدنية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي.

ويكاد يتطابق تعريف القانون المصري للبيانات الشخصية مع التعريف الوارد فى اللائحة الأوروبية، ومد نطاق تحديد هوية الشخص إلى النواحي الصحية أو الثقافية أو الاقتصادية أو الاجتماعية، بيد أن الأخير توسع بعض الشئ فى بيان المسائل الخاصة التى يمكن الاستعانة بها لتحديد هوية الشخص الطبيعي، وهي تشمل، لأول مرة، أمور مثل المعلومات الجينية أو العقلية ومع هذا جاء التعريف المصري عاماً وواسعاً أيضاً بما يسمح باستيعاب هذه المسائل لتحديد هوية الشخص الطبيعي.

وقد وجه بعض الفقه سهام النقد لتعريف البيانات الشخصية واعتبروه موسع للغاية[٣٨] منوهين أن التحليلات الضخمة للبيانات من شأنها أن تجعل التفرقة بين البيانات التى من شأنها أن تجعل الشخص قابل للتعريف وتلك التى لا تجعل الشخص قابل للتعريف لا قيمة لها[٣٩].



كذلك يعرف المشرع الفرنسي البيانات الشخصية فى المادة الثانية من قانون المعلوماتية والحريات (المعدل) بأنه: "يعتبر بياناً شخصياً أي معلومة تتعلق بشخص طبيعي محدد هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة، سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه".

ووفقاً للتعريف المشار إليه فإن أي معلومة تتعلق بشخص طبيعي يمكن تحديد هويته تُعتبر بياناً شخصياً يخضع للحماية القانونية، طالما أن هذا الشخص الطبيعي محدد هويته، أو أنه من الممكن تحديد هويته بأي طريقة مباشرة أو غير مباشرة.

ويبدو من ذلك أن تعريف البيانات يعتبر بمثابة معيار يمكن عن طريقه تحديد ما إذا كانت المعلومة تعتبر بياناً شخصياً أم لا، ومن ثم مدى خضوعها للحماية القانونية للبيانات الشخصية من عدمه.

وتجدر الإشارة إلى أن الحماية القانونية للبيانات الشخصية قاصرة فقط على البيانات الشخصية الخاصة بالأشخاص الطبيعيين، ومن ثم فالبيانات الخاصة بالشخص المعنوي مستبعدة من نطاق الحماية القانونية[٤٠]، كما سبق أن أشارت الدراسة[٤١].

٢- تعريف البيانات غير الشخصية

يُستفاد بمفهوم المخالفة من تعريف البيانات الشخصية وفقاً للقانون، أن البيانات الشخصية هى البيانات التى لا يمكن عن طريقها تحديد هوية الشخص الطبيعي بشكل مباشر أو غير مباشر، أو بمعنى آخر غير ناطقة الدلالة فى تحديد الشخص والتعرف عليه وتمييزه عن غيره.

ومن ثم "يقصد بالبيانات غير الشخصية Non-personal data" تلك البيانات التي لا يمكن أن تفصح عن هوية الشخص الفعلية، ومنها على سبيل المثال المعلومات الخاصة بنوع الجنس أو نوع المتصفح الذي تستخدمه أو نوع السيارة التي يفضلها.

وبطبيعة الحالة تعتبر بيانات غير شخصية، بيانات الشخص الاعتباري، فعلى سبيل المثال أورد المشرع المصري تعريفاً للبيانات الحكومية، وهى بيانات غير شخصية، في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، فعرفها بأنها: "بيانات متعلقة بالدولة أو أحد سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والأجهزة الرقابية، وغيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام

38 - Nadezhda Purtova (2018), The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176, p. 3.

39 - O Tene and J Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, (2013) 11 Northwestern Journal of Technology and Intellectual Property 258, pp. 19-20.

٤٠ – د. سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية "دراسة مقارنة بين القانون الفرنسي والقانون الكويتي"، مجلة كلية القانون الكويتية العالمية، السنة الثالثة، العدد التاسع، مارس ٢٠١٥م، ص ص ٤٠١-٤٠٢.

٤١ – راجع: "نطاق تطبيق قانون حماية البيانات الشخصية" من المحور التمهيدى من هذه الدراسة.

معلوماتي أو على حاسب أو ما في حكمها"[٤٢].

ومن ثم تخرج البيانات غير الشخصية من مجال الحماية التى يوفرها القانون، بيد أن ذلك لا يعني على الإطلاق عدم وجود حماية توفرها لها التشريعات الحديثة إزاء عمليات المعالجة، فهذه البيانات غير متروكة - كما قد يتصور البعض - دون أطر قانونية تحميها، فهناك العديد منها - مثل البيانات الحكومية - مشمولة بالحماية بموجب تشريعات مختلفة.

وإذا كان يبدو أن المشرع المصري قد قصر الحماية القانونية على عمليات المعالجة الخاصة بالبيانات الشخصية دون غيرها من البيانات فى إطار قانون حماية البيانات، وبالتالى فإن هذه البيانات غير الشخصية لا تخضع للحماية القانونية التى يوفرها هذا القانون إزاء عمليات المعالجة، ولهذا فإن البحث لن يشملها بالنقاش أبعد من القدر الذى يستدل به بمفهوم المخالفة على نطاق البيانات الشخصية.

٣- تعريف البيانات الشخصية الحساسة

وفقاً للمادة الأولى من القانون يقصد بالبيانات الشخصية الحساسة "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.

ويلاحظ على مسلك المشرع أنه وصف بعض البيانات بالحساسة، ومن ثم يغاير فى المعاملة بشأنها، من حيث الجمع والمعالجة، ومنها البيانات البدنية، أو الجينية، والأخيرة اعتبرتها اللائحة الأوروبية ضمن طوائف البيانات الشخصية، دون تفرقة بين البيانات العادية أو الحساسة.

ويلاحظ فى هذا الصدد، أن المشرع اعتبر كافة البيانات المتعلقة بالأطفال تعتبر بيانات حساسة، وهى عبارة عامة تنصرف بداهة ولأول وهلة إلى أى بيان يتعلق بالطفل حتى وإن كان يندرج ضمن البيانات الشخصية (العادية أى غير الحساسة)، مثل الاسم واللقب والصوت، وأى بيانات أخرى تحدد هويته.

بينما نجد أن اللائحة الأوروبية لم يرد بها تعريف لمسمى البيانات الحساسة، وإنما جاءت بتعريفات لبعض البيانات بصفة خاصة (م ٤ بنود من ١١-١٣)، فبجانب تعريف البيانات الشخصية، ذكرت تعريفاً لكل من البيانات الجينية وبيانات القياسات الحيوية "البيومترية" والبيانات المتعلقة بالصحة.

ومن هنا نلاحظ أن اللائحة الأوروبية أوردت تحديداً منفصلاً لتوضيح بعض البيانات، فعرفت المادة ٤ (بند ١٤) من اللائحة بيانات القياسات الحيوية "**البيومترية**" Biometric Data بأنها "تعني البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تؤكد التحديد الفريد لهذا الشخص الطبيعي، مثل صور الوجه".

كما عرفت أيضاً "البيانات المتعلقة بالحالة الصحية Data Concerning Health " (م ٤ بند ١٥) بأنها تعني "البيانات الشخصية المتعلقة بالصحة الجسدية أو العقلية للشخص الطبيعي، بما في ذلك توفير خدمات الرعاية الصحية، والتي تكشف عن معلومات حول حالته الصحية".

وكذلك عرفت اللائحة البيانات الجينية "الوراثية" Genetic Data (م ٤ بند ١٣)، بأنها "تعني البيانات الشخصية المتعلقة بالخصائص الجينية الموروثة أو المكتسبة لشخص طبيعي والتي تقدم معلومات فريدة عن فسيولوجيا أو صحة ذلك الشخص الطبيعي والتي تنتج، على وجه الخصوص، من تحليل عينة بيولوجية من الشخص الطبيعي المعنى".

ويستفاد مما تقدم إلى أنه على خلاف اللائحة الأوروبية تغاضى المشرع المصري عن تحديد المقصود بكل من البيانات التى ألحق بها صفة الحساسية (مثل البيانات البيومترية أو الجينية).

كما نجد أن المشرع الأوروبي وإن كان خص بعض البيانات بالتعريف إلا أنه لم يجمعها تحت مسمى البيانات الحساسة، ولقد ذكرت اللائحة فى هذا الشأن أن تحديد ما اذا كان بيان ما حساس من عدمه، هو أمر متروك تقديره للتشريعات الوطنية بدول الاتحاد.

وربما كان من الأفضل لو أورد المشرع المصري تعريفاً لأنواع البيانات الشخصية التى وصفها بالحساسة.

٤٢ - المادة الأولى من القانون رقم ١٧٥ لسنة ٢٠١٨م بإصدار قانون مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد (٣٢) مكرر (ج)، ١٤ أغسطس سنة ٢٠١٨م.

وتوصي الورشة بتدخل المشرع المصري لإدراج هذه التعريفات حال إجراء تعديلات على القانون أو أن يُفرد لها تعريفات فى اللائحة التنفيذية للقانون.

وربما كان من الأفضل لو أورد المشرع المصري تعريفاً لأنواع البيانات الشخصية التى وصفها بالحساسة.

وبينما أورد المشرع الأوروبي تعريفات لبعض البيانات التى وصفها المشرع المصري بكونها حساسة دون تعريفها، نجد أن كلا المشرعين قد أغفلا تعريف "البيانات المالية"، وربما كان من الأفضل أن يتم تعريف تلك البيانات لكي لا تبقى متروكة لتفسير الخاضعين للقانون.

إلا أن إغفال تعريف البيانات المالية من قبل المشرع المصري يترك مجالاً خصباً للتساؤلات، فربما يفهم أنه قد أغفلها عن قصد حينما استبعد بيانات البنك المركزي والبنوك (التى تتركز حول بيانات مالية) من نطاق تطبيقه. غير أن هذا الفرض ربما يكون مبالغاً فيه لأن مصطلح البيانات المالية أوسع من أن يتم قصره على البيانات المالية المتعلقة بالبنوك، وبالتالى حتى ولو كان هذا هو سبب إغفال تعريف المصطلح من قبل المشرع المصري فإن ذلك يعد قصورًا يستوجب التعديل أو إلحاق تعريف باللائحة التنفيذية المنتظر صدورها.

وكذلك إغفال تعريف البيانات المتعلقة بالصحة (سواء الجسدية أو النفسية أو العقلية) والبيانات الجينية وبيانات القياسات الحيوية قد يؤدى إلى صعوبات فى فهم وتفسير النص- تضييقاً أو توسيعاً - حال التطبيق العملى بما لا يؤدي معه الغرض المقصود منه، كما أنه حتى فى وجود تعريفات يظل هناك متسع من المجال لتفسيرات الفقه والقضاء.

ثانياً

مفهوم معالجة البيانات الشخصية وتحديد أطرافها

نتناول فى هذا المقام، تعريف المعالجة والمصطلحات المرتبطة بها، ثم نشير إلى تعريف المتحكم والمعالج والحائز للبيانات (بصفتهم القائمين على المعالجة).

١ - تعريف المعالجة والمصطلحات المرتبطة بها

أ - تعريف المعالجة:

عرف المشرع المصري **المعالجة** بأنها: "أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئياً أو كلياً".

وفى شأن هذا التعريف، ربما كان من الأفضل لو ابتعد المشرع المصري عن إيراد لفظ "الكترونياً" واكتفى بالإشارة إلى أن المعالجة هى تلك العمليات "التقنية"[٤٣] وذلك لضبط دقة الصياغة[٤٤].

٤٣ - يشير تقرير قسم التشريع بمجلس الدولة فى هذا الشأن أن لفظ "تقنية" لغة يعنى: "أى عملية فنية تستهدف التعامل مع الحواسيب الإلكترونية وبرمجيات الحاسوب لتحويل وتخزين وحماية ومعالجة البيانات والمعلومات" بينما لفظ "الكترونية" ينصرف إلى كافة الوسائط والأجهزة الإلكترونية التى يمكن أن يتم من خلالها أى من هذه العمليات والإجراءات التقنية. راجع: كتاب السيد المستشار/ نائب رئيس مجلس الدولة ورئيس قسم التشريع رقم (٢٤) بتاريخ ١٦ يناير ٢٠٢٠ المرفق بتقرير اللجنة المشتركة بشأن "مشروع قانون بإصدار قانون حماية البيانات الشخصية"، تعديل تعريف المعالجة، ص١٠٩ و ص ١٢٥.

٤٤ - كان قسم التشريع بمجلس الدولة قد أقترح ذلك حين عُرض عليه مشروع القانون، غير أن قطاع التشريع بوزارة العدل رفض هذا الاقتراح معللاً ذلك بأن تعريف المعالجة بتضمينه مصطلح إلكترونياً يعد تعريفاً متطابقاً مع تعريف المعالجة الإلكترونية الوارد بالقانون رقم (١٧٥) لعام ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الذى عرفها على أنها: "أى عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا لكتابة أو تجميع، أو تسجيل، أو حفظ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبال، أو تداول، أو نشر، أو محو، أو تغيير، أو تعديل، أو استرجاع، أو استنباط للبيانات والمعلومات الإلكترونية، وذلك باستخدام أى وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى". كما أضاف القطاع فى رده أن توحيد التعريفات الفنية هو أساس لصياغة التشريعات. راجع: كتاب السيد المستشار/ نائب رئيس مجلس الدولة ورئيس قسم التشريع رقم (٢٤) بتاريخ ١٦ يناير ٢٠٢٠ المشار إليه، ص١٠٩ و ص ١٢٥.

وفى المقابل تُعرف المادة ٤ من **اللائحة الأوروبية** لحماية البيانات "المعالجة Processing" بأنها: "أي عملية أو مجموعة من العمليات التي يتم إجراؤها على البيانات الشخصية أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أم لا، **مثل** التجميع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التكييف أو التغيير أو الاسترجاع أو التشاور أو الاستخدام أو الإفصاح عن طريق الإرسال أو النشر أو الإتاحة أو المحاذاة أو الدمج أو التقييد أو المحو أو التدمير".

ومن ثم فإن معالجة البيانات الشخصية، تشمل أية إجراءات متعلقة بالبيانات بغض النظر عن الطريقة التي استخدمت في هذا الإجراء، فأي إجراء يتم اتخاذه ويتعلق بالبيانات الشخصية يعتبر معالجة لهذه البيانات[٤٥].

وبمقارنة النص في التشريع المصري مع نظيره الأوروبي يظهر جلياً أن المشرع المصري ذكر العمليات التى تعد من قبيل المعالجة فى التعريف على سبيل الحصر، كما قصر عملية المعالجة على أي عمليات الكترونية أو تقنية تتم على البيانات، بينما أورد المشرع الأوروبي أن هذه العمليات وردت على سبيل المثال Such As، كما توسع فى وسيلة المعالجة أياً كان نوعها، إلكترونية أو غيرها.

وإن كان تعداد الأفعال التى تدخل فى نطاق المعالجة وفقا لتعريف المشرع المصري يكاد يبدو كافياً من الوهلة الأولى، وقد لا يتخيل وجود أفعال أو عمليات يمكن أن تقع على البيانات غير تلك الواردة فى التعريف إلا أنه ربما كان من الأفضل لو اقتدى المشرع المصري بنظيره الأوروبي فى هذا الشأن حتى يترك الباب مفتوحاً أمام استيعاب أى أفعال أخرى ربما تنشأ عن التطور المستمر فى التعامل مع البيانات باستخدام التكنولوجيا.

ويؤخذ على المشرع المصري عدم تعريفه للأفعال التى تدخل فى إطار المعالجة، فلم يحدد المقصود "بتجميع البيانات" أو "تسجيلها" أو "حفظها" أو "تخزينها وغير ذلك من الأفعال التى تناولها تعريف المعالجة، بينما تطرق المشرع الأوروبي إلى تعريف بعض العمليات دون غيرها، كما أضاف بعض المصطلحات التى ترتبط بالمعالجة وعرفها ووضح مدى خضوعها للائحة.

وقد أثير تساؤل فى ورشة العمل حول السبب فى خلو قانون حماية البيانات الشخصية المصري من تعريف لبعض المصطلحات المتعلقة بمفهوم المعالجة مثل مفهوم "الجمع" أو "تجميع البيانات".

45 - Sophie Pena Porta, Les Données personnelles et leur traitement, Art disponible sur www.pedagogie.ac-aix-marsille.fr, la date de mise en ligne est: 2 mars 2005.

وفى هذا الشأن أوضح البعض أن هذا الإغفال كان مقصوداً، وذلك لأن عمليات تجميع البيانات واسعة النطاق جداً ولا يمكن حصرها أو حتى ذكر أمثلة لها. كما يجب القاضى عند إثارة منازعة أمامه أن يستعين بخبراء فنيين للوقوف على مدى خضوع الفعل لمفهوم التجميع الخاضع لتنظيم القانون.

ب - المصطلحات الأخرى المرتبطة بمفهوم المعالجة:

يعد من قبيل الأفعال التى يمكن أن تختلط أو ترتبط بمفهوم معالجة البيانات والتى عرفتها التشريعات المنظمة لحماية البيانات الشخصية كل من مصطلح التنميط والتسمية المستعارة.

ويلاحظ أن المشرع المصري لم يتطرق لذكر أي من هذين المصطلحين على عكس نظيره الأوروبي فى إطار اللائحة العامة لحماية البيانات الشخصية.

فمن جهة أفرد المشرع الأوروبي تعريفًا خاصًا لما يطلق عليه "التنميط" (Profiling)، ويُقصد به، كما جاء فى المادة ٤ بند ٤ من اللائحة، أنه: " أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التى تتكون من استخدام البيانات الشخصية لتقييم جوانب شخصية معينة تتعلق بشخص طبيعي، وبخاصة لتحليل أو توقع الجوانب المتعلقة بأداء هذا الشخص الطبيعي فى العمل والوضع الاقتصادي والصحة والشخصية، التفضيلات أو الاهتمامات أو الموثوقية أو السلوك أو الموقع أو الحركات".

وأفردت اللائحة أيضاً تعريفاً لما قد يطلق عليه "نظام الإيداع" (Filing System) على عكس المشرع المصري الذى لم يفرد تعريفاً خاصاً بتلك العملية. ووفقاً للمادة الرابعة من اللائحة يقصد بنظام الإيداع: "أي مجموعة منظمة من البيانات الشخصية التي يمكن الوصول إليها وفقًا لمعايير محددة، سواء كانت مركزية أو لامركزية أو على أساس وظيفي أو جغرافي".

وعمليات المعالجة التى تعد من قبيل التنميط أو الإيداع وإن لم تكن مجرمة فى حد ذاتها إلا أنه لابد وأن تتبع الضوابط التى ترسمها التشريعات بخصوص معالجة البيانات.

وتدليلًا على أهمية هذه المصطلحات، نجد أن عدم التزام شركة Hennes & Mauritz (H&M) باتباع الإجراءات القانونية اللازمة عند إجراء عمليات المعالجة وتحديداً التنميط والإيداع قد كلفها مبالغ طائلة مؤخراً فى أكتوبر من عام (٢٠٢٠)، حيث فرض مفوض هامبورج لحماية البيانات الشخصية

وحرية المعلومات غرامة قدرها ٣٥,٣ مليون يورو على الشركة بسبب انتهاكاتها للبيانات الشخصية لموظفيها حيث جمعت الشركة واحتفظت بتسجيلات لموظفيها تحتوى بيانات على مستوى عال من الخصوصية ولفترات زمنية طويلة. كما تم استخدام تلك البيانات فى تقييم أداء العاملين وعمل ملفات تعريفية مفصلة لهم تستخدم وتؤثر فى اتخاذ قرارات تجاههم. والجدير بالذكر أن الموظفين لم تكن لديهم أدنى فكرة عن ذلك إلا حين حدث خطأ فنى فى أنظمة حواسيب الشركة مما جعل هذه البيانات متاحة لعدة ساعات فى أكتوبر من العام الماضي[٤٦].

ومن جهة أخرى أوردت اللائحة الأوروبية تعريفاً خاصاً **بالتسمية المستعارة** (Pseudonymisation) ليس بهدف خضوعها للحماية القانونية **إنما لتخرجها من نطاق البيانات الشخصية**، وعرفتها بأنها: "معالجة البيانات الشخصية بطريقة لا يمكن بعدها ربط البيانات الشخصية بشخص محدد هو موضوع تلك البيانات من دون استخدام معلومات إضافية، شريطة الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل وأن تكون تلك البيانات الإضافية خاضعة لتدابير تقنية وتنظيمية لضمان عدم انتسابها إلى شخص طبيعي معرف أو قابل للتعريف".

وعلى عكس التنميط والإيداع، باعتبارهما من قبيل معالجة البيانات الشخصية التى تشملها اللائحة بالحماية، نجد أن معالجة البيانات بطريقة التسمية المستعارة تخرج من نطاق حماية لائحة حماية البيانات (GDPR) لأنها لا تؤدي إلى التعريف بصاحب البيانات.[٤٧]

وجدير بالذكر أنه رغم وجود بعض الاختلافات بين تعريفات المعالجة التى أوردناها إلا أن كافة هذه التعاريف ما زالت بحاجة إلى توضيح وتفسير، ولذلك نتطرق لبعض تفسيرات قضاء المحكمة الأوروبية للمقصود بالمعالجة فى محاولة للوقوف على مدلول ذلك المصطلح وبالتالى الوقوف على نطاق حماية تلك التشريعات للبيانات الشخصية.

- تطبيقات تعريف المعالجة فى قضاء المحكمة الأوروبية:

تطرقت محكمة العدل الأوروبية فى العديد من أحكامها لتفسير مصطلح المعالجة وذكرت بعض الأعمال التى تعد من قبيل معالجة البيانات الشخصية، ولقد تطرقت لأول مرة لتفسير تعريف المعالجة عام ٢٠٠٣ فى قضيةLindqvist [٤٨] حين أوضحت أن نشر بيانات شخصية على صفحة إنترنت يعد من قبيل المعالجة التى تجعلها فى هذه الحالة مشمولة بالحماية التى تكفلها التوجيه الأوروبي رقم ٤٦/٩٥[٤٩].

كما أشارت المحكمة فى حكم لاحق إلى أن جمع البيانات الشخصية ونشرها ونقلها على قرص مضغوط عن طريق الرسائل النصية تعد كلها أشكالاً لمعالجة البيانات الشخصية بغض النظر عما اذا كانت البيانات التى تم نشرها قد تم تعديلها أم لا[٥٠].

وجدير بالملاحظة فى هذا الصدد أن المحكمة الأوروبية رفضت فى حكم حديث صادر عام ٢٠١٤ اعتبار التحليل القانونى الذى تقوم به جهة ما للرد على طلب تقدم به صاحب البيانات لها من قبيل البيانات الشخصية[٥١]، ولكنها رغم ذلك قررت أن ذلك لا يتعارض مع كون تسليم البيانات الشخصية قد تم استجابةً لطلب حصول على تلك البيانات مما يعد من قبيل أعمال المعالجة[٥٢].

كما صرحت المحكمة فى حكم شهير لها بأن أن تعديل أو تغيير (Alternation) البيانات الشخصية يعد فى حد ذاته من قبيل أعمال المعالجة، إلا أنه يمكن أن تنشأ عمليات معالجة أخرى للبيانات دون أن يتم تعديلها. كما أشارت المحكمة أن قدرة محرك البحث على "إتاحة" بيانات خاصة بتاريخ وتفاصيل البحث الذى قد يقوم به شخص، تعد من قبيل المعالجة كما هو الحال بالنسبة لكل العمليات السابقة على الإتاحة مثل قيام محرك البحث بجمع وتسجيل وتنظيم وتخزين تلك البيانات بصورة تلقائية ومستمرة وممنهجة[٥٣].

ولم تغفل المحكمة عن العمليات المتعلقة بأحدث التطورات التكنولوجية حين تطرقت لتفسير مصطلح المعالجة حيث تطرقت لعملية جمع وتخزين بصمات الأصابع وصنفتها على أنها تقع فى إطار المعالجة[٥٤].

46 - Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre; https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en Last Visited on the 19th of October 2020.

47 - GDPR, Recital (26): "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person"

48 - ECJ, Case C-101/01, 6th November 2003; [2003] ECR 1-12971), Found at: http://curia.europa.eu/juris/liste.jsf?num=C-101/01.

49 - The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies. Paragraph (24), (ECJ, Case C-101/01, 6th November 2003; [2003] ECR 1-12971).

50 - ECJ, Case C-73/07, 16th of December 2008, Tietosuojavaltuutettu [Finnish data protection ombudsman] v. Satakunnan Markkinaporssi Oy and Satamedia Oy, 16.12.2008 ("Tietosuojavaltuutettu").

51 - Joined Cases C-141/12 AND c372/12 YS v. Minister Voor Immigratie Integratie en Asiel and Minister Voor Immigratie, Integrate en Asiel V. M, S (2014).

52 - C-28/08, Commission V. Bavarian Lager CO., 29.6.2010 ("BAVARIAN LAGER").

53 - C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE"), Paragrapghs 26-31"

54 - C-291/12, Schwarz v. Bochum, 17.10.2014 ("Schwarz"), Para 28-29

٢- تعريف المتحكم والمعالج والحائز للبيانات (القائمين على عمليات المعالجة)

تضمن قانون حماية البيانات الشخصية تعريفات لكل من المعالج والمتحكم والحائز، وفى هذا يتفق إجمالاً مع التعريفات الواردة في اللائحة الأوروبية لحماية البيانات (GDPR).

وسوف نتناول فيما يلي تعريف كل من المتحكم والمعالج إضافة إلى خصوصية مفهوم الحائز في القانون المصري، وذلك على النحو التالى:

أ- تعريف المتحكم

عرف المشرع المصري "**المتحكم في البيانات**" فى المادة الأولى من القانون بأنه "أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول علي البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقًا للغرض المحدد أو نشاطه."

أما اللائحة الأوروبية فتعرف "**المتحكم** controller " بأنه: يعني الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تحدد، بمفردها أو بالاشتراك مع آخرين، أغراض ووسائل معالجة البيانات الشخصية؛ وعندما يتم تحديد أغراض ووسائل مثل هذه المعالجة بموجب قانون الاتحاد أو الدول الأعضاء، يجوز تحديد المتحكم أو المعايير المحددة لتحديده بموجب قانون الاتحاد أو قانون الدول الأعضاء" (م ٤ بند ٧).

ونرى أن المشرع المصري قد اتبع نهج المشرع الأوروبي في تحديد مفهوم المتحكم، حيث يعد المتحكم هو صانع القرار الرئيسي، ولديه السيطرة على عملية جمع البيانات وعلى وسائل وطريقة معالجتها.

وفي حالة **وجود أكثر من متحكم في البيانات** (المنظمات عادةً)، فيشكلوا وحدات تحكم مشتركة تتشارك المسئوليات والالتزامات القانونية كما تتشارك تحديد الهدف من جمع البيانات والتحكم فيها.

وقد أشارت اللائحة الأوروبية في المادة ٢٦ منها لمسألة **التحكم المشترك** "Joint Controllers" بقولها إن: "١- عندما يقوم اثنان أو أكثر من المتحكمين بشكل مشترك بتحديد أغراض ووسائل المعالجة، فيجب أن يكونا متحكمين مشتركين، وتحدد بطريقة شفافة مسئوليات كل منهما عن الامتثال للالتزامات بموجب هذه اللائحة، خاصة فيما يتعلق بممارسة حقوق صاحب البيانات وواجبات كل منهما فى تقديم المعلومات المشار إليها في المادتين ١٣ و ١٤، عن طريق الوسائل وبالترتيب بينهما ما لم يتم تحديد مسئوليات كل متحكم بموجب قانون الاتحاد أو قانون الدول الأعضاء الذي يخضع له المتحكمون، وقد يقوم الترتيب بتخصيص نقطة اتصال لأصحاب البيانات.

ويبدو أن القانون المصري قد تعرض أيضًا لفكرة التحكم المشترك في المادة ٤ (بند ١٢ فقرة ثانية) من قانون حماية البيانات الشخصية التى نصت على أن: "وفى **حال وجود أكثر من متحكم** يلتزم كل منهم بجميع الالتزامات المنصوص عليها فى هذا القانون، وللشخص المعنى ممارسة حقوقه تجاه كل متحكم على حدة".

ويتمثل معيار وجود تحكم مشترك فى تشارك كيانين أو أكثر في تحديد أغراض ووسائل عملية المعالجة، ويمكن أن يتجسد التحكم المشترك فى شكل قرار مشترك يتخذه كيانان أو أكثر أو ينتج عن قرارات متقاربة من قبل كيانين أو أكثر، حيث تكون القرارات مكملة لبعضها البعض وتكون ضرورية للمعالجة، بحيث تتم بطريقة يكون لها تأثير ملموس على تحديد أغراض ووسائل المعالجة. إضافة إلى ضرورة مشاركة كلا الطرفين فى المعالجة، وأن تشمل عملية التحكم المشترك على تحديد الأغراض من جهة وتحديد الوسائل من جهة أخرى[٥٥].

> وعلى خلاف اللائحة الأوروبية، التى تعرضت بإيجاز لوجوب تحديد المسئولية بين المتحكمين المشتركين، **لم يشر المشرع المصري لأي شروط خاصة بالتحكم المشترك ولم ينص على إمكانية تعيين نقطة اتصال لتسهيل الوصول للمتحكم بدلاً من وضع هذا العبء على الشخص المعنى البيانات.**

ويمكن تفسير هذا الاختلاف بين التشريعات بأن المشرع المصري قد وضع في قانون حماية البيانات ما يعتبره الحد الأدنى من الحماية المطلوبة وعليه فلا يسمح للأطراف بالاتفاق على تقسيم هذه الالتزامات أو نقل بعضها إلى شخص أخر، بل يجب أن يلتزم بها كل متحكم وذلك توفيرا لقدر أكبر من الحماية لصاحب البيانات الذي يستطيع الرجوع على أيهما لترتيب المسؤولية. ولكن لاتزال هناك اعتبارات عملية قد تثير إشكاليات في ظل غياب تنظيم ومعايير للتحكم المشترك. مثال ذلك تحديد مدى إمكانية أن يقرر أحد متحكمي البيانات إعادة استخدام البيانات لغرض جديد وهل توجد حاجة إلي أخذ موافقة المتحكم الآخر؟

ونخلص مما سبق إلى اتفاق القانون المصري مع اللائحة الأوروبية لحماية البيانات على أن المتحكم في البيانات هو الشخص الذي يحصل على البيانات بحسب طبيعة عمله وله الحق في تحديد طريقة وأسلوب الاحتفاظ بها ومعالجتها بشرط أن يكون ذلك في حدود الغرض المعلن والمحدد، الأمر الذي يحدده أيضاً المتحكم سواءً أكان متحكم واحد أو أكثر من متحكم مجتمعين.

55 - Guidelines 07/2020 on the concepts of controller and processor in the GDPRErpoian Data Protection Board Reoprt. 2020.

ب- تعريف المعالج

عرف القانون المصري (م١) "**معالج البيانات**" بأنه "أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقا لتعليماته".

ويلاحظ أن تقرير اللجنة المشتركة كان قد عدل هذا التعريف من مشروع القانون المقدم من الحكومة بحذف الجزء الذى يجعل الشخص المعالج للبيانات لصالحه معالج. فكان النص المقترح من قبل اللجنة كالآتي: " أي شخص طبيعي أو اعتباري يختص بطبيعة عمله بمعالجة البيانات الشخصية، لصالح المتحكم وبالاتفاق معه لتعليماته"[٥٦].

وترى الورشة أنه ربما كان من الأفضل لو جاء النص النهائى للمادة مماثلاً للنص المقترح من قبل اللجنة المشتركة وذلك لأنه لا داعي لذكر قابلية الشخص لمعالجة البيانات لصالح نفسه لأن ذلك يجعله متحكم.

بينما **تم تعريف المعالج**Processor **باللائحة الأوروبية** (م ٤ **بند** ٨) بأنه "يعني شخصًا طبيعيًا أو اعتباريًا أو سلطة عامة أو وكالة أو هيئة أخرى تعالج البيانات الشخصية نيابة عن المتحكم".

ويبدو من ذلك وجود قدر من الاختلاف الجزئي بين تعريف القانون المصري وتعريف اللائحة الأوروبية بشأن المعالج، حيث يجيز القانون المصري للمعالج بأن يقوم "**بعملية المعالجة**" لصالحه وليس لصالح المتحكم، بينما يحصره تعريف اللائحة الأوروبية فى قيامه بالمعالجة نيابة عن المتحكم. ويثور في هذا الشأن التساؤل حول مسئولية المعالج في حالة قيامه بعملية المعالجة لصالحه، وليس بناء على تعليمات المتحكم، وحول قصد المشرع المصري من إضافة إمكانية المعالجة لصالح المعالج.

وقد أوضحت مناقشات الورشة، أنه في حالة قيام المتحكم بالمعالجة لصالحه وليس لصالح المعالج، فإنه هنا يقوم بدور المعالج وليس المتحكم.

وبوجه عام، يتفق كل من القانون المصري واللائحة الأوروبية على تحديد علاقة المتحكم والمعالج من خلال تحديد من له سلطة اتخاذ القرار فيما يتعلق بمعالجة البيانات الشخصية، أي من له سلطة تحديد غرض وطريقة المعالجة[٥٧].

وبناءً على ما سبق فإنه يجب ألا يقوم المعالج بمعالجة البيانات خلافًا لتعليمات المتحكم، وللمتحكم السلطة المطلقة في تعيين أطر وأغراض المعالجة بما يسمح للمعالج باختيار أنسب الوسائل التقنية والتنظيمية لخدمة الغرض الأساسي الذي يتم تجميع البيانات من أجله. ومع ذلك ووفقاً لكل من القانون المصري واللائحة العامة لحماية البيانات لا يجوز للمعالج مخالفة تعليمات المتحكم[٥٨].

وفى محاولة لتوضيح الفرق بين المقصود بكل من المعالج والمتحكم، تعرضت ورشة العمل لذكر بعض الأمثلة التى توضح نطاق عمل كل منهما بشكل أفضل:

ففى حالة التعامل مع بيانات العملاء فى إطار تقديم خدمات الكهرباء، نجد أن مزود الخدمة بمقتضى عقد بينه وبين الشخص المعنى بالبيانات هو شركة الكهرباء والتى تعتبر فى هذه الحالة متحكمً بالبيانات، بينما نجد أن معالجة البيانات لاستخراج الفواتير لا يتم من قبل نفس الشركة فى مصر وإنما من قبل شركة أخرى، وتعد هذه الأخيرة فى تلك الحالة معالجًا للبيانات فقط دون أن تكون متحكمة بها.

وأشارت الورشة أيضاً إلى حالة معالجة بيانات شخصية فى إطار تقديم خدمات النقل الجوي، ففى هذا الشأن تقدم خدمة النقل الجوي شركة مصر للطيران وهى تحصل على البيانات الشخصية اللازمة لتقديم الخدمة وتتعامل معها بصفتها متحكم، بينما نجد أن عملية معالجة تلك البيانات لاستخراج تذاكر رحلات السفر يتم من قبل شركة أخرى (Amido) والتى تعتبر فى هذه الحالة معالجاً للبيانات.

ج - خصوصية مفهوم الحائز في القانون المصري

استحدث القانون المصري مصطلح "الحائز" فى قانون حماية البيانات، والذى لم تتطرق إليه اللائحة الأوروبية.

وقد أشارت الورشة إلى أن هدف المشرع من وراء استحداث الحائز هو معالجة ظاهرة انتشرت فى المجتمع المصري ألا وهى استخدام البيانات الشخصية للتسويق لسلع أو منتجات أو خدمات من قبل شخص يحوز بيانات شخصية لأخرين بغير وجه حق، ويطلق عليه أحياناً "مندوب مبيعات".

---

٥٦ – تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، مرجع سابق، ص ص ١٤ و٣٢.

57 - Rowenna Fielding, 'The Concept of Controller and Processor Data Entities' (2018).

٥٨ – يتشابه مفهوم "المتحكم Controller" وفقاً لقانون حماية البيانات الشخصية واللائحة العامة لحماية البيانات مع مفهوم "الشركة" أو "المؤسسة التجارية الذى ورد في قانون خصوصية المستهلك في كاليفورنيا، حيث إن كليهما له سلطة اتخاذ القرار فيما يتعلق بمعالجة البيانات الشخصية.

كما يحمل مفهوم "المعالج Processor " في قانون حماية البيانات الشخصية واللائحة العامة لحماية البيانات أوجه تشابه مع مصطلح "مقدمي الخدمات Service Provider" بموجب قانون خصوصية المستهلك في كاليفورنيا.

ولقد أكدت الجهة المعدة لمشروع القانون فى مذكرته الإيضاحية على ذلك بتوضيح أن وضع الحائز هو وضع قائم بالفعل وأنه سوف يتلاشى بعد فترة توفيق الأوضاع[٥٩].

ولقد عرف القانون المصري (م١) الحائز بأنه: "أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليا ببيانات شخصية في أي صورة من الصور، أو على أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة".

وجدير بالذكر أن مجلس الدولة كان قد علق على تعريف الحائز فى مشروع القانون مفضلاً ضبط صياغته بحذف عبارة "قانونياً أو فعلياً" وعلل ذلك بأن لفظ "يحتفظ" يشمل كافة أسباب حيازة البيانات الشخصية. كما أضاف مجلس الدولة أن حرف العطف (أو) يفيد المغايرة لغوياً بين كلاً من المعطوف والمعطوف عليه، وأن ذكر هذا الحرف بالتعريف يؤكد على أنه فى حالة احتفظ الشخص فعلياً بأي بيانات شخصية يعد من قبيل الحيازة غير المشروعة وفقاً لهذا التعريف مما يعد نتيجة غير منطقية لابد ألا يشملها مشروع هذا القانون[٦٠].

إلا أن رد قطاع التشريع بوزارة العدل جاء رافضًا لهذا المقترح وأجمعت اللجنة المعدة للمشروع على ضرورة الإشارة إلى كل من نوعي الحيازة، وذلك لإزالة أى غموض قد يلحق بالتعريف[٦١].

وإذا كان المشرع المصري قد انفرد بوضع تعريف خاص للحائز إلا أنه لم يفرض عليه أي التزامات خاصة به، بل اكتفى بالإشارة إليه في النصوص التي تنظم التزامات المتحكم والمعالج، ومع ذلك لم يخرج الحائز من إطار المحاسبة فنجد نصوصًا عقابية خاصة به في القانون، ومن هنا يثور التساؤل حول خصوصية مفهوم الحائز في القانون المصري، إذ لم نجد له مقابل في القوانين المقارنة وخاصة اللائحة الأوروبية، وتزداد المسألة صعوبة إذا بحثنا عن طبيعة العلاقة بين الحائز و المعالج وهل هناك تداخل بين مفهوم الحائز ومفهوم المعالجة حيث أن كلاهما يدخل في إطار تعريفه الاحتفاظ بالبيانات الشخصية؟

أسفرت المناقشات خلال ورشة العمل، **عن أن القانون لم يُلق على عاتق الحائز للبيانات الشخصية أية التزامات تذكر، وأن الحائز قد يكون أحد مندوبي التسويق أو المبيعات أو الشركات التي تعمل في هذا المجال حيث يمكن تداول مثل هذه البيانات بين العاملين في هذا المجال.**

وفى هذا الصدد أوصى البعض، إما بوضع التزامات واضحة على كاهل الحائز أو الاستغناء عن تعريفه ضمن قائمة التعريفات التي أوردها القانون.

٥٩ – كتاب السيد المستشار/ نائب رئيس مجلس الدولة ورئيس قسم التشريع رقم (٢٤) بتاريخ ١٦ يناير ٢٠٢٠ المرفق بتقرير اللجنة المشتركة بشأن "مشروع قانون بإصدار قانون حماية البيانات الشخصية"، تعديل تعريف الحائز، ص ١٠٨.

٦٠ – كتاب السيد المستشار/ نائب رئيس مجلس الدولة ورئيس قسم التشريع المشار إليه، تعديل تعريف الحائز، ص ١٠٨.

٦١ – مذكرة قطاع التشريع بوزارة العدل بتاريخ ٢١ فبراير ٢٠١٩ بالرد على ملاحظات قسم التشريع بمجلس الدولة رقم (٢٤) بتاريخ ١٦ يناير ٢٠٢٠ المرفقة بتقرير اللجنة المشتركة بشأن "مشروع قانون بإصدار قانون حماية البيانات الشخصية"، رأى القطاع على تعديل تعريف الحائز، ص ١٢٥.

المحور الثانى

حقوق الشخص المعنى
بالبيانات وشروط المعالجة

يعتبر الشخص الطبيعى الذى تتم جمع ومعالجة بياناته الشخصية أو ما يُعرف بصاحب البيانات أو "الشخص المعنى بالبيانات"، بحسب تعبير المشرع المصري، أحد الأطراف الأساسية فى عملية معالجة البيانات.

■ تعريف الشخص المعنى بالبيانات:

تكمن نقطة الانطلاق الأساسية فى بيان حقوق والتزامات هذا الشخص فى تعريفه على نحو يحدد ماهيته، ولهذا فقد عرفه القانون فى المادة الأولى منه بأنه: "**أي شخص طبيعى تُنسب إليه بيانات شخصية معالجة إلكترونياً تدل عليه قانوناً أو فعلاً، وتُمكن من تمييزه عن غيره**".

كما عرفت المادة ٤ من اللائحة الأوروبية "صاحب البيانات Data subject" بأنه "الشخص الطبيعي الذى يمكن التعرف عليه أو يمكن تحديده بشكل مباشر أو غير مباشر، وخاصة بالرجوع إلى رقم الهوية أو إلى عامل أو أكثر من العوامل المحددة لهويته البدنية أو الفسيولوجية أو العقلية أو الاقتصادية أو الاجتماعية"[٦٢].

ويستفاد من هذه المادة، وعلى غرار نطاق تطبيق القانون، فقد حصر المشرع المصري الشخص المعنى بالبيانات فى نطاق الشخص الطبيعي، منتهجاً طريق المشرع الأوروبي، ومن ثم يقتصر نطاق الحماية على الشخص الطبيعي فقط دون الشخص الاعتباري.

ويبدو من هذه التعريفات أن الشخص المعنى بالبيانات هو كل شخص طبيعي تكون بياناته الشخصية محلاً للجمع والمعالجة بناء على رضاء سليم غير مشوب بأي عيب من عيوب الإرادة.

ويمكن تقسيم البحث فى هذا المحور على النحو التالى:

أولاً: بيان حقوق الشخص المعنى بالبيانات

ثانياً: الجوانب الإجرائية لممارسة حقوق الشخص المعنى بالبيانات.

ثالثاً: شروط مشروعية جمع ومعالجة البيانات الشخصية

٦٢ - كما يُعرفه المشرع الفرنسى فى قانون المعلوماتية والحريات المعدل بأنه "كل شخص طبيعى تكون بياناته الشخصية موضوعاً للمعالجة (م ٢ من القانون).

أولاً

بيان حقوق الشخص المعنى بالبيانات

■ تعداد حقوق الشخص المعنى بالبيانات:

رسَّخ القانون حقوق الشخص المعنى بالبيانات فى المادة الثانية من القانون، التى يجري نصها على ما يلى: "ويكون للشخص المعنى بالبيانات الحقوق الآتية:

١- العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

٢- العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

٣- التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية.

٤- تخصيص المعالجة فى نطاق محدد.

٥- العلم والمعرفة بأى خرق أو انتهاك لبياناته الشخصية.

٦- الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات.

وباستثناء البند (٥) من الفقرة السابقة، يؤدى الشخص المعنى بالبيانات **مقابل تكلفة الخدمة المقدمة** إليه من المتحكم أو المعالج **فيما يخص ممارسته لحقوقه**، ويتولى المركز إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه".

ويتبين من هذه المادة أن المشرع عدَّد حقوق الشخص المعنى بالبيانات، مما يثير التساؤل حول إيرادها على سبيل الحصر أو أنها جاءت على سبيل المثال، مما يتيح المجال أمام وجود حقوق أخرى للشخص.

ولاشك أن ما ورد من حقوق فى القانون لا يخل بما للشخص من حقوق أخرى، وردت فى نصوص أخرى فى قانون حماية البيانات أو فى قوانين أخرى، مثل قانون حماية تقنية المعلومات أو قانون الأحوال المدنية.

وقد أوردت اللائحة الأوروبية GDPR حقوق صاحب البيانات Rights of the data subject فى الفصل الثالث منها (المواد من ١٢-٢٣).

وحقيقةً يجب التسليم بأن الاعتراف للشخص المعنى بالبيانات ببعض الحقوق على بياناته هو غاية أساسية يسعى لها القانون، هادفاً توفير حماية قانونية فعالة له باعتباره المقصود أساساً من هذه الحماية.

بيد أن المشرع المصري أورد أهم الحقوق التى يمكن منحها للشخص الطبيعي المعنى بالبيانات على بياناته الشخصية، ونتناولها فيما يلى:

١ - حق العلم بالبيانات الشخصية والاطلاع عليها والوصول إليها أو الحصول عليها

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

وفى الواقع ينطوي نص الفقرة الأولى من المادة الثالثة من القانون المصري على عدة صور لحقوق الشخص المعنى بالبيانات، هى:

أ- يكون للشخص الذى تم جمع ومعالجة بياناته **الحق فى العلم** ببياناته الموجودة لدى أى حائز أو متحكم أو معالج، ومن المسلم به أن العلم لغةً هو مصدر من الفعل عَلِمَ، وهو إدراك الشيء على حقيقته، أى إدراكه على ما هو عليه إدراكاً جازماً، كما أنه المعرفة واليقين، وهو نقيض الجهل.

بيد أن القانون لم يحدد صورة وآلية تحقق هذا العلم وعناصره، الذى يلبي هذا الاشتراط القانوني، فهل يكفى فيه مجرد الاطلاع أم يلزم الإخطار الكتابي؟

وتوحي صياغة النص "العلم بالبيانات.. الموجودة لدى المتحكم.." أن هذا الحق قاصر على مجرد تعرف الشخص على ما يوجد لدى المتحكم وغيره من بيانات شخصية خاصة به، دون غيرها من صور العلم، كأغراض المعالجة والجهات التى حصلت على البيانات وتحديد الفترة الزمنية التي سيتم خلالها تخزين البيانات الشخصية.

تُوصي الورشة: بأن تحدد اللائحة التنفيذية ضوابط تحقق علم الشخص ببياناته وعناصر هذا العلم، واعتبارها فى الوقت نفسه التزامات على عاتق المتحكم أو الحائز أو المعالج.

ب- حق الشخص المعنى بالبيانات فى **الاطلاع علي بياناته والوصول إليها**: ويقتضي هذا الحق تمكين هذا الشخص أو ورثته أو من ينوب عنه قانوناً من الاطلاع على جميع بياناته موضوع المعالجة، ولا يجوز التنازل عن هذا الحق أو الحد منه إلا فى حدود القانون.

وقد يثور التساؤل حو دقة الصياغة اللفظية فى هذا الصدد، حيث يشير النص لحق الاطلاع على البيانات وأيضاً حق الوصول للبيانات، رغم أن الأول يفيد الثانى فالاطلاع يأتى بطبيعة الحال لاحقاً للوصول للبيانات، فضلاً عن أن حق العلم بالبيانات، لفظ شامل، يتضمن بين طياته الاطلاع والوصول، إذ كيف يتسنى للشخص العلم بالشىء إلا من طريق الوصول إليه والاطلاع عليه.

ويرتبط حق الوصول والاطلاع على البيانات بالحق فى الحصول عليها، كما عبر عن ذلك النص، ويقصد من ذلك حق الشخص فى الحصول على نسخة من بياناته بلغة واضحة ومطابقة لما هو موجود لدى المتحكم وغيره، بناء على طلبه، وفقاً للإجراءات المقررة، ودفع المقابل المالى لهذه الخدمة.

تُوصي الورشة: بأن تتضمن اللائحة التنفيذية ضوابط ممارسة هذا الحق، على غرار ما فعل المشرع الأوروبي

٢ - حق العدول عن الموافقة على الاحتفاظ بالبيانات أو معالجتها :

يشترط القانون، فى مادته الثانية، ضرورة صدور موافقة صريحة من الشخص المعنى بالبيانات على عمليات جمع البيانات أو معالجتها، إلا في الأحوال المصرح بها قانوناً، ومن ثم فمن الطبيعي أن يكون للشخص العدول عن هذه الموافقة، أي سحب موافقته فى أي وقت، لتعلقها بحقوقه اللصيقة بشخصيته، فقد تطرأ أمور خاصة لدى الشخص تستدعي عدم الاحتفاظ بالبيانات أو معالجتها.

ويصدر طلب العدول من الشخص أو من كل ذي صفة قانونية (كالورثة أو من ينوب عنه) ويوجه للمتحكم أو المعالج أو الحائز، ويجب عليه أن يبت فيه، خلال فترة معقولة، ويترتب على هذا العدول عدم جواز قيام المتحكم أو المعالج بالاحتفاظ بالبيانات أو معالجتها.

وقد أقرت اللائحة الأوروبية الحق فى سحب الموافقة The right to withdraw of consent فى الفقرة الثالثة من المادة ٧ منها، فأجازت لصاحب البيانات سحب موافقته في أي وقت. بيد أن سحب الموافقة لا يؤثر على مشروعية المعالجة التى جرت بناءً على الموافقة السابقة على سحبها، على أنه يجب إبلاغ صاحب البيانات بذلك قبل إبداء الموافقة، ويجب تيسير عملية سحب الموافقة.

تُوصى الورشة: أن تتضمن اللائحة التنفيذية شروط ومحددات ممارسة حق الشخص فى العدول عن الموافقة.

٣ - الحق فى تصحيح أو تعديل أو محو البيانات الشخصية:

يتضمن هذا الحق صور متعددة، فيشمل التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية.

وجدير بالملاحظة أن صياغة هذه الكلمات تنطوي على تكرار لا داعي له، فالتصحيح أو الإضافة أو التحديث هى مسائل فى حد ذاته تندرج تحت وصف التعديل، فهناك تعديل بالإضافة أو الحذف أو التصحيح أو التحديث.

أ- **الحق فى التصحيح**: يكون للشخص المعنى بالبيانات، أو كل ذي صفة، الحق فى طلب تصحيحها إذا ما شاب البيانات أخطاء أثناء جمعها ومعالجتها.

كما يكون له التعديل على هذه البيانات سواء بالإضافة أو التحديث إلى هذه البيانات إذا كان يشوبها نقص أو تغييرها متى كانت غير دقيقة أو غير صحيحة أو مضللة أو غامضة.

وقد نصت المادة ١٦ من اللائحة الأوروبية على الحق فى التصحيح Right to rectification، بقولها أنه يكون لصاحب البيانات الحق فى الحصول من المتحكم دون تأخير غير مبرر على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به، ومع مراعاة أغراض المعالجة، يجب أن يكون له الحق فى استكمال البيانات الشخصية الناقصة، بوسائل منها تقديم بيان إضافي.

ب - **الحق فى المحو (الحق فى النسيان** Right to be forgotten):

تتسم شبكة الانترنت، وما يرتبط بها من خوادم ضخمة تخضع لسيطرة شركات عملاقة، بشراهتها لجمع وتخزين المعلومات، وذاكرتها المطلقة التى لا يمكن محو ما يختزن فيها بسهولة من قبل المستخدمين، وهو أمر جعل النسيان الطبيعي

أمراً صعب المنال فى الوقت الحاضر، فهى تُحصي على مستخدميها أنشطتهم سواء كانت فى شكل تعليقات أو أخبار خاصة أو صور أو معلومات شخصية، وتجمع وتسجل بياناتهم ومعلوماتهم وتخزنها وتحتفظ بها لمدة غير محدودة، مع إتاحة هذه البيانات والمعلومات من أي مكان فى العالم ولكل من يريد وفى الوقت الذى يحلو له، مع العلم أن هذه البيانات والمعلومات قد تكون قديمة أو مغلوطة أو غير صحيحة، ومع هذا تظل متاحة للجميع وعلى الدوام إلى ما لا نهاية.

ومن شأن هذه المخاطر أن تسبب للشخص المعنى بالبيانات أضراراً بالغة الخطورة وتشكل تهديداً صريحاً للخصوصية، وحقهم فى محو البيانات الخاصة بهم مع على الانترنت، وهو ما دعا الفكر القانوني إلى البحث عن حلول لهذه المشكلة لحماية خصوصية الأشخاص، ووجد ضالته فى مفهوم "الحق فى النسيان" فى البيئة الرقمية، باعتباره أحد الحقوق المرتبطة بحرمة الحياة الخاصة للإنسان.

ولهذا نص المشرع المصري (م٢ من القانون) على حق الشخص المعنى بالبيانات فى محو بياناته الشخصية، ويُطلق على الحق فى المحو تسمية "الحق فى النسيان" أو الحق فى الدخول فى طي النسيان، أو الحق فى النسيان الرقمي[٦٣].

ويقصد بهذا الحق أن لكل شخص الحق في حذف البيانات الشخصية المحفوظة لدى المعالج أو المتحكم أو الحائز نهائياً عند إلغاء أو مغادرة الخدمة أو التطبيق، وعدم الاحتفاظ بنسخ منها لأى سبب كان، بما يتضمنه ذلك من إزالة الروابط التي تؤدي إلى معلومات عنه على الانترنت (محركات البحث، مواقع إلكترونية، مواقع التواصل الاجتماعي...)، كما يعنى أيضاً التزام المسئولون عن معالجة البيانات الشخصية أو حفظها بعدم حفظ تلك البيانات لمدة تتجاوز الغاية التي جمعت من أجلها[٦٤].

وقد حظى هذا الحق باهتمام بالغ فى أوروبا، وخاصة بعد صدور حكم محكمة العدل الأوروبية رقم C-131/12 الصادر بتاريخ ١٣ مايو ٢٠١٤ ضد محرك البحث "Google"[٦٥]، الذى أوصى المشرع الأوروبي بضرورة وضع ضمانات لحماية هذا الحق، وقد استجاب المشرع لذلك حيث اعترف صراحة بهذا الحق فى المادة ١٧ من اللائحة الأوروبية لحماية البيانات، حيث تنص فى الفقرة الأولى على أن يكون لصاحب البيانات الحق فى أن يحصل من المتحكم على محو البيانات الشخصية المتعلقة به دون تأخير لا مبرر له، ويجب على المتحكم أن يحذف البيانات الشخصية دون تأخير.

وبناءً على ذلك تمكن المستخدم الأوروبي من مطالبة شركات الانترنت بحقه في محو بياناته الشخصية واحترام حقه في الدخول في طي النسيان الرقمي[٦٦].

■ أسباب تطبيق الحق فى النسيان:

لم يحدد المشرع المصري الحالات التى ينطبق فيها الحق فى المحو Right to erasure أو ما يطلق عليه الحق فى النسيان Right to be forgotten، وهو ما تحوط له المشرع الأوروبي فى اللائحة الأوروبية، حيث تضمنت المادة ١٧ منه أحكام واضحة لتنظيم هذا الحق، واشترطت لتطبيق الحق فى النسيان ضرورة توافر أحد الأسباب التالية:

– لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها من أجلها؛

– قيام صاحب البيانات بسحب الموافقة التي تستند إليها المعالجة وفقًا للفقرة الأولى من المادة ٦، أو الفقرة الأولى من المادة ٩، وحيث لا يوجد أساس قانوني آخر للمعالجة؛

– اعتراض صاحب البيانات على المعالجة وفقًا للمادة ١/٢١ ولا توجد أسباب مشروعة تبرر المعالجة، أو اعتراضه على المعالجة وفقاً للمادة ٢/٢١؛

– إذا جرى معالجة البيانات الشخصية بشكل غير قانونى؛

٦٣ – لمزيد من التفصيل فى شأن هذا الحق، راجع: د. عبد الهادى فوزى العوضى: الحق فى الدخول فى طى النسيان على شبكة الانترنت، دار النهضة العربية، الطبعة الأولى، ٢٠١٤. وأيضاً:

Maxime BESÈME :Le droit à l'oubli numérique dans le droit de l'Union européne, Consécration prétorienne et legislative ,Mémoire UCL) Université catholique de Louvain ,(2015-2016 .Disponiple sur Internet :https//:dial.uclouvain.be/memoire/ucl/en/object/thesis:7609/datastream/PDF_01/view

٦٤ – عرفت اللجنة الوطنية للمعلوماتية فى فرنسا، الحق فى النسيان الرقمى، بأنه الحق الذى يخول صاحبه مكنة السيطرة من حيث الزمان على بياناته الشخصية، بغية الحصول على حذفها أو محوها عندما يرغب فى ذلك".

٦٥ – صدر حكم محكمة العدل التابعة للاتحاد الأوروبي رقم C-131/12 في ١٣ مايو (آيار) ٢٠١٤، بشأن قضية اشتهرت بقضية ماريو كوستيغا ضد محرك البحث جوجل Google أسبانيا وجوجل الرئيسى الكائن فى الولايات المتحدة الأمريكي، حيث قضت المحكمة بحق مستخدمى الانترنت في مطالبة محركات البحث مثل Google بإزالة نتائج طلبات البحث التى تتعلق بالبيانات الشخصية، متى كانت الروابط المعنية "غير كافية أو غير ذات صلة أو لم تعد ذات صلة بموضوع البحث أو مبالغًا فيها"، حتى ولو كان المحتوى صحيحاً ومنشوراً بشكل قانونى طالما رغب الشخص فى نسيانها. وقد استندت المحكمة فى قرارها إلى الأحكام الواردة فى التوجيه الأوروبى رقم ٤٦/٩٥ بشأن حماية معالجة البيانات الشخصية ونقلها، وأيضاً الاتفاقية الأوروبية لحقوق الانسان الصادرة عام ١٩٥٠. لمزيد من التفصيل راجع: الصالحين محمد العيش، تعليق حول حكم محكمة العدل الأوروبية الصادر في ١٣ مايو ٢٠١٤ بشأن الحق في اعتبار بعض الوقائع في طي النسيان، بحث منشور بمجلة معهد دبي القضائى، العدد ٥، ٣ فبراير ٢٠١٥، ص١٦٩ وما بعدها؛ د. معاذ سليمان الملا: فكرة الحق فى الدخول فى طي النسيان الرقمي فى التشريعات الجزائية الإلكترونية الحديثة دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس، ٩ – ١٠ مايو ٢٠١٨، ملحق خاص، العدد ٣، الجزء الأول، مايو ٢٠١٨م، ص ١١٧ وما بعدها.

٦٦ – يُشار فى هذا الصدد، إلى قيام شركة Google بتضمين سياستها لتقرير الشفافية إعلان المستخدمين لمحركها بتأثير قانون الخصوصية الأوروبي في نتائج بحث Google، وبيان "طلبات حذف المحتوى بموجب قانون الخصوصية الأوروبى"، وطلبات إزالة عناوين URL من بحث Google للحفاظ على الخصوصية، وذلك على موقعها التالى:

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

– يجب محو البيانات الشخصية للوفاء بالتزام قانوني في قانون الاتحاد الأوروبي أو الدول الأعضاء يخضع له المتحكم؛

– تم جمع البيانات الشخصية بخصوص عرض خدمات مجتمع المعلومات المشار إليها في المادة ١/٨.

وفي حالة قيام المتحكم بإتاحة البيانات الشخصية للجمهور، وكان ملزماً بمحو البيانات الشخصية، يجب عليه، مع مراعاة التكنولوجيا المتاحة وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير التقنية، لإبلاغ المتحكمين في معالجة البيانات الشخصية بأن صاحب البيانات قد طلب محو أي روابط لديهم أو نُسخ لهذه البيانات الشخصية (المادة ١٧ فقرة ثانية من اللائحة الأوروبية).

■ مجالات تطبيق الحق فى النسيان:

ينحصر مجال تطبيق الحق فى النسيان فى البيئة الرقمية فيما يتعلق بالآثار الإلكترونية أو الذكريات الرقمية، وهى كل البيانات والمعلومات المتعلقة بالشخص ونشاطه خلال استخدامه لنشاط معلوماتي أو وسيلة الكترونية أياً كان نوعها (مواقع شبكات التواصل الاجتماعي - محركات بحث - مدونات - مواقع التجارة الالكترونية.. وغيرها) يكون من شأنها أن تساهم فى تحديد هويته الرقمية، كما يعتبر من الآثار الرقمية أراء الشخص ومساهماته على الانترنت مهما كان نوعها.

وحديثاً، قضت محكمة العدل الأوروبية، بتاريخ ٢٤ سبتمبر ٢٠١٩، بأنه إذا كان يتوجب على شركة "Google" سحب روابط بطلب من هيئة تنظيمية أو محكمة في دولة بالاتحاد الأوروبي من جميع نسخ مواقعها الأوروبية، إلا أن "الحق في النسيان" عبر الإنترنت يتوقف عند هذا الحد، ومن ثم فهى غير مطالبة بتطبيق هذا الحق على محركات البحث التابعة لها خارج أوروبا.

وأشارت المحكمة إلى أن قانون الاتحاد الأوروبي لا يشترط على مشغلي محركات البحث على غرار Google القيام بعملية سحب روابط كهذه في جميع نسخ محرك البحث التابع لها.

لكنها شددت على أن سحب الروابط من المواقع الأوروبية يجب أن يتضمن إجراءات "تثني جدياً" مستخدم الإنترنت الأوروبي عن التمكن من الالتفاف على "حق النسيان" من خلال الوصول إلى نتائج لا قيود عليها عبر محرك بحث في نطاق خارج الاتحاد الأوروبي، ويتطلب ذلك فرض "حجب جغرافي"، وهو أمر تشير جوجل إلى أنها تطبقه بفعالية في أوروبا.

تُوصي الورشة: بتعديل القانون للنص على تحديد مدة معينة يتعين تصحيح البيانات خلالها أو حذفها على غرار ما فعلت بعض التشريعات[٦٧].

٦٧ – حدد القانون المغربى بشان حماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصى، فى المادة ١/٨ منه هذه المدة بعشرة أيام.

تُوصي الورشة بأن: تتضمن اللائحة التنفيذية شروط وضوابط ممارسة هذه الحقوق (الحق فى التصحيح - الحق فى التعديل – الحق فى المحو "أو النسيان")، تحديداً دقيقاً.

٤ – الحق فى تخصيص المعالجة فى نطاق محدد (تقييد المعالجة):

يجيز القانون للشخص المعنى بالبيانات تحديد نطاق المعالجة أى تقييدها (م ٢)، وقد نصت اللائحة الأوروبية على هذا الحق فى المدة ١٨ منها.

ولكن المشرع المصري لم يحدد ضوابط وشروط هذا التقييد، وهو ما راعته اللائحة الأوروبية، ونفذته فعلياً الشركات والكيانات التى تخضع لنطاق تطبيقها، حيث يجوز للشخص طلب تقييد معالجة بياناته الشخصية وفقًا للشروط التالية:

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

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

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

– إذا اعترض الشخص على المعالجة وفقا للمادة ٢١ الفقرة ١ من اللائحة الأوروبية، ولم يتم بعد تحديد ما إذا كانت الأسباب المشروعة للشخص المسئول تفوق أسباب الشخص المعنى بالبيانات.

في حالة تقييد معالجة البيانات الشخصية المتعلقة بالشخص المعنى بالبيانات، لا يجوز استخدام هذه البيانات إلا بموافقته (باستثناء تخزين البيانات) لغرض تأكيد أو إقامة دعاوى قانونية، أو الدفاع فيها أو حماية حقوق شخص طبيعي أو اعتباري آخر أو لأسباب المصلحة العامة الهامة للاتحاد الأوروبي أو الدولة العضو.

إذا تم تقييد المعالجة وفقًا للشروط المذكورة أعلاه، فسيقوم الشخص المسؤول بإبلاغ الشخص المعنى قبل رفع هذا التقييد.

تُوصي الورشة: بأهمية أن تولي اللائحة التنفيذية فى اعتبارها ضوابط ممارسة الحق فى تقييد المعالجة، على غرار اللائحة الأوروبية .

٥ – الحق فى معرفة أى خرق أو انتهاك للبيانات الشخصية:

تشير المادة الثانية من القانون إلى حق الشخص فى العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

وهذا الحق يعد من البديهيات، فمن الطبيعي إلزام المتحكم أو المعالج بإخطار الشخص المعنى بما قد يطرأ على هذه البيانات، وما يحدث لها من اعتداءات، بأي شكل أو وسيلة كانت.

ويفيد التعرف على الاعتداد على البيانات فى تدبر الشخص المعنى بالبيانات لأموره واتخاذ قراره الذى يحقق مصلحته، فقد يسحب موافقته أو يطلب تعديل أو تصحيح البيانات متى حدث لها أى تشويه أو يطلب حذف البيانات كلية.

■ التزام المتحكم والمعالج بإخطار المركز بأي خرق أو انتهاك للبيانات:

وفقاً للمادة ٧ من القانون يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ مركز حماية البيانات الشخصية خلال ٧٢ ساعة، وفى حال كان هذا الخرق أو الانتهاك متعلقاً باعتبارات حماية الأمن القومى فيكون الإبلاغ فورياً، وعلى المركز وفى جميع الأحوال إخطار جهات الأمن القومي بالواقعة فوراً، كما يلتزم بموافاة المركز خلال ٧٢ ساعة من تاريخ علمه بما يأتى:

١ - وصف 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.

وفى جميع الأحوال يجب على المتحكم أو المعالج، بحسب الأحوال، إخطار الشخص المعنى بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ بما تم اتخاذه من إجراءات. وتُحدد اللائحة التنفيذية لهذا القانون الإجراءات الخاصة بالإبلاغ والإخطار.

تُوصي الورشة: بأن تتضمن اللائحة التنفيذية ضوابط ممارسة حق الشخص المعنى بالبيانات فى معرفة أي خرق أو انتهاك للبيانات، على نسق المشرع الأوروبي

٦ – الحق فى الاعتراض على معالجة البيانات الشخصية:

تشير المادة الثانية من القانون إلى حق الشخص المعنى بالبيانات فى الاعتراض على معالجة البيانات أو نتائجها متى تعارضت مع حقوقه وحرياته الأساسية.

ووفقاً للمادة ٢١ من اللائحة الأوروبية لحماية البيانات يحق للشخص في أي وقت الاعتراض على معالجة بياناته الشخصية Right to object وفقًا للفقرة الأولى من المادة (٦) البند (هـ) أو (و) من اللائحة وذلك للأسباب التي تنشأ من وضعه الخاص؛ وهذا ينطبق أيضًا على إعداد الملفات الشخصية على أساس هذه الأحكام. ومن هنا لا يجوز للشخص المسئول بعد ذلك أن يقوم بمعالجة البيانات الشخصية المتعلقة بصاحب البيانات ما لم يتمكن من إثبات أسباب مشروعة مقنعة للمعالجة تفوق مصالحه وحقوقه وحرياته، أو أن المعالجة تهدف إلى فرض إقامة دعاوى قانونية أو الدفاع فيها.

وإذا ما جرت معالجة البيانات الشخصية المتعلقة بصاحب البيانات لأغراض التسويق المباشر، فلديه الحق في الاعتراض في أي وقت على معالجة بياناته الشخصية لأغراض هذا الإعلان؛ وهذا ينطبق أيضًا على إعداد الملفات الشخصية طالما أنه مرتبط بهذا البريد المباشر. وإذا اعترض صاحب البيانات على المعالجة لأغراض التسويق المباشر، فلا يجوز بعدها معالجة بياناته الشخصية لهذه الأغراض (م٢١/٢، ٣ من اللائحة).

وبغض النظر عن توجيهات 2002/58/EC، يكون للشخص المعنى بالبيانات الخيار، في سياق استخدام خدمات مجتمع المعلومات، في ممارسة حقه في الاعتراض من خلال الإجراءات الآلية التي تستخدم المواصفات الفنية (م ٢١/ ٥ من اللائحة).

وعندما تتم معالجة البيانات الشخصية لأغراض بحثية أو تاريخية أو أغراض إحصائية، وفقاً للمادة ٨٩/١، يكون لصاحب البيانات، لأسباب تتعلق بوضعه الخاص، الحق فى الاعتراض على معالجة بياناته الشخصية، ما لم تكن المعالجة ضرورية لأداء مهمة يجرى تنفيذها لأغراض المصلحة العامة (م٢١/ ٦ من اللائحة).

تُوصي الورشة: أن تبين اللائحة التنفيذية ضوابط ممارسة حق الشخص المعنى بالبيانات فى الاعتراض على المعالجة، على غرار ما فعل المشرع الأوروبي.

٧ – الحق في إمكانية نقل البيانات:

أغفل المشرع المصري النص على حق الشخص المعنى بالبيانات فى نقل البيانات الشخصية الخاصة به، رغم أنه من الحقوق المهمة.

ولم يفت المشرع الأوروبي النص على هذا الحق فى إمكانية نقل البيانات Right to data portability فى اللائحة الأوروبية حيث تضمنها نص المادة ٢٠ منها، الذى يجرى على أن يكون للشخص المعنى بالبيانات الحق في تلقي بياناته الشخصية التي قدمها إلى الشخص المسئول بتنسيق منظم ومعروف ويمكن قراءته آليًا. وبالإضافة إلى ذلك، لديك الحق في نقل هذه البيانات إلى شخص آخر مسؤول عنها دون عائق من قبل الشخص المسؤول عن توفير البيانات الشخصية، شريطة أن:

– تعتمد المعالجة على الموافقة على النحو الوارد فى المادة ٦ الفقرة ١ البند (أ) من اللائحة أو المادة ٩ الفقرة ٢ البند (أ) من اللائحة أو بعقد وفقًا للمادة ٦ الفقرة ١ البند (ب) من اللائحة.

– تتم المعالجة بوسائل آلية.

وبممارسة هذا الحق، يكون لصاحب البيانات أيضًا الحق في التحقق من إرسال بياناته الشخصية مباشرةً من شخص إلى آخر، طالما أن ذلك ممكن من الناحية التقنية. ولا يجوز أن تتأثر الحريات وحقوق الأشخاص الآخرين.

ولا ينطبق الحق في نقل البيانات على معالجة البيانات الشخصية اللازمة لأداء مهمة لأغراض المصلحة العامة أو في ممارسة السلطة الرسمية المفوضة للشخص المسئول.

تُوصي الورشة: بتعديل القانون للنص على الحق فى نقل البيانات (على غرار ما فعل المشرع الأوروبي)، باعتبار أن القانون هو الذى ينشأ الحق ويحميه، ولا يجوز للائحة تُوضع من قبل السلطة التنفيذية (وزير الاتصالات) أن تنشئ الحقوق.

■ **خلاصة ما سبق:**

يبدو مما تقدم أن المشرع المصري اكتفى بمجرد تعداد وحصر حقوق الشخص المعنى بالبيانات دون الدخول فى تفصيلاتها وابتعد عن تحديد ضوابط إنفاذ هذه الحقوق، رغم أن اللائحة الأوروبية تتضمن تفصيلات دقيقة لضوابط ومحددات هذه الحقوق، ولم تكتف بمجرد النص عليها.

لهذا تُوصي الورشة: بأن تتضمن اللائحة التنفيذية شروط وضوابط ممارسة حقوق الشخص المعنى بالبيانات، على غرار مسلك اللائحة الأوروبية.

ثانياً

الجوانب الإجرائية لممارسة حقوق الشخص المعنى بالبيانات

١ – وفاء الشخص المعنى بالبيانات بمقابل تكلفة استفادته من الخدمات المتعلقة بممارسة حقوقه:

فى لفتة غير منطقية، وتتعارض مع الأصول القانونية المستقرة لممارسة الحق، ألزم المشرع، فى الفقرة الثالثة من المادة الثانية، الشخص المعنى بالبيانات، بأداء مقابل مالي للمتحكم أو المعالج عند حصوله على خدمات تتعلق بممارسته للحقوق التى خولها له القانون.

ويثير ذلك الدهشة، كيف يمنح القانون الحق للشخص الطبيعي من ناحية، ويكبله من ناحية أخرى بدفع مقابل مالي عند ممارسة كل حق على حدة؟ على الرغم من أن الخدمات التى يقدمها المتحكم فى هذا المجال لا تخرج عن كونها خدمات إدارية لا تتكلف مبالغ تذكر، كما أنها تدخل فى صميم عمل المتحكم أو المعالج.

وتشمل الحقوق التى تخضع للوفاء بمقابل مالي للمتحكم أو المعالج كافة الحقوق المتقدم ذكرها (العلم بالبيانات - العدول عن الموافقة - التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات - تقييد المعالجة – الاعتراض على المعالجة).

واستثنى المشرع فقط من دفع هذا المقابل حالة العلم والمعرفة بأي خرق أو اعتداء على البيانات الشخصية.

ويتولى مركز حماية البيانات الشخصية إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه.

ولا شك أن إلقاء هذا العبء المالي على عاتق الشخص الطبيعى قد يتعارض مع حقه الطبيعي فى ممارسة الحقوق التى يخولها القانون، وخاصة فى حالة إذا ما كان يرغب فى ممارسة أكثر من حق، ومن ثم سيكون مضطراً للوفاء بمقابل مالي لكل خدمة على حدة.

وعلى النقيض من ذلك راعت اللائحة الأوروبية مصالح الشخص المعنى بالبيانات وأتاحت له ممارسة جميع الحقوق

المذكورة مجاناً، بلا أي مقابل، وهو ما يعزز من فرص حماية البيانات الشخصية[٦٨].

وقد ناقشت الورشة هذه المسألة وتفاوت فيها أراء المشاركين، فاتجه البعض (رأي واحد) إلى أن هذه المقابل ضرورة حتى لا يحدث إفراط في ممارسة الحقوق وتضخم الطلبات على المعالج أو المتحكم.

بينما اتجه الرأي الغالب إلى التوصية بتعديل القانون لإلغاء مقابل ممارسة الحقوق وأن يكون ذلك بصورة مجانية، كما فعلت بعض التشريعات.

وتحوطاً، لحين تعديل القانون، يُراعى أن يكون هذا المقابل رمزياً حتى لا يرهق الشخص المعنى البيانات، وقد تحدد اللائحة التنفيذية ضوابط تحديد هذا المقابل.

٢ - الالتزام بالإخطار فى شأن تصحيح أو محو البيانات الشخصية أو تقييد المعالجة:

لم يتضمن القانون أي التزام على المعالج والمتحكم بالإخطار فى حالة **تصحيح أو محو البيانات الشخصية أو تقييد المعالجة**، واكتفى بالنص على الالتزام بالإخطار فى حالة خرق أو انتهاك للبيانات الشخصية لديه، وفقاً للمادة ٧ من القانون، على نحو ما أشرنا.

وفى المقابل نظمت المادة ١٩ من اللائحة الأوروبية الالتزام بالإخطار فيما يتعلق بتصحيح أو محو البيانات الشخصية أو تقييد المعالجة Notification obligation regarding rectification or erasure of personal data or restriction of processing، التى تلزم المتحكم بإخطار كل متلق للبيانات تم الكشف عن البيانات الشخصية له، عن أي تصحيح أو محو للبيانات الشخصية أو تقييد المعالجة، ما لم يتبين أن ذلك مستحيل أو أنه يقتضى جهود لا تناسب قدراته. ويجب على المتحكم إخطار صاحب البيانات عن هؤلاء المتلقين متى طلب ذلك.

٣ - تقديم الطلبات والشكاوى فما يتعلق بممارسة الحقوق:

(أ) **الطلبات**: يجوز للشخص المعنى بالبيانات ولكل ذي صفة أن يتقدم إلى حائز أو متحكم أو معالج بطلب يتعلق بممارسة حقوقه المنصوص عليها فى هذا القانون، مثل تعديل البيانات أو حذفها، وفى هذه الحالة يلتزم المقدم إليه الطلب بالرد عليه خلال ستة أيام عمل من تاريخ تقديمه إليه (م٣٢ من القانون)

(ب) **الشكاوى**:

قد يحدث أن يرفض المعالج أو المتحكم تمكين الشخص المعنى بالبيانات أو كل ذي صفة من استيفاء حقوقه المشار إليها، ومن ذلك رفض تمكينه من الاطلاع على البيانات أو الوصول إليها أو عدم تسليمه نسخة من البيانات أو تأجيل طلبه بالاطلاع أو الوصول أو الحصول على البيانات، وفى هذه الحالة يجوز للشخص ولكل ذي صفة ومصلحة مباشرة حق الشكوى للجهة المختصة، وهى مركز حماية البيانات الشخصية، وفقاً لنص المادة ٣٣ من القانون، ويكون للمركز عقب تقديم الشكوى اتخاذ ما يلزم من إجراءات التحقيق، وعليه أن يصدر قراره بنتيجة الفحص خلال ثلاثين يوم عمل من تاريخ تقديمها، على أن يُخطر الشاكي والمشكو فى حقه بالقرار المتخذ فى هذا الشأن، ويلتزم المشكو فى حقه بتنفيذ قرار المركز خلال سبعة أيام عمل من تاريخ إخطاره به، وإفادة المركز بما تم نحو تنفيذه. ويلاحظ أن لجوء الشخص المعنى للبيانات للشكوى لمركز حماية البيانات لا يخل بحقه الدستوري فى اللجوء للقضاء للمنازعة فى المسائل الخاصة بحماية البيانات.

٦٨ - كما كان المشرع المغربي أكثر مراعاة لمصالح الشخص المعنى بالبيانات، فقد منحه ممارسة الحقوق بدون مقابل، ونص صراحة على أن يكون ذلك "دون عوض". ومثال ذلك ما نصت عليه المادة ٨ أ من القانون على أن: "ويلتزم المسئول عن المعالجة بالقيام بالتصحيحات اللازمة دون عوض لفائدة الطالب..".

ثالثاً

شروط مشروعية جمع ومعالجة البيانات الشخصية

اشترط القانون، فى المادة الثانية منه، لجمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل، **صدور موافقة صريحة** من الشخص المعنى بالبيانات أو فى الأحوال المصرح بها قانونا.

كما اشترط، فى المادة الثالثة، لجمع البيانات ومعالجتها والاحتفاظ بها، ضرورة توافر أربعة شروط، هي:

١- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعنى.

٢- أن تكون صحيحة وسليمة ومؤمنة.

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

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

إحالة القانون للائحة التنفيذية:

"على أن تحدد اللائحة التنفيذية للقانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات".

ويلاحظ أن المشرع المصري أشار إلي هذه المسائل باعتبارها شروط للجمع والمعالجة، بينما نجد **اللائحة الأوروبية** تشير إليها فى الفصل الثانى منها، الخاص بالمبادئ، باعتبارها المبادئ المتعلقة بمعالجة البيانات الشخصية Principles relating to processing of personal data (م ٥)[٦٩]، والتى تتمثل فى المشروعية والشفافية وتحديد الغرض الصريح والواضح والمشروع واشتراط الملاءمة والصلة للأغراض التي تم تجميع البيانات من أجلها.

وبناء على ما تقدم، يمكن تقسيم هذا الموضوع على النحو التالى:

١- رضا الشخص المعنى بالبيانات.

٢- جمع ومعالجة البيانات لأغراض مشروعة ومحددة وواضحة.

٣- صحة وسلامة معالجة البيانات الشخصية وتأمينها.

٤- جمع ومعالجة البيانات بطريقة مشروعة وملائمة لأغراض تجميعها.

٥- تحديد مدة الاحتفاظ بالبيانات الشخصية.

١- رضا الشخص المعنى بالبيانات

أ- وجود الرضا:

يعد الرضا الصريح للشخص المعنى بالبيانات شرطاً أساسياً لمشروعية كافة العمليات التى تتم على البيانات الشخصية، سواء جمع البيانات أو معالجتها أو الإفصاح عنها أو إفشائها، ما لم يصرح القانون بغير ذلك.

ومن ثم يجب لتوافر رضا الشخص وجود الإرادة وأن يعبر عنها بصورة صريحة جازمة تُعبر عن موافقته على العمليات المزمع القيام بها على بياناته. ومن ثم لا يعتد بالتعبير الضمني عن الموافقة أو المعلقة على شرط، وبهذا تعد موافقة الشخص هي الأساس القانوني للمعالجة، ومرجع ذلك إلى أن بياناته تمس خصوصيته وقد تمتد إلى حياته العائلية التى يحرص أن تكون بعيدة عن الأنظار.

وقد تطلب المشرع المصري صراحة فى المادة الثانية وجود الرضا الصريح للشخص على جمع ومعالجة البيانات، وهو عين ما أخذت به اللائحة الأوروبية فى المادة ٦ منها، كما حددت المادة ٧ من اللائحة شروط الموافقة Conditions for consent.

وقد عرفت المادة ١١/٤ من اللائحة الأوروبية "موافقة صاحب البيانات consent» of the data subject" بأنها تعني أي إشارة صريحة ومحددة وواضحة لا لبس فيها، تدل على رضا صاحب البيانات والتي يشير من خلالها إلى الموافقة على معالجة البيانات الشخصية المتعلقة به أو بها، من خلال بيان أو بعمل إيجابي واضح.

بينما أغفل المشرع المصري تعريف "موافقة الشخص المعنى بالبيانات" على جمع ومعالجة البيانات، على عكس المشرع الأوروبي، وقد أكد المشاركون بالورشة أنه رغم وجود هذا

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

التعريف باللائحة الأوروبية إلا أن التطبيق قد يثير العديد من الصعوبات حال تطبيقه، لاختلاف وجهة النظر حوله.

تُوصي الورشة: أن تتضمن اللائحة التنفيذية تعريف موافقة الشخص المعنى بالبيانات، فى المادة الخاصة بالتعاريف، على أن تذكر شروط ومعايير واضحة لهذه الموافقة، فى مادة مستقلة، وتحدد شكل هذه الموافقة، سواء أكانت كتابية أو مجرد علامة علي خانة فى موقع إلكتروني، حتى تأتي الموافقة مستنيرة ومبنية على فهم وإرادة حقيقية، ويضاف إلى ذلك موافقة من ينوب عن الشخص المعنى متى كان عديم الأهلية أو ناقصها.

وتوصي الورشة بتناول المسائل المتعلقة بالموافقة في اللائحة التنفيذية للقانون من خلال الإحالة المنصوص عليها في المادة ٣ من القانون، حتي وإن كانت المادة ١/٦ الخاصة بالموافقة لم تنص على الإحالة للائحة التنفيذية.

ومن جهة أخرى، يثور تساؤل حول مصير البيانات التي تم تجميعها وحفظها بالفعل قبل صدور قانون حماية البيانات الشخصية الجديد وبدون الحصول على موافقة مسبقة للشخص المعنى على غرض محدد.

وقد أجابت المناقشات في ورشة العمل على هذا التساؤل حيث جرى الإشارة إلى أنها سوف تدخل ضمن إجراءات توفيق أوضاع المخاطبين بأحكام القانون ولائحته التنفيذية (خلال سنة من صدور اللائحة).

ب- شكل موافقة الشخص المعنى:

هناك مفارقة مصدرها نصوص القانون، فقد غاير المشرع فى الشكل الذى يجب أن تفرغ فيه الموافقة، فمن ناحية تطلبت المادة ٢، فى حالة البيانات الشخصية، صدور موافقة صريحة من الشخص المعنى بالبيانات، بينما تستلزم المادة ١٢، فى حالة البيانات الشخصية الحساسة، الحصول على موافقة كتابية صريحة من الشخص المعنى، وهو ما يصوره الشكل التالى:

البيانات الشخصية:	موافقة صريحة
البيانات الشخصية الحساسة:	موافقة كتابية صريحة

وهو ما يقطع بما لايدع مجالا للشك حول استلزم الكتابة عند صدور الموافقة على معالجة وجمع البيانات الشخصية الحساسة.

ولكن يظل التساؤل مُثاراً عن الصورة التى تُفرغ فيها الموافقة الصريحة التى تطلبها القانون المصري فى حالة البيانات الشخصية (غير الحساسة)، فالقانون لم يستلزم أن تتخذ هذه الموافقة طريقاً معيناً أو شكلاً مخصوصاً، ومن ثم يكون للشخص وفقاً للقواعد العامة حرية كاملة فى التعبير عن الموافقة على الوجه الذى يراه، فالتعبير يكون صريحاً إذا قصد به صاحبه إحاطة الغير علماً بإرادته، أياً كان المظهر الذى يتخذه، شفاهة أو بالكتابة، أياً كانت عباراتها أو صورتها، سواء بصورة شخصية، كخطاب أو برقية، أو بصفة غير شخصية، كإعلان أو نشرة، أو بالإشارة التى لها دلالة بين الناس[٧٠].

وفى هذا الصدد تنص المادة ١/٩٠ مدني على أن: "التعبير عن الإرادة يكون باللفظ وبالكتابة وبالإشارة المتداولة عرفاً كما يكون باتخاذ موقف لا تدع ظروف الحال شكا فى دلالته على حقيقة المقصود".

ونعتقد أنه رغم عدم اشتراط المشرع إفراغ الموافقة فى شكل مكتوب، إلا أن الشخص المسئول، المتحكم أو المعالج، سيكون حريصاً على الحصول عليها فى صورة مكتوبة لضمان نسبتها لصاحبها وتيسيراً لإثباتها، وغالباً ما يتم إعداد نماذج محددة لإفراغ هذه الموافقة وفق الضوابط التى يتطلبها القانون.

جـ - صحة رضا الشخص المعنى بالبيانات:

لا يكفي مجرد وجود رضا الشخص المعنى بالبيانات، إنما يجب فوق ذلك أن يكون صحيحاً، وهو يكون كذلك متى وجدت الإرادة، فإذا انعدمت الإرادة انعدم الرضا، واستحال توافره نتيجة لانعدامه، وعلى ذلك لا يتوافر الرضا إلا إذا توافرت الأهلية لدى الشخص المعنى بالبيانات، والأهلية المطلوبة هنا هى أهلية الأداء أى صلاحية الشخص لاستعمال الحق[٧١]، أو بمعنى آخر قدرة الشخص على أداء التصرفات القانونية لحساب نفسه، ومناطها التمييز أو الرشد، إذ تتأثر بالسن والعقل، فيجب أن يصدر التعبير من شخص اكتملت مداركه ونضجت، فأصبح يقدر الآثار المترتبة على تصرفاته.

وباستقراء نصوص القانون نجدها تخلو من اشتراط أن يكون الشخص المعنى بالبيانات بالغاً سن الرشد (٢١ عاماً) أو تحديد سن معين، وهو فى اعتقادنا شرط بديهي لخطورة الآثار القانونية المترتبة على عمليات معالجة البيانات وهو ما يتطلب اكتمال إدراك الشخص حتى يتبين تصرفاته.

٧٠ - د. محمود جمال الدين زكى: الوجيز فى نظرية الالتزام فى القانون المدني المصري، الجزء الأول فى مصادر الالتزام، مطبعة لجنة التأليف والترجمة والنشر، ١٩٦٨، ص٢٩.

٧١ - د. عبد الرزاق السنهوري: الوسيط فى شرح القانون المدنى، الجزء الأول: نظرية الالتزام بوجه عام، مصادر الالتزام، تنقيح المستشار/ أحمد مدحت المراغى، طبعة نادى قضاة مجلس الدولة، ٢٠٠٨، ص٢٢٤.

وفى هذا الصدد تنص المادة ٤٥ مدني على أن:

(١) لا يكون أهلاً لمباشرة حقوقه المدنية من كان فاقد التمييز لصغر فى السن أو عته أو جنون.

(٢) وكل من لم يبلغ السابعة يعتبر فاقداً للتمييز.

كما تنص المادة ٤٦ مدني على أن: "كل من بلغ سن التمييز ولم يبلغ سن الرشد، وكل من بلغ سن الرشد وكان سفيها أو ذا غفلة، يكون ناقص الأهلية وفقاً لما يقرره القانون".

ومن ثم لا يتوافر الرضا إذا صدر عن شخص غير مميز، كالمجنون والمعتوه، والصغير دون السابعة، وفاقد الوعي لسبب عارض، كمرض أو سُكر أو تخدير أو تنويم، لأن هؤلاء معدومي الإرادة[٧٢]. كذلك لا تصح الموافقة إذا صدرت ممن لم يبلغ سن الرشد أو بلغه ولكن كان مصاباً بسفه أو غفلة.

وحيث تنص المادة ٤٧ مدني على أن: "يخضع فاقدو الأهلية وناقصوها بحسب الأحوال لأحكام الولاية أو الوصاية أو القوامة بالشروط ووفقاً للقواعد المقررة فى القانون".

ومن ثم يجب موافقة الشخص على عمليات المعالجة، متى كان بالغاً سن الرشد، أما فى حالة عدم بلوغه، أو كان بالغاً ومصاباً بعاهة عقلية، فيجب الحصول على موافقة من ينوب عنه قانوناً (كالولي أو الوصى).

ومن الغريب أن المشرع استلزم موافقة "ولي الأمر" فى حالة إجراء أى عملية جمع أو معالجة أو غيره على البيانات الشخصية الحساسة التى تتعلق ببيانات الأطفال، دون بيان شكل هذه الموافقة.

كما أن نص المادة ١٢ من القانون يستخدم لفظ الطفل، وهذا اللفظ يُقصد به من لم يبلغ الثامنة عشر من عمره، وفقاً للمادة الثانية من قانون الطفل (رقم ١٢ لسنة ١٩٩٦ والمعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨)، فما هو حال من بلغ هذه السن، ١٩ عاماً مثلاً، فهو فى نظر القانون ليس طفلاً، وفى الوقت نفسه، لا يعتبر رشيداً، طالما لم يبلغ سن الرشد، **ومن ثم وفقاً للنص الحالى للقانون لا يشترط موافقة الولي، سواء فى البيانات الحساسة أو غيرها.**

ولهذا كان يُفضل تحديد سن محدد للرضا، كما فعلت اللائحة الأوروبية، فى المادة ٨ منها، حيث اعتبرت معالجة بيانات الطفل فى إطار خدمات مجتمع المعلومات مشروعة، حين يكون سن الطفل ١٦ عاماً على الأقل، أما إذا كان سنه لا يتجاوز ذلك، فإن المعالجة لا تكون مشروعة، إلا إذا صدر الرضا من قبل صاحب السلطة الأبوية على الطفل (من ينوب عنه قانوناً). ويجوز للدول الأعضاء تخفيض هذا السن بشرط ألا يقل بأى حال من الأحوال عن ١٣ سنة (م ١/٨ من اللائحة)..

د - الموافقة الصريحة على حركة البيانات الشخصية عبر الحدود حال عدم توافر مستوى الحماية المطلوب:

تشترط المادة ١٥ من القانون عند نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية المنصوص عليه فى القانون، ضرورة الحصول على الموافقة الصريحة للشخص المعنى أو من ينوب عنه، وذلك فى الحالات الآتية:

١- المحافظة على حياة الشخص المعنى 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 المعنى بالبيانات.

٤- تنفيذ إجراء خاص بتعاون قضائي دولي.

٥- وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة.

٦- إجراء تحويلات نقدية إلى دولة أخرى وفقاً لتشريعاتها المحددة والسارية.

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

هـ- اشتراط موافقة الشخص المعنى على التسويق الإلكتروني المباشر له:

تحظر المادة ١٧ من القانون إجراء أى اتصال إلكتروني بغرض التسويق المباشر للشخص المعنى بالبيانات إلا بعد الحصول على موافقة منه، إلى جانب توافر الشروط الأخرى التى يتطلبها نص المادة ومنها وضع آليات واضحة وميسرة لتمكين الشخص المعنى بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها.

ويلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعنى بالبيانات وتعديلاتها أو عدم اعتراضه على استمراره، بشأن تلقى الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث

٧٢ - د. محمود جمال الدين زكي: الوجيز فى نظرية الالتزام فى القانون المدنى المصرى، مرجع سابق، ص٢٧.

سنوات من تاريخ آخر إرسال (م ١٨ من القانون).

و - الحالات المستثناة من الحصول على موافقة الشخص المعنى:

أجاز المشرع استبعاد الحصول على موافقة الشخص المعنى فى الأحوال المصرح بها قانوناً، ومن ذلك على سبيل المثال، متى كانت معالجة البيانات تحقق مصلحته وتعذر الاتصال به أو كان الحصول علي موافقته يتطلب مجهوداً مرهقاً أو كانت معالجة البيانات يقتضيها القانون أو وفقاً لاتفاق يكون صاحب البيانات طرفاً فيه، أو للحفاظ على المصالح الحيوية للشخص المعنى إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه، أو لأغراض الصالح العام أو لإنجاز مصلحة مشروعة يتوخاها المسئول عن المعالجة مع مراعاة عدم تجاهل مصلحة الشخص المعنى أو حقوقه وحرياته الأساسية[٧٣].

وفى هذا الصدد، تشير صياغة المادة ٦ من القانون، المعنية بشروط المعالجة، إلى أن المعالجة تعد مشروعة وقانونية فى حال توافر أي من الحالات الآتية، وأول هذه الحالات هى موافقة الشخص المعنى بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر، ثم أضافت ثلاث حالات أخرى، وهو ما يعنى بمفهوم المخالفة عدم اشتراط موافقة الشخص فى هذه الحالات الثلاث، وهي:

- أن تكون المعالجة لازمة وضرورية تنفيذاً لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعنى بالبيانات، أو لمباشرة أى من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها.
- تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناء على حكم قضائي.
- تمكين المتحكم من القيام بالتزاماته أو أي ذى صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات.

وتقابل هذه الأحكام ما ورد فى المادة السادسة من اللائحة الأوروبية، التى تتناول قانونية المعالجة Lawfulness of processing،

٧٣ - د. عمرو طه بدوى: التنظيم القانونى لمعالجة البيانات الشخصية - دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية، أكاديمية أبوظبى القضائية، ٢٠١٩، ص ص ١٠٩، ١١٠. وراجع أيضاً المادة ٤ من القانون المغربى المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، حيث تشير فقرتها الثانية إلى ما يلى: "... غير أن الرضى لا يكون مطلوباً إذا كانت المعالجة ضرورية: (أ) لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة؛ (ب) لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد تتخذ بطلب من الشخص المذكور؛ (ج) للحفاظ على المصالح الحيوية للشخص المعني إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه؛ (د) لتنفيذ مهمة تدخل ضمن الصالح العام أو ضمن ممارسة السلطة العمومية التي يتولاها المسؤول عن المعالجة أو أحد الأغيار الذي يتم إطلاعه على المعطيات؛ (هـ) لإنجاز مصلحة مشروعة يتوخاها المسؤول عن المعالجة أو المرسل إليه مع مراعاة عدم تجاهل مصلحة الشخص المعني أو حقوقه وحرياته الأساسية".

وفى السياق نفسه سار المشرع الفرنسي فى المادة السابعة من قانون المعلوماتية والحريات والمُعدّل بالقانون رقم (٤٩٣) لسنة ٢٠١٨ بشأن حماية البيانات الشخصية إلى الحالات التى يجوز فيها معالجة البيانات دون حاجة لموافقة الشخص المعنى.

حيث تشير المادة السادسة من اللائحة الأوروبية، فى فقرتها الأولى، وهى تكاد تتطابق مع المادة السابعة من القانون الفرنسي، إلى أنه: تكون المعالجة قانونية في حالة توافر أي من الحالات الآتية:

(أ) موافقة صاحب البيانات على معالجة بياناته الشخصية لغرض محدد أو أكثر؛

(ب) أن تكون المعالجة ضرورية لأداء العقد الذي يكون صاحب البيانات طرفًا فيه أو من أجل اتخاذ خطوات بناءً على طلب من صاحب البيانات قبل إبرام العقد؛

(ج) أن تكون المعالجة ضرورية للامتثال لالتزام قانوني يخضع له المتحكم؛

(د) أن تكون المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر؛

(هـ) المعالجة ضرورية لأداء مهمة يتم تنفيذها للمصلحة العامة أو ضمن ممارسة السلطة الرسمية المخولة للمتحكم؛

(و) المعالجة ضرورية لأغراض المصالح المشروعة التي ينتهجها المتحكم أو طرف ثالث، إلا إذا كانت المصالح تتعارض مع الحقوق والحريات الأساسية لصاحب البيانات التي تتطلب حماية البيانات الشخصية، وخاصة حين يكون صاحب البيانات طفلاً.

٢- جمع البيانات لأغراض مشروعة ومحددة وواضحة

يجب أن يكون لجمع البيانات ومعالجتها أغراض أو أهداف مشروعة ومحددة وواضحة ومعلنة للشخص المعنى، على نحو ما صرحت المادة الثالثة (فقرة أولى بند ١) من قانون حماية البيانات الشخصية، ويُعد هذا الشرط من الشروط الجوهرية التي ينبغى توافرها سواء أكان ذلك بالنسبة للمعالج أو المتحكم أو الغير الذي ترسل اليه البيانات، ويجب أن يظل هذا الشرط قائماً خلال فترة الجمع أو المعالجة أو الاحتفاظ بالبيانات، كما يجب أن يظل متوافراً أيضاً بعدها[٧٤].

وقد أشارت اللائحة الأوروبية فى الفصل الثاني منها، الخاص بالمبادئ، إلى المبادئ المتعلقة بمعالجة البيانات الشخصية

٧٤ - فى هذا الصدد، راجع: د. سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية - دراسة القانون الفرنسي، القسم الأول، مجلة الحقوق جامعة الكويت، المجلد ٣٥، العدد ١١، ٢٠١١، ص ٤١٥ وما بعدها؛ د. عمرو طه بدوى: مرجع سابق، ص ١٠٩ وما بعدها.

(م٥)، وأشارت فى الفقرة الأولى منها (بند ب) إلى ضرورة أن تكون البيانات الشخصية قد جُمعت لأغراض محددة وصريحة ومشروعة collected for specified, explicit and legitimate purposes ولم تتم معالجتها بطريقة تتنافى مع هذه الأغراض؛ ولا تعتبر المعالجة الإضافية لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو البحثي أو الأغراض الإحصائية، وفقاً للمادة ٨٩ بند ١، متعارضة مع الأغراض الأولية (تحديد الغرض).

وجدير بالذكر أن المعالجة تكون مشروعة متى كانت لا ترمي الى الإساءة للأشخاص أو التشهير بهم، ومن ذلك على سبيل المثال، اذا كانت المعالجة لازمة لأغراض منع أو كشف الجرائم بناءً على طلب من جهات التحقيق، أو كانت مطلوبة أو مصرحاً بها بموجب أي قانون أو كان ذلك بقرار صادر من المحكمة، أو إذا كانت البيانات ضرورية لتقدير أو تحصيل الضرائب أو الرسوم، أو إذا كانت لحماية مصلحة حيوية للشخص المعنى بالبيانات[٧٥].

وفى هذا الصدد، قد تلتزم الجهات القائمة بجمع ومعالجة البيانات الشخصية بتوضيح الغرض من الجمع والمعالجة، علي أنه يُحظر استخدام المعلومات والبيانات المسجلة لدى القائم بالمعالجة في أغراض غير التي جمعت أو تم معالجتها من أجلها.

وعلى العكس من ذلك، يجوز معالجة البيانات فى غير الأغراض التي جمعت من أجلها في بعض الحالات، ويتحقق ذلك، مثلاً، فى حالة المعالجة التي تتم بناء على موافقة الشخص المعنى بالأمر.

يُلاحظ: أن نص المادة (٣ فقرة أولى، بند ١) اقتصر على حالة جمع البيانات، ولم يذكر المعالجة أو الاحتفاظ بالبيانات في هذه الفقرة، علماً بأن صدر الفقرة ينص علي ضرورة توافر بعض الشروط في حالة الجمع والمعالجة والاحتفاظ بالبيانات.

تُوصي الورشة: أن يراعى القانون ضبط هذا الشرط، بأن تجمع البيانات "وتعالج ويحتفظ بها" لأغراض مشروعة ومحددة ومعلنة للشخص المعنى بالبيانات.

٣- صحة وسلامة البيانات الشخصية وتأمينها

اشترطت المادة الثالثة (فقرة أولى) لجمع البيانات ومعالجتها والاحتفاظ بها ضرورة توافر الشروط الآتية: ... "٣- أن تكون صحيحة وسليمة ومؤمنة".

بيد أن صياغة هذا النص توحي لأول وهلة باشتراط الصحة والسلامة والتأمين لعمليات الجمع والمعالجة، بيد أن المقصود بها هو أن تكون "البيانات" صحيحة وسليمة ومؤمنة، حتى يمكن جمعها ومعالجتها.

وقد راعت اللائحة الأوروبية هذا الأمر، فى المادة ٥ منها (الخاصة بالمبادئ المتعلقة بمعالجة البيانات)، فى البند د، مع اختلاف فى الصياغة، فنصت على ضرورة أن تكون البيانات الشخصية دقيقة accurate، ويجرى تحديثها kept up to date عند الضرورة؛ ويجب اتخاذ اللازم لضمان محو أو تصحيح البيانات الشخصية غير الدقيقة دون تأخير، مع مراعاة الأغراض التي تتم معالجتها من أجلها ("الدقة accuracy").

ويقتضي ذلك من المعالج أو المتحكم قبل البدء في جمع أو معالجة البيانات الشخصية، أن يتحقق من أن البيانات التي تم جمعها أو معالجتها ذات صلة بالأغراض المشروعة او كافية لتحقيقها، كما يجب التحقق من أن تلك البيانات دقيقة ومكتملة وحديثة بما يفى بالأغراض المشروعة.

كما يتطلب هذا الإلتزام التحقق من دقة البيانات أو المعلومات الشخصية والمسجلة لديه بأنظمة المعلومات و المتعلقة بالشخص المعنى بالبيانات وإستكمالها وتحديثها بانتظام والقيام بمحو أو تعديل أي بيانات أو معلومات تتعلق بها.

كذلك تشير اللائحة الأوروبية فى المادة ٥ بند ج، إلى ضرورة أن تكون البيانات الشخصية ملائمة adequate وذات صلة relevant ومحددة limited لما هو ضروري بالنسبة للأغراض التي تتم معالجتها من أجلها (الحد الأدنى من البيانات data minimisation).

وبالنسبة للالتزام بسلامة المعالجة security of processing ألزم المشرع المصري في المادة الرابعة (بند٦) من قانون حماية البيانات الشخصية "اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظاً علي سريتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قبل أي إجراء غير مشروع".

وتعقيبا على مسلك المشرع المصري في بيان شروط الجمع والمعالجة انه تغاضي عن اشتراط أن يتم جمعها ومعالجتها بما يحافظ على سرية البيانات التي تمت معالجتها.

تُوصي الورشة: بتعديل البند الثالث من المادة الثالثة من القانون بإضافة كلمة سرية اليه علي أن تعالج بطريقة مشروعة و ملائمة للأغراض التي يتم تجميعها لأجلها وبما يحافظ على سريتها.

٧٥ – د. عمرو طه بدوي: مرجع سابق، ص١١٠.

٤- جمع ومعالجة البيانات بطريقة مشروعة وملائمة لأغراض تجميعها

لم يكتف المشرع المصري بالنص على ضرورة جمع البيانات بطريقة مشروعة، وإنما اشترط أيضاً، فى المادة الثالثة (فقرة أولى، بند ٣) "أن **تُعالج** بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها".

ويعني هذا الشرط عدم جواز جمع أو تجهيز أو تسجيل أية بيانات شخصية أو معلومات بأساليب أو بطرق غير مشروعة أو بغير رضا الشخص المعنى أو من ينوب عنه[٧٦]. لذلك يحظر على القائمين على معالجة البيانات القيام بجمعها أو تسجيلها بأساليب أو بطرق غير مشروعة.

وحتى يسوغ القول بأن عملية جمع البيانات قد تمت بطريقة مشروعة، فإنه يجب أن يتم إعلام الشخص المعنى بالبيانات عن وجود تجميع لهذه البيانات وعن طريقة التجميع والغرض من التجميع وأنواع البيانات التي تم تجميعها[٧٧].

وفي الإتجاه نفسه نصت اللائحة الاوروبية، فى المادة ٥ (الخاصة بالمبادئ المتعلقة بمعالجة البيانات الشخصية)، بند أ، على أن تكون البيانات قد تم معالجتها بطريقة مشروعة lawfully وعادلة fairly وبطريقة شفافة transparent manner بالنسبة لصاحب البيانات (المشروعية lawfulness والعدالة fairness والشفافية transparency).

ومن ثم تتطلب عملية معالجة البيانات أن تجري بدقة وأمانة من المتحكم أو المعالج وعدم إستخدام أية وسائل إحتيالية أو غير مشروعة لجمع ومعالجة البيانات، وكذلك يحظر القيام بجمع بيانات شخصية لأغراض غير مشروعة، أو مخالفة للنظام العام، أو بيانات شخصية غير صحيحة، أو غير ضرورية لنشاط المعالجة.

تعقيب: رغم أن نص المادة الثالثة من القانون المصري يتناول في صدر المادة قواعد جمع ومعالجة البيانات إلا أن البند الثالث تضمن الإشارة إلى أن تجري المعالجة بطريقة مشروعة، دون جمع البيانات، الذى اقتصر فى شأنه على أن يكون لأغراض مشروعة، وهو ما يثير التساؤل حول اشتراط أن يكون الجمع بطريقة نزيهة ومشروعة وملائمة، ونعتقد أن النص يمتد أيضاً لجمع البيانات، فيجب أن تتم بطريقة مشروعة، باعتبارها مسألة بديهية.

٧٦ – د. عمرو طه بدوي: مرجع سابق، ص ١٠٥.

٧٧ – د. سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية، مرجع سابق، ص ٤٠٤.

٥- تحديد مدة الاحتفاظ بالبيانات الشخصية

حظر المشرع المصري، فى المادة الثالثة من قانون حماية البيانات الشخصية، الفقره الرابعة بند ٤، أن يتم الاحتفاظ بالبيانات التي يتم معالجتها **لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.**

فالاحتفاظ بالبيانات لا يجوز أن يكون أبدياً بل يكون مؤقتاً ومحدداً لمدة معينة، ويعنى ذلك أنه يتعين على المعالج أن يقوم بحفظ البيانات التي تمت معالجتها لمدة زمنية معينة بحيث لا تتجاوز المدة المطلوبة للأغراض التي جمعت من أجلها[٧٨].

وتأكيداً على هذا الشرط اتجهت اللائحة الاوروبية، فى المادة ٥ بند هـ، إلى ضرورة أن يتم معالجة البيانات في شكل يسمح بتحديد هوية صاحب البيانات لمدة معينة، لا تزيد عما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها.

ومع ذلك أجازت المادة نفسها (بند هـ)، لأغراض معالجة البيانات الشخصية، تخزين البيانات الشخصية لفترات أطول، لأغراض الأرشفة من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية، مع مراعاة التنفيذ الفني والتنظيمي المناسب واتخاذ التدابير المطلوبة للحفاظ على حقوق وحريات صاحب البيانات.

ورغم أهمية شرط الاحتفاظ بالبيانات الشخصية لمدة معينة، إلا أنه لا يوجد ضابط لتحديد هذه المدة.

ولهذا يقع على عاتق اللائحة التنفيذية وضع الضوابط اللازمة لذلك.

كذلك لم يقرر المشرع المصري عقوبة في حالة اذا ما تم الاحتفاظ بالبيانات الشخصية لمدة تزيد عن المدة اللازمة للوفاء بالغرض المحدد لها.

و لهذا نوصي المشرع بضرورة النص علي عقوبة في حالة الاحتفاظ بالمعلومات لمدة أطول من المدة المنصوص عليها في القانون أو اللائحة.

٧٨ – د. عمرو طه بدوي: مرجع سابق، ص ص ١٠٢، ١٠٣.

المحور الثالث

التزامات أطراف معالجة وحماية البيانات

■ تمهيد:

يؤدي كل من المتحكم والمعالج دوراً بالغ الخصوصية وشديد الأهمية فى نطاق معالجة البيانات الشخصية، لدرجة يمكن القول معها أنهما فى قلب القانون الجديد وجوهر أحكامه. وفضلاً عن ذلك اشترط القانون على الممثل القانون للشخص الاعتبارى لأي متحكم أو معالج تعيين شخص يكون مسئولاً عن حماية البيانات الشخصية، وألقى المشرع على عاتقه لفيف من الالتزامات.

ويدعونا ذلك لبيان التزامات المتحكم ومعالج البيانات كما ورد في قانون حماية البيانات المصري، مقارنة مع اللائحة الأوروبية لحماية البيانات (GDPR)[٧٩]، ثم نشير لمسئول حماية البيانات الشخصية.

أولاً – التزامات المتحكم والمعالج فى إطار حماية البيانات.

ثانياً – دور مسئول حماية البيانات الشخصية والتزاماته.

٧٩ – من الجدير بالملاحظة فى هذا الصدد أن قانون خصوصية المستهلك في كاليفورنيا (California Consumer Privacy Act of 2018) يتشابه لحد كبير مع اللائحة العامة لحماية البيانات (GDPR)، ومن المتوقع أن يكون له تأثير عالمي، نظرًا لوضع كاليفورنيا الاقتصادي المتقدم في العالم.
وقد اتجه نهج قانون كاليفورنيا إلى التركيز على كيفية التعامل مع النشاط الاقتصادي والضرر الفردي وكيفية حماية البيانات بشكل عام بدلا من حظر الجمع والمعالجة، و قد أنتهج المشرع المصري نهج المشرع الأوروبي.

أولاً

التزامات المتحكم والمعالج فى إطار حماية البيانات

أشارت الدراسة إلى تعرض المشرع المصري إلى القائمين على عملية جمع ومعالجة البيانات، فأشار إلى المتحكم والمعالج، وأيضاً الحائز، والأخير لم يفرض عليه التزامات مطلقاً، نظراً لدوره الضعيف فى هذا المجال.

ومن هنا تقتصر الدراسة هنا على بيان التزامات المتحكم، من ناحية أولي، ثم تشير لالتزامات المعالج، من ناحية أخرى، ونخص لكل من هذه المسائل فقرة مستقلة.

١ - التزامات المتحكم في البيانات

تضع المادة ٤ من قانون حماية البيانات الشخصية المصري على عاتق المتحكم عدد كبير من الالتزامات (١٢ التزامًا)، عددتها وحصرتها هذه المادة، بينما أشارت اللائحة الأوروبية إلى التزامات المتحكم فى نصوص متفرقة، ووضعت المبدأ العام لمسئوليته فى المادة ١/٢٤ منها، حيث نصت على أن: ١- مع الأخذ في الاعتبار طبيعة المعالجة ونطاقها وسياقها وأغراضها، وكذلك مخاطر تنوع احتمالية وشدة حقوق وحريات الأشخاص الطبيعيين، يجب على المتحكم تنفيذ التدابير التقنية والتنظيمية المناسبة لضمان وإمكان إثبات أن المعالجة تتم وفقًا لهذه اللائحة. ويجب مراجعة هذه التدابير وتحديثها عند الضرورة.

٢- حينما تكون متناسبة مع أنشطة المعالجة، يجب أن تشمل التدابير المشار إليها في الفقرة ١ تنفيذ سياسات حماية البيانات المناسبة من قبل المتحكم.

٣- يجوز استخدام الالتزام بقواعد السلوك المعتمدة كما هو مشار إليه في المادة ٤٠ من اللائحة أو آليات التصديق المعتمدة على النحو المشار إليه في المادة ٤٢ من اللائحة كعنصر لإثبات الامتثال لالتزامات المتحكم المالية.

ويبدو من ذلك من جماع الالتزامات الملقاة على عاتق المتحكم أنه يعتبر المسئول الأساسى عن ضمان إجراء عملية المعالجة وفقًا للقواعد المنصوص عليها في اللائحة، ويقع على عاتقه مسئولية إثبات اتخاذ الإجراءات اللازمة للامتثال لقواعد اللائحة، وتمنحه اللائحة إرشادات حول كيفية إثبات قانونية أنشطة المعالجة التي يقوم بالإشراف عليها. ومن ثم يكون المتحكم هو المسئول عن توفير الإجراءات التقنية والتنظيمية والمعايير الكافية التي تسمح لصاحب البيانات أن يمارس حقوقه المنصوص عليها في اللائحة بسهولة كافية.

وعوداً لالتزامات المتحكم فى القانون المصري، نصت المادة ٤ من القانون على أن: مع مراعاة أحكام المادة ١٢ من هذا القانون (المعنية بالبيانات الحساسة وحظر إجراء أي عملية عليها إلا بإذن مركز حماية البيانات)، يلتزم المتحكم بما يأتي:

أ - الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعنى بالبيانات، أو فى الأحوال المصرح بها قانونًا.

تُلقى هذه الفقرة على عاتق المتحكم التزاماً بالتأكد من موافقة الشخص المعنى بالبيانات وإثبات هذه الموافقة[٨٠]، وقد وضع المشرع الأوروبي نفس الالتزام على عاتق المتحكم في المادة السابعة منه، حيث يجري نصها على أن:

١- عندما تعتمد المعالجة على الموافقة، يجب أن يكون المتحكم قادرًا على إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية.

٢- إذا كانت موافقة صاحب البيانات مقدمة في سياق إعلان مكتوب يتعلق أيضًا بأمور أخرى، فيجب تقديم طلب الموافقة بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، وفي شكل واضح يسهل الوصول إليه، وباستخدام لغة واضحة ومفهومة، وأي جزء من هذا الإعلان يشكل انتهاكًا لهذه اللائحة لن يكون ملزمًا.

٣- يحق لصاحب البيانات سحب موافقته في أي وقت، ولن يؤثر سحب الموافقة على قانونية المعالجة، طالما كان هناك سابقة موافقة.

وجدير بالذكر فى هذا الصدد وجود اتفاق بين مسلك كل من المشرعين المصري والأوروبي على أن الحصول على موافقة الشخص المعنى البيانات على المعالجة يقع على عاتق المتحكم، إلا أنهم اختلفوا في طريقة اشتراط ذلك.

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

وفى هذا الإطار تقرر المادة ٢٥ بند ٢ من اللائحة الأوروبية التزاماً على عاتق المتحكم بتنفيذ التدابير الفنية والتنظيمية المناسبة لضمان أن البيانات الشخصية الضرورية فقط لكل غرض محدد للمعالجة تتم بشكل افتراضي.

٨٠ - يمكن إثارة سؤال في هذا الشأن حول كيفية الإثبات وعلاقة هذا القانون بقانون التوقيع الإلكتروني ومعايير الدليل الإلكترونى بشكل عام.

جـ - وضع طريقة وأسلوب ومعايير المعالجة طبقا للغرض المحدد، ما لم يقرر تفويض المعالج فى ذلك بموجب تعاقد مكتوب.

ويتسق هذا الالتزام مع تعريف المتحكم، فى القانون المصري واللائحة الأوروبية، الذى يشير إلى أنه يكون له بحكم أو طبيعة عمله تحديد طريقة وأسلوب ومعايير الاحتفاظ بالبيانات أو معالجتها the purposes and means of the processing of personal data أو التحكم فيها طبقا للغرض المحدد أو نشاطه.

و يمكن إعتبار هذه القاعدة هى أساس ترتيب مسئولية المتحكم بصفته المسئول الأساسي عن حماية البيانات الشخصية.

ولكن يجوز **تفويض** وضع طريقة وأسلوب ومعايير المعالجة طبقاً للغرض **إلى المعالج** بناء على تعاقد مكتوب، وهو ما قد ينبني عليه عدم وضوح الرؤية لدى تحديد المسئول الفعلي عن حماية البيانات.

وقد أشارت ورشة العمل إلى أن من شأن السماح بوجود مثل هذا التفويض قد يؤدي إلى خلط لا داعي له بين المسئوليات، الأمر الذي يحتاج إلى بعض التوضيح والتنظيم، فضلاً عن ضرورة أن يتم ذلك وفقاً لمعايير تقنية واضحة.

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

ويهدف هذا الالتزام لضمان حيدة المتحكم فى عملية جمع البيانات وضمان جمعها للأغراض المحددة للمعالجة.

هـ - القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية إلا فى الأحوال المصرح بها قانونًا.

يؤكد المشرع المصري وفقاً لهذا النص التزام المتحكم بالحفاظ على البيانات الشخصية وعدم إتاحتها إلا فى الأحوال التى يصرح بها القانون، ويتفق في ذلك مع اللائحة العامة التي تؤكد ذلك سواء في المادة الرابعة أو المادة الخامسة.

بيد أن صياغة النص جاءت غير منضبطة، فهى توحى فى البداية بالتزامه بالعمل أو الامتناع عن عمل من شأنه إتاحة البيانات ثم عاد وقصرها على الأحوال المصرح بها قانوناً، فكان من الأولى أن يستهل الفقرة بكلمة "عدم" القيام بعمل ... إلا فى الأحوال المصرح بها قانوناً، كما كان يمكن إضافة "أو موافقة صريحة من الشخص المعنى بالبيانات"، اتساقاً مع المادة ٢ من القانون الخاصة بشروط جمع ومعالجة البيانات.

و - اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية وتأمين البيانات الشخصية حفاظًا على سريتها، وعدم اختراقها، أو إتلافها، أو تغييرها أو العبث بها قبل أى إجراء غير مشروع.

تأتي هذه الفقرة متسقة مع الفقرة الأولى من المادة ٥ من اللائحة الأوروبية بند هـ[٨١] حيث تنص أيضًا على مبدأ أمن البيانات، بيد أنها لم تتعرض لبيان المقصود بأمن البيانات أو وضع معايير معينة لتحديدها، بل اكتفت بتقرير أن اشتراط الأمن يجب أن يكون "مناسب Appropriate Security"، وقد اتبع المشرع في ذلك النهج القائم على قياس المخاطر "Risk Based Approach" وتحديد مناسبة الإجراءات الأمنية حسب حجم المخاطر التي قد تتعرض لها البيانات[٨٢]. وعليه فمن الأفضل أن يتطرق المشرع المصري إلى وضع هذه المعايير في اللائحة التنفيذية للقانون أو من خلال اعتماد معايير عالمية أو اقتراح معايير مصرية تشرح ما هو الحد الأدنى من الأمن أو ماهو المقصود بالأمن بشكل عام.

ولقد أحسن المشرع المصري صنعاً عندما اتبع هذا النهج فترك تحديد الأمور التقنية التي تكون بطبيعتها سريعة التغيير وتحتاج إلى توفيق مع طبيعة البيانات إلى تنظيم اللائحة التنفيذية.

وقد أوصت الورشة في هذا السياق أن تكون تلك المعايير معايير تقنية متماشية مع المعايير الدولية في هذا المجال.

إضافة إلى ذلك أوصت الورشة بإعداد معايير مصرية، واعتمادها من الهيئات والجهات الرسمية بما يتماشى مع متطلبات القانون والثقافة المصرية.

ز - محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما فى حال الاحتفاظ بها لسبب من الأسباب المشروعة بعد انتهاء الغرض فيجب ألا تبقى فى صورة تسمح بتحديد الشخص المعنى بالبيانات.

يتماشى هذا الالتزام مع حق المحو الذي يقرره المشرع المصري للشخص المعنى للبيانات، وهو ما ورد أيضاً فى اللائحة الأوروبية، حيث أقرت حق الأفراد في مسح ومحو البيانات الشخصية "الحق في النسيان"، كما أشارت الدراسة تفصيلاً فى الفصل الثانى" من هذه الدراسة.

---

٨١ - تنص الفقرة الأولى من المادة الخامسة بند (هـ) على أن : تتم معالجتها بطريقة تضمن الأمان المناسب للبيانات الشخصية، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقد أو التلف أو التلف العرضي ، باستخدام التدابير التقنية أو التنظيمية المناسبة ("النزاهة والسرية").

٨٢ - يتفق ذلك أيضا مع قانون خصوصية المستهلك في كاليفورنيا، حيث ينص أيضا على التزام الشركة بتوفير إجراءات أمنية مناسبة وذلك بدون تعريف ما هو مستوى الأمن المعقول "Reasonable Security". ولكن قامت وزارة العدل بكاليفورنيا بإصدار يمكن إستخدامه لتحديد عناصر الحد الأدنى من الحماية التي يجب أن تتبعها جميع الشركات الخاضعة لنطاق القانون.. يمكن تصفح هذا التقرير الصلدر بتاريخ فبراير ٢٠١٦ عبر الموقع التالى:
https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

وهذا الحق ليس هو الطريقة الوحيدة التي تفرض بها اللائحة العامة لحماية البيانات التزامًا على المتحكم للنظر في حذف البيانات الشخصية بل يتعلق الأمر أيضًا بالبيانات الخاصة الأطفال التى يتم تم جمعها - يعكس هذا الحماية المعززة لبيانات الأطفال - وبخاصة عبر الإنترنت.

ح: تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به:

وهذا الالتزام بديهي، يجب أن يضطلع به المتحكم، حتى ولو لم ينص عليه القانون، نظراً لأن الخطأ فى البيانات قد يرتب ضرراً بالغاً للشخص المعنى بالبيانات، ويكون مؤثراً عليه.

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

ويتسق مسلك المشرع المصري في هذا الالتزام مع مسلك المشرع الأوروبي، حيث تنص المادة (٣٠) من اللائحة الأوروبية على أن: على كل متحكم، وعند الضرورة، ممثل المتحكم، الاحتفاظ بسجل لأنشطة المعالجة تحت مسئوليته. ويجب أن يتضمن هذا السجل على جميع المعلومات التالية:

- اسم وتفاصيل الاتصال الخاصة بالمتحكم، وعند الاقتضاء، المتحكم المشترك وممثل المتحكم ومسئول حماية البيانات؛
- أغراض المعالجة؛
- وصف لفئات مواضيع البيانات وفئات البيانات الشخصية ؛
- فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم أو سيتم الكشف عنها بما في ذلك المستلمين في دول ثالثة أو المنظمات الدولية؛
- عند الاقتضاء، نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، بما في ذلك تحديد ذلك البلد الثالث أو المنظمة الدولية، وفي حالة عمليات النقل المشار إليها في الفقرة الفرعية الثانية من المادة ٤٩ (١)، وثائق مناسبة الضمانات.
- حيثما أمكن، الحدود الزمنية المتوخاة لمحو مختلف فئات البيانات ؛
- حيثما أمكن، وصف عام للتدابير الأمنية التقنية والتنظيمية المشار إليها في المادة ٣٢/١.
- يجب على كل معالج، وعند الاقتضاء ممثل المعالج، الاحتفاظ بسجل لجميع فئات أنشطة المعالجة المنفذة نيابة عن المتحكم، يحتوي على:
  - اسم وتفاصيل الاتصال الخاصة بالمعالج أو المعالجين ولكل وحدة تحكم يعمل المعالج نيابة عنها، وحيثما أمكن، المتحكم أو ممثل المعالج ومسئول حماية البيانات؛
  - فئات المعالجة المنفذة نيابة عن كل وحدة تحكم؛
  - عند الاقتضاء، نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، بما في ذلك تحديد ذلك البلد الثالث أو المنظمة الدولية، وفي حالة عمليات النقل المشار إليها في الفقرة الفرعية الثانية من المادة ٤٩/١ اللائحة، وثائق مناسبة الضمانات ...."

ى - الحصول على ترخيص أو تصريح من المركز (مركز حماية البيانات الشخصية) للتعامل مع البيانات الشخصية.

ينفرد القانون المصري بهذا الالتزام فلا يوجد نظير له في اللائحة الأوروبية، فلم تشترط الأخيرة ضرورة الحصول على تصريح أو ترخيص مسبق بل اكتفت بوضع معايير وجزاءات لمخالفة هذه المعايير.

ك - يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له فى جمهورية مصر العربية وذلك على النحو الذى تبينه اللائحة التنفيذية.

ومن ثم يتعين على اللائحة التنفيذية تحديد قواعد وضوابط تعيين ممثل المتحكم الذى يقع خارج مصر، حتى يتم التعامل معه من قبل المركز أو الشخص المعنى بالبيانات لأغراض ضمان الامتثال لهذا القانون.

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

تتشابه هذه الفقرة مع مضمون المادة ٢٤ من اللائحة الأوروبية المشار إليها، حيث توضح أن الالتزام الأساسي للمتحكم هو وضع طريقة المعالجة وغرضها طبقا للقانون ويكون هو المسؤل عن توفير الإمكانيات اللازمة لذلك وعن إثبات هذا الإلتزام.

ولكن بخلاف اللائحة الأوروبية لم يتطرق القانون المصري إلى مبدأ التناسب Proportionality[٨٣]. ومبدأ التناسب هو مبدأ عام مهم في قانون الاتحاد الأوروبي بشكل عام لضمان أن مستوى

٨٣ - مبدأ التناسب هو مبدأ عام للائحة الأوروبية يقيد الجهات في ممارسة سلطاتها من خلال مطالبتهم بتحقيق التوازن بين الوسائل المستخدمة والهدف المقصود. وفي سياق الحق في حماية البيانات الشخصية، يبدو التناسب هو التبرير لأي قيود على أي من حقوق أصحاب البيانات. لمزيد من المعلومات فضلا أنظر الموقع الألكتروني لمركز حماية البيانات الأوروبي الآتي:
https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

الحماية يتناسب مع غرض الحماية ولا يؤدي إلى مساوئ قد تفوق الغرض والمزايا المحققة من الحماية.

أشارت ورشة العمل إلى أن المشرع المصري اختار سلوك نهج اللائحة الأوروبية في تفصيل الالتزامات وتشديد شروط عمليات جمع ومعالجة البيانات، وهي مسائل تحتاج حقيقةً إلى إمكانات تقنية ومالية عالية للغاية، فكان يجدر عليه التعرض لمسألة تخفيف أو إعفاء بعض المتحكمين من هذه الشروط والالتزامات، بالنظر إلى أنها من الممكن أن تفوق في الكثير من الأحيان قدرات الشركات الصغيرة والمتوسطة مثلا، الأمر الذي يحتاج إلى مراجعة لذلك.

وهذا ما نصت عليه اللائحة الأوروبية، بجانب مبدأ التناسب، عندما قررت إمكانية إعفاء المؤسسات التي توظف أقل من ٢٥٠ شخص من إمساك سجلات لكل أنشطة المعالجة (م ٣٠ من اللائحة).

وتشير الفقرة قبل الأخيرة من المادة ٤ من قانون حماية البيانات إلى أنه في **حال وجود أكثر من متحكم** يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعنى ممارسة حقوقه تجاه كل متحكم على حدة".

وأخيراً يحيل القانون إلى اللائحة التنفيذية في شأن تحديد السياسات والإجراءات والضوابط والمعايير الفنية لالتزامات المتحكم (المشار إليها في المادة ٤ من القانون).

٢ - التزامات المعالج للبيانات

تنظم المادة ٥ من قانون حماية البيانات الشخصية التزامات المعالج في مجال حماية البيانات، فتنص على جملة من الالتزامات تشبه في العديد منها الالتزامات التي وضعها المشرع الأوروبي في المادة ٢٨ من اللائحة الأوروبية لحماية البيانات GDPR.

فتنص المادة ٥ من قانون حماية البيانات على أن: مع مراعاة أحكام المادة ١٢ من هذا القانون (المعنية بالبيانات الحساسة وحظر إجراء أي عملية عليها إلا بإذن مركز حماية البيانات)، يلتزم المعالج بما يأتي:

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

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

وهو شرط قانونى بديهي، يخضع له المتحكم أيضاً، وكافة أطراف عملية المعالجة، فالتصرفات عموماً لابد من عدم مخالفتها للنظام العام والأداب.

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

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

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

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

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

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

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

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

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

ل - يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذى تبينه اللائحة التنفيذية.

ومن ثم يتعين على اللائحة التنفيذية تحديد قواعد وضوابط تعيين ممثل المعالج الذى يقع خارج مصر، حتى يتم التعامل معه من قبل المركز أو الشخص المعنى بالبيانات لأغراض ضمان الامتثال لهذا القانون.

وتشير الفقرة قبل الأخيرة من المادة ٤ من قانون حماية البيانات إلى أنه في **حال وجود أكثر من متحكم** يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعني ممارسة حقوقه تجاه كل متحكم على حدة".

وفى هذا الشأن يحيل القانون إلى اللائحة التنفيذية فى شأن تحديد السياسات والإجراءات والضوابط والمعايير الفنية لالتزامات المعالج (المشار إليها فى المادة ٥ من القانون).

■ – طبيعة العلاقة بين المعالج والمتحكم:

وفقاً للمادة ١/٢٨ من اللائحة الأوروبية، عند إجراء المعالجة نيابة عن المتحكم، يجب على الأخير اختيار المعالج الذي يوفر ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تجعل المعالجة تلبي متطلبات هذه اللائحة وتضمن حماية حقوق صاحب البيانات.

ويمكن أن تتمثل هذه المعايير في المعرفة المتخصصة لدى المعالج (على سبيل المثال، الخبرة الفنية فيما يتعلق بالتدابير الأمنية وخرق البيانات)؛ موثوقية المعالج؛ موارد المعالج والتزام المعالج بقواعد السلوك المعتمدة أو آلية الاعتماد.

كما تفرض الفقرة الثانية من هذه المادة على المعالج التزاماً بعدم الاستعانة بمعالج آخر دون إذن كتابي مسبق ومحدد من المتحكم، وفى حالة الحصول على إذن كتابي عام، يجب على المعالج إبلاغ المتحكم بأي تغييرات مقصودة تتعلق بإضافة أو استبدال معالجين آخرين، مما يمنح المتحكم الفرصة للاعتراض على هذه التغييرات.

كما تتطلب الفقرة الثالثة من هذه المادة **إبرام عقد للمعالجة بين المتحكم والمعالج أو أي تصرف قانوني آخر** بموجب قانون الاتحاد أو الدول الأعضاء[٨٤]، يحدد موضوع المعالجة ومدتها، وطبيعة وغرض المعالجة، ونوع البيانات الشخصية وفئات أصحاب البيانات والتزامات وحقوق المتحكم[٨٥].

ويجب أن يكون هذا العقد أو التصرف القانونى فى صورة مكتوبة، بما في ذلك الكتابة فى الشكل الإلكترونى (م ٢٨ فقرة ٩ من اللائحة).

ومع ذلك، يجب ألا يكتفي عقد المعالجة بإعادة صياغة أحكام اللائحة الأوروبية لحماية البيانات؛ فيجب أن يتضمن معلومات أكثر تحديدًا وملموسة حول كيفية تلبية المتطلبات ومستوى الأمان المطلوب لمعالجة البيانات الشخصية موضوع عقد المعالجة.

وفى حالة قيام المعالج بإشراك معالج فرعي للقيام بأنشطة معالجة محددة نيابة عن المتحكم، يتم فرض نفس الالتزامات الخاصة بحماية البيانات المنصوص عليها في العقد أو أي تصرف قانوني آخر بين المتحكم والمعالج (على النحو المشار إليه في الفقرة ٣ من هذه المادة) على المعالج الفرعي بناء على عقد أو أي تصرف قانوني آخر بموجب قانون الاتحاد أو الدول الأعضاء، وبخاصة توفير ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تجعل المعالجة تلبي متطلبات هذه اللائحة. وفي حالة إخلال المعالج الفرعي بالوفاء بالتزامات حماية البيانات الخاصة به، يجب أن يظل المعالج الأصلي مسئولاً بصورة كاملة تجاه المتحكم عن أداء التزامات المعالج الفرعي (م ٢٨ فقرة ٤ من اللائحة).

وجدير بالذكر أن القانون المصري لم ينظم مسائل وأحكام المعالج الفرعى أو ما يطلق عليه المعالج من الباطن.

وتتناول المادة ٢٨ فقرة ١٠ من اللائحة حالة مخالفة المعالج لأحكام هذه اللائحة وقيامه بتحديد أغراض ووسائل المعالجة، ففى هذه الحالة يجب اعتبار المعالج بمثابة متحكم فيما يتعلق بهذه المعالجة، وذلك مع عدم الإخلال بالمواد ٨٢ و ٨٣ و ٨٤ من هذه اللائحة.

ومن جهة أخرى تتناول المادة ٢٩ من اللائحة الأوروبية حالة

---

٨٤ – أيضاً يتطلب قانون خصوصية المستهلك في كاليفورنيا أن يتم الكشف عن البيانات الشخصية للمعالج بموجب عقد مكتوب، ولكن يضع القانون المصري واللائحة الأوروبية التزامات مباشرة وتفصيلية على المعالج لا يرتبها القانون في كاليفورنيا على "مقدم الخدمة" بل على "الشركة" فقط.

٨٥ – ووفقاً للمادة ٢٨ فقرة ثالثة من اللائحة الأوروبية، يجب أن ينص هذا العقد أو أي تصرف قانوني آخر، على وجه الخصوص، على أن المعالج:

(أ) يتولى معالجة البيانات الشخصية فقط بناءً على تعليمات موثقة من المتحكم، بما في ذلك ما يتعلق بنقل البيانات الشخصية إلى دولة ثالثة أو منظمة دولية، ما لم يكن ذلك مطلوبًا بموجب قانون الاتحاد أو الدول الأعضاء الذي يخضع له المعالج ؛ وفى هذه الحالة ، يجب على المعالج إبلاغ المتحكم بهذا الشرط القانوني قبل المعالجة، ما لم يحظر هذا القانون هذه المعلومات لأسباب مهمة تتعلق بالمصلحة العامة؛

(ب) التأكد أن الأشخاص المرخص لهم بمعالجة البيانات الشخصية قد التزموا بالسرية أو خضوعهم لالتزام قانوني ملائم للسرية؛

(ج) يتخذ جميع التدابير المطلوبة عملاً بالمادة ٣٢ من اللائحة (الخاصة بأمن المعالجة)؛

(د) يحترم الشروط المشار إليها في الفقرتين ٢ و ٤ لإشراك معالج فرعى؛

(هـ) مراعاة طبيعة المعالجة، ومساعدة المتحكم على اتخاذ التدابير الفنية والتنظيمية المناسبة، بقدر ما يكون ذلك ممكنًا، للوفاء بالتزام المتحكم بالرد على طلبات ممارسة حقوق صاحب البيانات المنصوص عليها في الفصل الثالث؛

(و) يساعد المتحكم في ضمان الامتثال للالتزامات بموجب المواد من ٣٢ إلى ٣٦ مع مراعاة طبيعة المعالجة والمعلومات المتاحة للمعالج؛

(ز) عند اختيار المتحكم، يحذف أو يعيد جميع البيانات الشخصية إلى المتحكم بعد انتهاء تقديم الخدمات المتعلقة بالمعالجة، ويحذف النسخ الموجودة ما لم يشترط قانون الاتحاد أو الدول الأعضاء تخزين البيانات الشخصية؛

(ح) يتيح للمتحكم جميع المعلومات اللازمة لإثبات الامتثال للالتزامات المنصوص عليها في هذه المادة والسماح بعمليات التدقيق والمساهمة فيها، بما في ذلك عمليات التفتيش التي يجريها المتحكم أو أي مراجع آخر يفوضه المتحكم.

المعالجة تحت سلطة المتحكم والمعالج، فأشارت إلى أنه لا يجوز للمعالج وأي شخص يتصرف تحت سلطة المتحكم أو المعالج، وله حق الوصول إلى البيانات الشخصية، أن يقوم بمعالجة تلك البيانات إلا بناء على تعليمات من المتحكم، ما لم يكن مطلوباً بموجب قانون الاتحاد أو الدولة العضو.

وقد أوصت الورشة بأن تكون علاقة المتحكم بالمعالج في القانون المصري بناء على تعليمات تعاقدية واضحة، وأكدت على ضرورة أن تكون في صورة تعاقدية، على أن يفرض ذلك أيضاً على كل متحكم أو معالج من الباطن. ويجب أن تخضع أنشطة معالجة البيانات لعقد أو أي تصرف قانوني آخر مع المتحكم، على أن يحدد العقد موضوع ومدة وغرض المعالجة، وأنواع معالجة البيانات الشخصية والإجراءات الأمنية والتزامات وحقوق المعالج والمتحكم. وعند إنهاء العقد مع المتحكم، يجب على المعالج إعادة البيانات الشخصية أو حذفها، بالإضافة إلى ذلك، إذا أراد المعالج إشراك معالج آخر (معالج فرعي) وجب عليه الحصول على إذن كتابي من المتحكم.

كما أوصت الورشة بأن المبالغة في فرض الالتزامات على جميع القائمين على معالجة البيانات قد يكون غير مناسب حالياً للمجتمع المصري.
كما يجب من جهة أخرى تحديد طبيعة علاقة الشخص المعنى بالبيانات مع الحائز أو المعالج أو المتحكم.

ثانياً

دور مسئول حماية البيانات الشخصية والتزاماته

استحدث قانون حماية البيانات الشخصية مفهوم "مسئول حماية البيانات الشخصية"، وهو الشخص الطبيعي الذي يعني بمباشرة مهام حماية البيانات الشخصية داخل المؤسسة أو الجهة. وقد تناول الفصل الرابع من القانون تنظيم تعيين مسئول حماية البيانات في المادة (٨) وبيان التزاماته في المادة (٩) منه.

وعلى النسق نفسه، تعرضت اللائحة الأوروبية لمسئول حماية البيانات Data protection officer في المبحث الرابع من الفصل الرابع منها، بشئ من التفصيل، فأشارت لمسألة تعيينه Designation of the data protection officer في المادة ٣٧، ووضعه أو مركزه Position of the data protection officer في المادة ٣٨، ومهامه Tasks of the data protection officer في المادة ٣٩ من اللائحة.

وباستقراء تلك المواد والمواد المتعلقة بالعقوبات يتضح لنا بسهولة أن مسئول حماية البيانات هو الجهة المسئولة داخل كل مؤسسة عن تطبيق أحكام القانون، ويتحمل بمعظم المسئوليات في هذا الصدد، وهو ما لم يتوانى القانون عن ذكره.

ولبيان التحديات المتعلقة بمسئول حماية البيانات نناقش التزاماته، وكذلك ظروف تعيينه.

١- تعيين مسئول حماية البيانات

يوجب القانون في المادة (٨) على الممثل القانوني للشخص الاعتباري للمتحكم أو المعالج بأن يعين داخل كيانه القانوني وهيكله الوظيفي موظفاً مختصاً يكون مسئولاً عن حماية البيانات الشخصية، وهو التزام يهدف إلى ضمان مزيد من التنسيق والامتثال لأحكام القانون، وفي ذات الوقت يخدم المتحكم والمعالج ذاتهم بأن يوزع الأدوار ويرفع من على كاهلهم بعض المسئوليات[٨٦].

86 - Giurgiu, Andra, and Gerard Lommel, A New Approach to EU Data Protection: - More Control over Personal Data and Increased Responsibility, KritV, CritQ, RCrit. Kritische Vierteljahresschrift Für Gesetzgebung Und Rechtswissenschaft / Critical Quarterly for Legislation and Law / Revue Critique Trimestrielle De Jurisprudence Et De Législation, vol. 97, no. 1, 2014, p24.

كذلك تلزم المادة ٣٧ من اللائحة الأوروبية لحماية البيانات GDPR، الخاصة بتعيين مسئول حماية البيانات، فى فقرتها الأولى، كل من المتحكم والمعالج بتعيين مسئول حماية البيانات.

وقد أوضحت المادة ٨ من القانون المصري أن عملية التعيين تتطلب توافر شكلية معينة تتمثل في قيد الشخص المعين في سجل مسئولي حماية البيانات الشخصية بالمركز، ثم الإعلان عن ذلك التعيين، وهو ما يعني أن الالتزام بالتعيين لا يسقط بمجرد تعيين المسئول داخليًا في الكيان وإدراجه على قوائم العاملين بها، وإنما يتطلب التعيين كي يقع تامًا وفقًا لتحديد هذه المادة القيد والإعلان.

وقد أحالت المادة (٨) إلى اللائحة التنفيذية في تحديد شروط وإجراءات القيد في سجل مسئولي حماية البيانات في المركز.

ويعد اشتراط الإعلان لإتمام إجراءات تعيين مسئول الحماية منطقيًا في ظل ما أشرنا إليه توًا من أن مسئول الحماية يعتبر حلقة وصل المتحكم أو المعالج مع المعنيين فيما يتعلق بشئون البيانات الشخصية، وهو على الأخص المسئول عن التواصل مع الشخص المعنى بالبيانات، فهو الذي يتلقى منه طلباته ويعمل على تنفيذها، على نحو أشرنا إليه فى الفئة الثانية من التزامات مسئول الحماية.

لذلك فإن الإعلان عن شغل شخص بعينه لموقع مسئول الحماية في الكيان وكذلك وسائل الاتصال به -على ما نحو ستوضحه اللائحة من شروط الإعلان- يخدم وصول المعنيين بالبيانات لمسئول حماية البيانات لدى كل متحكم أو معالج.

واشتراط توافر هذه الإجراءات لإتمام تعيين مسئول الحماية يترتب عليه من ناحية سقوط التزام الممثل القانوني للمتحكم والمعالج كما أوضحنا سلفًا، وهو المعاقب على مخالفته بغرامة تتراوح بين ٢٠٠ ألف و ٢ مليون جنيه. إضافةً إلى ذلك، يترتب على مسألة إتمام إجراءات التعيين بالقيد والإعلان تحديد توقيت بداية مسئولية مسئول حماية البيانات.

ونرى أن التوقيت الذي تبدأ فيه مسئولية الموظف مسئول الحماية يكون عقب الإعلان عن تعيينه، وذلك لاعتبارات مختلفة: فمن ناحية نجد القانون نص صراحةً على أن التعيين لا يكون إلا بالقيد والإعلان، وهو بذلك يقيم قيدًا شكليًا لابد من استيفاءه، وبدونه لا يعتبر في نظر القانون قد تم تعيين مسئول الحماية. ومن ناحية أخرى فإن توقف إعمال الأمر على هذا النحو يضع على المتحكم أو المعالج ضغطًا من الناحية العملية للإسراع في إتمام إجراءات القيد والإعلان كي يسقط عن كاهلهم الكم الهائل من المسئوليات التي نص القانون على أن يتحملها مسئول الحماية.

واشتراط الإعلان كمتمم للإجراءات يتماشى مع التوجه العام للمشرع في أن يخرج العمل للضوء بالإعلان، وهو الحال على سبيل المثال بالنسبة لشهر الشركات في السجل التجاري، إذ لا تكتسب الشركة الشخصية المعنوية إلا من تاريخ شهرها. وعلى صعيد آخر فإن الإعلان يساعد أن يبدأ المسئول مهامه في مواجهة الجمهور بأن يعرف الأخير شخص المسئول عن حماية البيانات، ومن ناحية أخرى يساعد القيد سجل المسئولين في المركز في أن يعرف المركز إلى من سيتوجه بالحديث فيما يتعلق بالتزامات مسئول حماية البيانات التي وقعها القانون.

وفى ظل هذا الوضع نجد أن تعيين مسئول حماية بيانات يحتمل أحد أمرين: إما أن يتم تعيين شخص في الشركة يتفرغ لهذه الوظيفة في الشركة فحسب، أو أن يتم إسناد هذه الوظيفة لشخص غير متفرغ خارج الشركة. ويبدو أن القانون الحالي قد أقصى الفرضية الأخيرة وهى أن يتم تعيين شخص غير متفرغ من خارج الشركة، حيث تنص المادة (٨) على أن "يلتزم الممثل القانوني للشخص الاعتباري... بأن يعين داخل كيانه القانوني وهيكله الوظيفي موظفًا مسئولًا عن حماية البيانات الشخصية...". ويستفاد من ذلك أن المشرع قد حصر التعيين على إلحاق الشخص بالهيكل الوظيفي للمؤسسة أو الجهة وأن يكون "داخل" الكيان القانوني لها، وبالتالي يخرج عن مفهوم التعيين على هذا النحو مجرد إسناد مهام مسئول الحماية لشخص خارج الشركة.

وجاء موقف المشرع المصري مختلفًا عن أحكام اللائحة الأوروبية، حيث تسمح الأخيرة بأن يكون مسئول حماية البيانات تابع لهيئة العاملين في الجهة أو المؤسسة، كما قد يتولى ذلك الموقع بناءً على عقد خدمة، أي دون تفرغ (المادة ٣٧ فقرة ٦ من اللائحة)، حتى أنه من الممكن تعيين مسئول حماية بيانات لأكثر من جهة في ذات الوقت (المادة ٣٧ فقرة ٢ من اللائحة).

ومن الملاحظ في هذا الصدد أن قانون حماية البيانات المصري قد صمت عن ضمانات عمل مسئول حماية البيانات، إذ يفترض أن يتمتع مسئول حماية البيانات بقدر من الاستقلال في ممارسة مهامه، وهو ما يستدعي ألا يتلقى أي توجيهات من مرؤوسيه بخصوص عمله وأن يقوم بوظيفته وفقًا للقانون وتعليمات مركز حماية البيانات فحسب.

وعلة استقلالية مسئول الحماية، المطلوبة، مستمدة من طبيعة دوره؛ إذا أشرنا إلى أنه يعتبر عين المركز داخل الكيان؛ فيفترض به تصحيح المخالفات والإبلاغ عنها وتوجيه الشركة بما يضمن حماية بيانات مستخدميها والتعامل مع طلبات هؤلاء المستخدمين، وكل ذلك لن يستقيم لو كان عمل المسئول مهدد بالتدخل والضغط ممن يرأسه. وقد أشاح القانون المصري بوجهه عن هذه الضمانة الجوهرية، مع العلم بأن مكانها الطبيعي هو القانون وليس اللائحة التنفيذية لأنها

تعكس توجه مشرع وليس مجرد إجراء لتنفيذ القاعدة. بالتالي يصبح الأمر متروكًا لتقدير القضاء عند التطبيق.

كذلك فإن القانون لم يضع أية ضمانات لحماية مسئول حماية البيانات عن الإجراءات التعسفية من المتحكم والمعالج التي قد تعود عليه جراء قيامه بدوره؛ إذ يفترض فيه أثناء قيامه بعمله الالتزام ببعض الاستقلال والحيادية كما ذكرنا، وهو ما يعني إمكانية أن تكون إدارته لملف حماية البيانات ليست بالضرورة مما يسر المتحكم، كما لو قام بإبلاغ المركز عن خرق بغير رضا المتحكم ففي هذه الحالة قد يصبح مهددًا بالفصل على سبيل المثال أو حرمانه من بعض الامتيازات المالية مثلًا[٨٧]، ولا يقيه في ذلك إلا قانون العمل أو قانون الخدمة المدنية بحسب الأحوال، وهو ما لا يتماشى بالضرورة مع دوره الحساس والمختلف عن الموظف أو العامل العادي.

وعلى العكس من ذلك، بالنسبة **للائحة الأوروبية** لحماية البيانات، فقد كان موقفها فيما يتعلق بضمانات مسئول حماية البيانات أكثر إيجابية ووضوحًا، حيث وضعت، فى المادة ٣٨ منها، ضمانات وضوابط لتيسير عمل مسئول حماية البيانات باستقلال عن المتحكم والمعالج، فلا يجوز لهما توجيه أي تعليمات للمسئول عن حماية البيانات فيما يتعلق بممارسة مهام وظيفته، ولا يجوز فصله أو معاقبته من قبل المتحكم أو المعالج عند أداء مهامه، كما تقدم تقاريره لأعلى مستوى إدارة في الجهة أو المؤسسة (م ٣٨ فقرة ٣ من اللائحة).

كذلك، وفقاً للائحة الأوروبية، يجب على المتحكم أو المعالج إطلاع وإشراك مسئول الحماية في المسائل التي تتعلق بحماية البيانات، وأن يكون ذلك بشكل صحيح وفى الوقت المناسب (م ٣٨ فقرة ١ من اللائحة). كما يلزم أن يدعم المتحكم والمعالج مسئول الحماية فى أداء مهامه التي تحددها اللائحة من خلال تزويده بالموارد اللازمة لمزاولته لعمله ومنحه حق الوصول للبيانات الشخصية لديهما وكذلك لعمليات معالجة البيانات، وفوق ذلك على أن يحرصا على الحفاظ على خبرته وتطويرها (م ٣٨ فقرة ٢ من اللائحة).

وفى هذا الصدد، يقع القانون المصري أمام معضلة أخرى تخص الأشخاص الملزمين بتعيين مسئول حماية بيانات شخصية، فالقانون يلزم في المادة (٨) "أي" متحكم أو معالج بتعيين مسئول حماية البيانات. وترتيب الالتزام على هذا النحو قد يكون تعسفيًا وغير ضروري في بعض الأحيان، فالقانون لم يصمت فحسب عن تحديد معايير الجهات الملزمة بتعيين مسئول حماية البيانات، أو حتى ترتيب الالتزام على المتحكمين أو المعالجين في العموم على أن تحدد اللائحة فيما بعد تلك المعايير، بل ذهب إلى تعميم ذلك الالتزام صراحةً على "أي" متحكم أو معالج دون تمييز، وهو ما يعني أنه بما أن كل من يتعامل في البيانات الشخصية سواءً كان شخصًا طبيعيًا أم اعتباريًا يعتبر متحكم أو معالج، فإنه سيصبح بالتالي مطالبًا بتعيين مسئول حماية، أيًا كان حجم نشاطه وطبيعة البيانات الشخصية التي يتعامل فيها.

ولا يخفى ما في ذلك التعميم من تهور، فهناك أنشطة صغيرة الحجم لا تتحمل ميزانياتها وهيكلها تعيين مسئول لحماية البيانات وخاصةً الشركات الناشئة التي قد تجمع بيانات عملائها لأسباب بسيطة للغاية، كمن يجمع أرقام الهواتف لتحديد ميعاد للعميل مثلًا، وبالطبع فإن ذلك مما يتعارض مع توجه الدولة في تشجيع الأنشطة الصغيرة والشركات الناشئة، كما يوجد أيضًا أنشطة تنطوى على جمع بيانات شخصية عادية ولأسباب بسيطة وبكميات صغيرة كذلك، والتي يصير معها الالتزام بتعيين مسئول حماية تزيّد لا داعي له.

وبما أن ذلك الشرط لن يتحمله الواقع العملي وسيصير تعجيزيًا لبعض الأنشطة إذا تم تطبيقه، فقد تتجه اللائحة التنفيذية إلى تجاوز ذلك التعميم بأن تحدد هي من تلقاء ذاتها فئات معينة من الأنشطة التي تخضع للالتزام بتعيين مسئول حماية بيانات، وهي إن أقدمت على تلك الخطوة فإنها ستصبح قابلة للطعن عليه بالإلغاء لمخالفتها للقانون الذي نص – بقدر كافٍ من الوضوح والجزم – على أن الالتزام بتعيين مسئول الحماية ينصرف إلى "أي" متحكم أو معالج، وهو تقييد لما لا يحتمل التقييد.

وبالنظر إلى اللائحة الأوروبية نجد أنها تجنبت هذا الوضع، فى المادة ٣٧ فقرة ١ منها، بأن حددت ثلاث حالات يلتزم فيها المتحكم والمعالج بشكل رئيسي بتعيين مسئول حماية بيانات، وهى:

(أ) إجراء المعالجة من قبل سلطة أو هيئة عامة، باستثناء المحاكم التي تعمل بصفتها القضائية.

(ب) إذا كانت الأنشطة الرئيسية للمتحكم أو المعالج تقتضي رقابة منظمة ومنتظمة للأشخاص المعنية بالبيانات على نطاق واسع.

(ج) إذا كانت الأنشطة الأساسية للمتحكم أو المعالج تنطوي على معالجة على نطاق واسع للبيانات الشخصية، أو معالجة لبيانات حساسة (الأصل العرقي أو المعتقدات الدينية أو السياسية أو البيانات الجينية ..إلخ)، أو بيانات شخصية تتعلق بالأحكام الجنائية والجرائم المشار إليها في المادة ١٠ من اللائحة.

٢ – التزامات مسئول حماية البيانات

تناولت المادة (٩) من القانون الالتزامات الواقعة على مسئول

٨٧ – أشرنا إلى أن المادة ٣٨ فقرة ٣ من اللائحة الأوروبية نصت صراحةً على عدم جواز فصل أو عقاب مسئول الحماية لقيامه بمهام عمله.

حماية البيانات الشخصية، وقامت في هذا الصدد برسم إطار عام وطرح أمثلة خاصة للالتزامات التي يتحملها مسئول حماية البيانات، وهو ما يعني أن تلك الالتزامات المذكورة في المادة (٩) جاءت على سبيل المثال وليس الحصر.

ومما يؤكد وجهة النظر الخاصة بأن مسئول حماية البيانات هو محط المسئولية الرئيسي في المؤسسات والجهات المعنية بالقانون؛ نجد أنه بينما جعل القانون للممثل القانونى للمتحكم والمعالج التزامات بعينها، اعتبر القانون في المقابل مسئول حماية البيانات صاحب الاختصاص العام بحماية البيانات، أي أنه هو من يدخل في جعبته كل عمل يتعلق بحماية البيانات في المؤسسة أو الجهة لا يدخل فى اختصاص أحد.

وقد أجملت المادة (٩) سالفة الذكر في فقرتها الأولى طبيعة التزامات مسئول حماية البيانات في العموم قبل أن تفصل بعضها، فتنص على أن مسئول حماية البيانات هو المسئول عن تنفيذ أحكام القانون وقرارات المركز، ومراقبة الإجراءات المعمول بها داخل كيانه والإشراف عليها[٨٨]، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقًا لأحكام القانون.

وقد أحال القانون للائحة التنفيذية لتحديد المزيد من الالتزامات التي قد تقع على مسئول حماية البيانات وبطبيعة الحال الإجراءات اللازمة للقيام بهذه المهام.

وبالنظر إلى الأمثلة التي ساقها القانون لالتزامات مسئول حماية البيانات، نجد أنها قد انصرفت إلى ثلاثة فئات بحسب الجهة المعنية بالالتزام؛ فهناك التزامات داخلية، والتزامات في مواجهة الشخص المعنى بالبيانات، وأخرى في مواجهة المركز.

وقد أوصت الورشة بضرورة بيان وتوضيح الدور المحوري لمسئول حماية البيانات و إيضاح حدود مسئولياته وطبيعة تبعيته الإدارية لما في توضيح ذلك من أثر على فاعلية دورة وقدرته على القيام به بشكل فعال. والتأكيد عن استقلاله عن المؤسسة أو الشركة في حدد ما بينه هذا القانون.

أ – الالتزامات الداخلية لمسئول حماية البيانات:

يلتزم مسئول حماية البيانات داخل كيانه بتقييم وفحص نظم حماية البيانات الشخصية، وهو أحد الالتزامات الجوهرية التي ينصب عليها عمل مسئول الحماية، بيد أن الالتزام بصيانة أنظمة الحماية هو وظيفة تقنية معقدة، وهو ما يجعل أحد الشروط الواجب توافرها فيمن يشغل هذا الموقع هو أن يكون على دراية فنية احترافية بمجال حماية تكنولوجيا المعلومات بالإضافة إلى اطلاعه على قانون حماية البيانات وأحكامه. والفقرة الأولى من المادة (٩) إذ هي تمعن أكثر وتوجب عليه "منع اختراق" نظم حماية البيانات الشخصية، وهو على ما نرى التزام ببذل عناية وليس التزامًا بتحقيق نتيجة، ذلك أنه من الصعب ضمان الحماية الكاملة حتى بالنسبة للمحترفين، وذلك للتطور المستمر في وسائل الاختراق كما هو الأمر بالنسبة لأنظمة الحماية.

ومن جهة أخرى، بموجب البند السادس من ذات المادة، يُحمِّل القانون مسئول الحماية الالتزام بالإشراف على سجلات البيانات والمعالجة بأن يقوم بمتابعة عمليات القيد والتحديث لسجل البيانات الشخصية إذا كان يعمل لدى متحكم، ولسجل عمليات المعالجة إذا كان يعمل لدى معالج وهو التزام منطقي متماشٍ مع دور مسئول البيانات الطبيعي.

ويزيد على ذلك أن المشرع قد أحسن اختيار وصف الالتزام، فهو ينص على أن يقوم المسئول بـ"متابعة" القيد والتحديث لسجل البيانات الشخصية أو سجل عمليات المعالجة، عوضًا عن أن يصفه بأنه التزام ب "قيد وتحديث" هذه السجلات مباشرةً. وذلك يعني تخفيف عبء المسئولية على مسئول الحماية ووضعها في مكانها الصحيح، فدور مسئول الحماية ليس القيام بالعمليات مباشرةً وبنفسه كما يصفه القانون في معظم المواضع، وإنما أن يقوم بالإشراف والتوجيه والمتابعة ويعاونه في ذلك المتحكم والمعالج بتوفير الإمكانيات والاستجابة لتوجيهاته، كما يعاونه فريق عمل يتسع أو يضيق بحسب حجم نشاط المنشأة، لهذا كان من الطبيعي أن يكون التزامه منصبًا على المتابعة فحسب.

واتجهت اللائحة الأوروبية لحماية البيانات (GDPR) ذات النهج في اختيار الألفاظ، فمسئول حماية البيانات وفقًا للمادة (٣٩ فقرة ١/ب) يلتزم بـ"الرقابة" على امتثال الجهة أو المؤسسة للائحة، ولم تُلقي على عاتقه المسئولية عن امتثالهم لها. كما يجب أن يراعي مسئول حماية البيانات في أداء مهامه المخاطر المرتبطة بعمليات المعالجة، مع الأخذ في الاعتبار طبيعة المعالجة ونطاقها وسياقها وأغراضها (٣٩ فقرة ٢). كما يلتزم أيضاً بالسرية فيما يتعلق بأداء مهامه، وفقاً لقانون الاتحاد أو الدول الأعضاء (م ٥/٣٨ من اللائحة)

ويلاحظ على صعيد آخر أن المشرع المصري قد أخضع عمليات المتابعة والتحديث المشار إليها لتحديد قد يقع محل انتقاد، فهو يقصر الالتزام بمتابعة القيد والتحديث على سجل البيانات الشخصية لدى المتحكم، ويقصره بالنسبة للمعالج على سجل المعالجة (م ٩ بند ٦ من القانون) [٨٩]، وهو ما يثير

٨٨ – يُلاحظ وجود خطأ في الصياغة في نص الفقرة الأولى من المادة ٩ من القانون، إذ يجرى على أن: "ومراقبة الإجراءات المعمول بها داخل كيانه الإشراف عليها"، وغالب الظن أن المشرع قصد عطف الإشراف على المراقبة لكنه نسي سهوًا أن يضع الواو.

٨٩ – تنص المادة (٩) بند (٦) من القانون على أن: يلتزم بـ"متابعة القيد والتحديث لسجل البيانات الشخصية لدى المتحكم أو سجل عمليات المعالجة لدى المعالج...".

التساؤل حول دور كل منهما وكذلك مفهوم المعالج ذاته.

فالنص على ذلك النحو يفترض أن المتحكم لن يقوم بعمليات معالجة وهو على ذلك ليس بحاجة لأن يمسك لها سجلًا خاصًا، بالرغم من أن ذلك لا يتفق بالضرورة مع دور المتحكم، الذي يستطيع أن يقوم بعمليات معالجة متعددة سواء استعان فى عمله بمعالج مستقل أم لا، وهو قد يقوم بجميع عمليات المعالجة بنفسه، ولا يؤثر ذلك على وصفه كمتحكم، فمعيار تحديد المتحكم هو أن يكون الشخص الذي يحدد طريقة وأغراض استعمال البيانات، كما أنه هو من يتسلم البيانات من الشخص المعنى بالبيانات في معظم الأحيان، فإذا توافر ذلك فيه أصبح متحكمًا ولو قام بعمليات المعالجة[٩٠].

وبالمثل يفترض المشرع أن المعالج لن يحتفظ ببيانات، وهو بالتالي ليس بحاجة إلى سجل لهذه البيانات، وهو أمر ليس بالضرورة صحيحًا، فعمليات المعالجة التي يقوم بها المعالج قد تتطلب أن يحتفظ بالبيانات الشخصية لقدر من الوقت، ذلك بالإضافة إلى أن مفهوم المعالج ذاته يفترض أنه يتحصل على بيانات شخصية وأنها تصبح تحت تصرفه لمدة طالت أم قصرت، إلا إذا كان مجرد قناة لنقل البيانات (mere conduit)، فهنا يقتصر تصميم عملياته على تمرير البيانات دون وقوفها عنده[٩١]. وبناءً على هذا النص نواجه فرضين: الأول هو عدم الاحتفاظ بهذه السجلات والثانى هو الاحتفاظ بها، لكن لن ينصب عليها التزام مسئول الحماية بالمتابعة، وهو الأصعب تصورًا.

وحتى إن تداركت اللائحة التنفيذية ذلك السهو بأن أضافت من الإجراءات ما يجعل المتحكم يسجل عمليات المعالجة التي يقوم بها، وكذلك جعلت المعالج يمسك سجلًا للبيانات الشخصية التي يعالجها، فإن التزام مسئول حماية البيانات بالمتابعة لن يمتد لهما تلقائيًا؛ حيث أنه -كما أوضحنا للتو- مقتصرًا على سجل البيانات لدى المتحكم، وسجل المعالجة لدى المعالج وفقًا للمادة ٩ من القانون.

وبالتالي فإن اللائحة في سبيل ذلك سيتوجب عليها مخاطبة مسئول الحماية مباشرةً بمتابعة القيد والتحديث بالنسبة لما قد تستحدثه من سجل بيانات لدى المعالج وسجل معالجة لدى المتحكم، وقد تستند اللائحة في مد التزام المسئول لهذين السجلين غير المنصوص عليهما في القانون إلى التزامه العام بتنفيذ القانون وتطبيق أحكامه الوارد في المادتين(٨) و(٩)، بحيث يتأكد الرأي السابق بأن مسئول حماية البيانات هو صاحب النطاق العام للمسئولية تحت هذا القانون.

ووفقًا للبند السابع من المادة (٩) من القانون يلتزم مسئول حماية البيانات بإزالة "أي" مخالفات متعلقة بالبيانات داخل كيانه، واتخاذ الإجراءات التصحيحية حيالها، ويعد هذا الالتزام لاحقًا على وقوع المخالفة، وهو يقابل الالتزام العام باتخاذ التدابير الوقائية وتعزيز أنظمة الحماية.

ويلاحظ أن استخدام المشرع لعبارة الالتزام بإزالة "أي" مخالفات هو مما فضل فيه المشرع التوسع والتعميم والذي قد لا يستقيم والواقع، فذلك الالتزام الشامل بإزالة أي مخالفات يفترض من ناحية أن مسئول حماية البيانات هو الشخص القائم على جميع عمليات المعالجة في الكيان التابع له، ومن ناحية أخرى أنه يملك السلطة للتعديل من تلقاء ذاته أو توجيه المسئولين عن المعالجة للتعديل والتصحيح وانصياعهم له بالضرورة.

والوضع ليس بالضرورة كذلك، أو هو بالأحرى ليس كذلك؛ فدور مسئول حماية البيانات لن يمتد ليشمل توجيه كل عمليات البيانات الشخصية، بل يقتصر في كثير من الأحيان على مجرد إخطار المسئول عن تحديد عمليات المعالجة برأيه دون أن يقدم على ذلك بنفسه، وينعكس هذا التحديد للأدوار على العقوبات أيضًا إذ يساعد في معرفة متى يُسأل مسئول حماية البيانات مع المتحكم أوالمعالج ومتى يسأل كل منهم على حدة[٩٢].

وفي البند الثامن من المادة (٩) من القانون يلتزم مسئول الحماية بتنظيم البرامج التدريبية اللازمة لموظفي الكيان التابع له، بحيث يتم تأهيلهم لتطبيق القانون والامتثال له، وهو مما يكفل توفيق أسرع للأوضاع[٩٣]؛ حيث إن مختلف التخصصات المتعاملة في البيانات الشخصية في الكيان ذاته، مثل مسئولي الموارد البشرية وتكنولوجيا المعلومات، ينبغي عليهم استيعاب التغييرات التي جاء بها القانون.

ب - الالتزامات في مواجهة الشخص المعنى بالبيانات:

أما الفئة الثانية من الالتزامات فهي تلك الواقعة في مواجهة الشخص المعنى بالبيانات، ووفقًا للمادة (٩) من القانون يكون مسئول حماية البيانات هو الملتزم بتمكين الشخص المعنى بالبيانات من ممارسة حقوقه المنصوص عليها في القانون. وذلك يعني أن مسئول الحماية هو قناة الشخص المعنى بالبيانات للعلم سواءً بالبيانات التى تم تجميعها لدى الكيان أو الانتهاكات الواقعة على هذه البيانات، كما أنه المسئول عن

٩٠ - ذلك بالإضافة إلا أنه وفقًا لمفهوم المعالجة، فإن كل من يتعامل في البيانات يقوم بعملية معالجة أيًا كان شكل هذا التعامل، فجمع البيانات ونقل والاحتفاظ بها وتعديلها وحذفها هو مما يدخل في مفهوم المعالجة، وبالتالي ففكرة المعالجة تلك ليست قاصرة على المعالج كما يتعامل معها القانون في عدة مواضع.

91 - See the Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 1.0, issued by the European Data Protection Board, adopted on 02 September 2020.

٩٢ - ذلك بالإضافة إلا أنه وفقًا لمفهوم المعالجة، فإن كل من يتعامل في البيانات يقوم بعملية معالجة أيًا كان شكل هذا التعامل، فجمع البيانات ونقل والاحتفاظ بها وتعديلها وحذفها هو مما يدخل في مفهوم المعالجة، وبالتالي ففكرة المعالجة تلك ليست قاصرة على المعالج كما يتعامل معها القانون في عدة مواضع.

93 - EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, IT Governance Privacy Team, 2nd edition, 2017, p25.

تلقي وتنفيذ طلباته المتعلقة ببياناته الشخصية سواءً كانت بالتعديل أو الحذف وتوجيه عمليات المعالجة في العموم.

وفى هذا الصدد، تجيز المادة ٤/٣٨ من اللائحة الأوروبية لأصحاب البيانات الاتصال بمسئول حماية البيانات فيما يتعلق بجميع القضايا المتعلقة بمعالجة بياناتهم الشخصية وممارسة حقوقهم بموجب هذه اللائحة.

ج - الالتزامات في مواجهة مركز حماية البيانات:

تأتي أخيرًا فئة الالتزامات في مواجهة مركز حماية البيانات، والتي تتمثل فى أن يكون مسئول حماية البيانات بمثابة نقطة اتصال مباشرة مع المركز، والرد على التظلمات الواردة إليه من خلال المركز[٩٤]، وإخطاره في حالة وجود أي خرق أو انتهاك للبيانات، كما تشمل أن يقوم مسئول الحماية بتنفيذ قرارات المركز المتعلقة بأحكام القانون.

وقد اكتفت اللائحة الأوروبية هنا بأن تسند إلى مسئول حماية البيانات مهمة التعاون مع السلطة الرقابية supervisory authority (م ٣٩ فقرة ١/ هـ)، وكذلك أن يعمل كقناة اتصال بين هذه السلطة والمتحكم والمعالج فيما يخص معالجة البيانات الشخصية (م ٣٩ فقرة ١/ هـ).

وبقراءة النصوص المنظمة لعمله في القانون المصري، يمكن القول إنه حلقة الوصل بين المركز والمتحكم أو المعالج، وبينهما والأشخاص المعنيين بالبيانات، أيضًا يمكن القول إن مسئول حماية البيانات سيكون عملًا "المسئول" الأول عن تطبيق القانون، كذلك من الجائز إجمال دوره في أنه عين المركز وأداته في الشركات، وإن كان تابعًا للشركة ويتقاضى راتبه منها.

ويخشى في ظل هذا التنظيم أن يتحول مسئول حماية البيانات إلى كبش فداء فنطاق مسئولياته ضخم للغاية؛ فهو مسئول عن "تنفيذ القانون" وليس الإشراف على تنفيذه، وهو ما تم التأكيد عليه في المادتين (٨) و (٩) معًا. وفي المقابل لا يوجد في القانون ما يلزم الشخص المتحكم أو المعالج بتوفير الإمكانيات اللازمة لعمل مسئول حماية البيانات ولا يوجد ما يلزمهم بأن يلتزموا بتوجيهاته.

وذلك التوجه ينعكس كذلك في الجزاء، فالجزاء الموقع عليه - وهو شخص طبيعي- ضخم للغاية، ويوازي ما يوقع على المتحكم أو المعالج وهم مؤسسات، كذلك فهو إن أضاع ورقة أو لم يجب على بريد من المركز أو الشخص المعنى بالبيانات يصبح في خرق لالتزاماته وفقًا للمادة (٩) وبالتالي يستحق العقاب المقرر في المادة (٤٠)، فيعاقب بغرامة من ٢٠٠ ألف جنيه إلى ٢ مليون جنيه. وحتى وإن كانت الغرامة في حالة الإهمال أقل من ذلك، فهي تتراوح بين ٥٠ ألف إلى ٥٠٠ فإن ذلك لا يزال كثيرًا بل وتعجيزي بالنسبة للبعض، وخاصةً فيما أشرنا إليه سابقًا من أن هناك أنشطة صغيرة يصعب عليها تعيين مسئول حماية البيانات من الأساس، فإذا ما تم تعيينه فإن راتبه لن يكفي لتغطية الخطر الذي تحتمله الوظيفة.

وقد أوصت الورشة بضرورة ضبط التزامات مسئول حماية البيانات لما يترتب علي الإخلال بها من عقوبات قاسية.

٩٤ - جدير بالذكر أنه لا يتصور عملاً أن يصدر عن المركز ذاته تظلمات، وإنما غالب الظن أن البند ٥ من المادة ٩ عندما تتحدث عن التظلمات التي يقدمها المركز إنما تقصد التظلمات التي يقدمها المعنيون بالبيانات ويقوم هو بتمريرها لمسئول حماية البيانات في الكيان المعني.

المحور الرابع

وسائل إنفاذ قانون
حماية البيانات الشخصية

■ تمهيد:

يعتبر قانون حماية البيانات الشخصية هو التجربة التشريعية الأولى في نطاق خصوصية البيانات الشخصية في مصر، وبما أنه في مهده، فمن المتوقع أن يشهد تطبيق هذا القانون العديد من التحديات، خاصةً مع استحداثه لمفاهيم وأدوار جديدة على سوق البيانات المصري.

ومن بين هذه التحديات هو تناول ورؤية المشرع ذاته لدور الأدوات التنفيذية للقانون، فالقانون الجديد قد سار على نهج التشريعات المقارنة بأن استحدث سلطة رقابية في صورة هيئة عامة تقوم على الإشراف على تطبيق القانون ومنحها في سبيل ذلك العديد من الصلاحيات.

ولضمان إنفاذ أكثر فعالية فقد نص كذلك على التزام المتحكمين والمعالجين بتعيين شخصًا يصبح مسئولًا عن حماية البيانات داخل الكيان ذاته، وحمله بمسئوليات عدة.

ولم يغفل المشرع أيضًا عن استخدام الأداة العقابية لكفالة الامتثال لأحكامه، فأفرد الفصل الرابع عشر للجرائم والعقوبات، وقام فيه بمواجهة الأشخاص الخاضعين للقانون بعقوبات أغلبها الغرامات وبعضها الحبس.

ونتناول هذه المسائل على النحو التالي:

أولاً- دور مركز حماية البيانات الشخصية.

ثانياً- الإطار العقابي لقانون حماية البيانات الشخصية.

أولاً

دور مركز حماية البيانات الشخصية

ساير القانون المصري ما جرى عليه العمل في قوانين حماية البيانات الشخصية حول العالم بإنشاء هيئة تشرف على تطبيق هذه القوانين، فنص القانون المصري على إنشاء مركز أطلق عليه تسمية "مركز حماية البيانات الشخصية"[٩٥]، ونظم عمله في الفصل التاسع، بموجب المواد من (١٩ إلى ٢٥)، ليكون قبلة المتعاملين في البيانات الشخصية، وهو ما زال فى طور التأسيس.

وتتنوع الأدوار التي خولها القانون للمركزبحيث يمكن القول بأنه سيكون الفاعل الرئيسي في ساحة حماية البيانات الشخصية المصرية[٩٦]، وبشكل عام فإن المركز سيضطلع بمهام تتعلق برسم السياسة العامة الخاصة بحماية البيانات وتوجيه المتعاملين فيها وإعطائهم التعليمات اللازمة لذلك. وترتيباً على ذلك فقد خوله القانون إصدار التصاريح والتراخيص والاعتمادات، وهم بمثابة الإجازة التي يتوجب على كل من يستدعي نشاطه العمل في البيانات الشخصية الحصول عليها، ولضمان فعالية أكثر فقد خوله القانون كذلك سلطة توقيع بعض الجزاءات الإدارية على من يتخلف عن الامتثال للتعليمات.

ويعتبر مركز حماية البيانات الشخصية هيئة عامة اقتصادية ومن ثم يخضع لتنظيم قانون الهيئات العامة رقم ٦١ لسنة ١٩٦٣ فيما لم يرد فى شأنه نص في قانون حماية البيانات الشخصية (باعتباره قانونًا خاصًا)، ويكون مقره الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، ويتتبع الوزير المختص، وهو وزير الاتصالات وتكنولوجيا المعلومات، وحدد القانون مهمته في حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها (م ١٩ من القانون).

وتضيف المادة ١/٥١ من اللائحة الأوروبية على ذلك أن من أهداف المركز هو تسهيل تداول البيانات عبر الاتحاد الأوروبي، وهو ما يعني أنه على السلطة الرقابية supervisory authority - كما اسمتها اللائحة - احترام اعتبارين معًا في الوقت ذاته هما: حماية البيانات من ناحية وتيسير التداول الحر للبيانات داخل الاتحاد من ناحية أخرى.

وقد أوصت الورشة أن يكون هناك دوراً واضحاً لمركز حماية البيانات حتى يتمكن من القيام بدوره المزمع وفقاً لرؤية المشرع.

هذا وقد تنوعت الاختصاصات التي يفترض اضطلاع المركز بها، بين ما يمكن تقسيمه إلى أدوار استشارية، وأخرى رقابية، مواجهًا في سبيل ذلك بعض التحديات، وهو ما نتناوله فيما يلى:

١- الدور التوجيهي والاستشاري لمركز حماية البيانات الشخصية:

أناط القانون بالمركز مهمة رسم الملامح العامة لخريطة حماية البيانات الشخصية في مصر، في ظل القانون واللائحة المزعم إصدارها، لذلك نجد المادة (١٩) تنص على أن المركز هو الجهة المخولة بوضع وتطوير السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية والقيام على تنفيذها. وكذلك يتولى توحيد سياسات وخطط حماية ومعالجة البيانات الشخصية داخل الجمهورية. كما أن المركز سيقوم إعمالًا لدوره الارشادي بوضع إطار إرشادي لمدونات السلوك الخاصة بحماية البيانات الشخصية بالجهات المختلفة، وهو ما يعني أن يقوم المركز إما برسم الخطوط العريضة التي تتبعها الجهات المعنية في وضع مدونات سلوكها، أو أن يضع المركز مدونات سلوك قياسية يقتدى بها مباشرةً[٩٧].

وعملاً على اطلاع الجهات المعنية بالبيانات الشخصية بشكل دائم على آخر المستجدات في مجال حماية البيانات الشخصية ونظم وإجراءات الحماية، خصوصًا مع كون هذا المجال في تطور مستمر استجابةً للتطورات التكنولوجية، يتولى المركز إصدار الدوريات الخاصة بتحديث إجراءات الحماية بما يتوافق مع أنشطة القطاعات المختلفة، كما ينقل رؤيته وتوجيهاته عبر إصدار توصياته في هذا الصدد.

كذلك، وفقاً للمادة ١٩ من القانون، يعني المركز بمهمة دعم جهود تطوير كفاءة الأشخاص المفترض بهم القيام على حماية البيانات الشخصية في جميع الجهات الحكومية وغير الحكومية، وهو ما يدلل على دور المركز في تمهيد

٩٥ - منى الأشقر، محمود جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى، ٢٠١٨، ص ١٥١.

٩٦ - حددت المادة الأولى من قانون حماية البيانات الشخصية الخاصة بالتعريفات المقصود بـ "المركز" بأنه "مركز حماية البيانات الشخصية".

٩٧ - يكون للسلطة الرقابية في الأنظمة المقارنة اختصاصات تدور بين التحقيق في المخالفات، وسلطة التنظيم، وكذلك سلطة إنزال العقاب؛ أنظر منى الأشقر، محمود جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، مرجع سابق، ص ١٥٧.

بيئة البيانات الشخصية في مصر لاستقبال القانون الجديد والتغيرات التي يقتضيها، ويشير القانون في هذا السبيل إلى قيام المركز بتنظيم المؤتمرات وورش العمل والدورات التدريبية والتثقيفية، وإصدار المطبوعات بغرض نشر الوعي والتثقيف للأفراد والجهات حول حقوقهم فيما يتعلق بالتعامل على البيانات الشخصية.

وإجمالًا يضطلع مركز حماية البيانات الشخصية بمهمة تقديم جميع أنواع الخبرة والاستشارات المتعلقة بحماية البيانات الشخصية، وهو ما يعضد من دور المركز الاستشاري والتوعوي بالنسبة للأشخاص والمؤسسات على السواء، سواء أكان ذلك في مصر أو في الخارج.

بالإضافة إلى ذلك، يصبح المركز والعاملين فيه بمثابة الخبير في المسائل المتعلقة بالبيانات الشخصية في حالات التحقيق والجهات القضائية، فيتم الاستعانة بهم كخبراء في مسائل حماية البينات الشخصية سواءً كانت تلك الإجراءات تضطلع بها النيابة العامة أو المحكمة الاقتصادية أو غيرها من جهات القضاء، العادي منها والإداري، كما القضاء العسكري والدستوري والنيابة الإدارية.

واتصالًا بدوره في رسم السياسات المتعلقة بحماية البيانات الشخصية، يقوم المركز أيضًا بالتنسيق والتعاون مع جميع الجهات والأجهزة الحكومية وغير الحكومية في إجراءات حماية البيانات الشخصية، ولا يقتصر هذا الدور على مجرد التواصل والتنسيق التقليدي مع الشركات والمؤسسات التي تتعامل في البيانات؛ المتحكمين أو المعالجين التقليديين.

إذ تمتد هذه الفقرة لتشمل التنسيق على مستوى الجهات التي قد يكون لها تأثير على امتثال غيرها من الجهات، والجهات المعنية بمجال حماية البينات الشخصية ذاته وكذلك الأجهزة والجهات الكبرى كانت حكومية أو غير حكومية. وهذا ما أوصت به ورشة العمل.

وفي السياق نفسه، يعطي القانون للمركز الحق في إبرام الاتفاقيات ومذكرات التفاهم والتنسيق والتعاون وتبادل الخبرات مع الجهات الدولية التي يتصل نشاطها بعمل المركز، وهو ما يعزز خبرات المركز إذا تم تفعيله. فالمركز والقانون من الأساس يعتبران متأخرين بعض الشيء إذا ما قورنا بالوضع في الأنظمة المقارنة، لذا فالتعاون مع الجهات الدولية والاستفادة من الخبرات السابقة سيساهم في تطور أسرع للمركز وللممارسات حماية البيانات الشخصية. ذلك مما تؤيده المادة ٢٥ أيضًا، إذ تؤسس للتعاون والتنسيق وتبادل البيانات والمعلومات مع السلطات المختصة في البلاد الأجنبية في سياقات مختلفة[٩٨].

٢- الدور الرقابي لمركز حماية البيانات الشخصية

إن أحد الدعائم الرئيسية لحماية البيانات الشخصية وفقًا للإطار الذي رسمه القانون الجديد هو الدور الرقابي لمركز حماية البيانات الشخصية، فالمركز يفترض فيه أن يكون الذراع التقني للقانون، بما يشمله ذلك من الرقابة على تطبيق القانون وبحث امتثال الجهات المعنية لأحكامه. وعلى ذلك، فقد انعكست تلك الفلسفة في الدور الرقابي الذي اسكنه القانون المركز، والأدوات التي يملكها في سبيل ذلك.

وتحدد المادة (١٩) من القانون أن أحد مهام المركز الهامة، هي القيام على تنفيذ السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات، والتي يضطلع هو ذاته بوضعها. وقد منح القانون المركز اختصاصًا عامًا للمركز حينما نص في المادة المذكورة على قيام المركز على تطبيق أحكام هذا القانون، كما أن للمركز في هذا الصدد سلطة إجازة العديد من الأنشطة وفقًا للقانون، فهو من بيده اعتماد الجهات والأفراد الذين يعتزمون تقديم الاستشارات في إجراءات حماية البيانات الشخصية، كما أنه هو الجهة المعنية بإصدار التراخيص والتصاريح والموافقة المتعلقة بحماية البيانات. وبخلاف ذلك فهو الجهة المنوط بها اعتماد مدونات السلوك الخاصة بالجهات المختلفة.

وهذا يعني أن المركز هو المتحكم عملًا في مزاولة كافة الأنشطة المتعلقة بالبيانات؛ فهو من يرخص للمتحكمين والمعالجين، ومن ناحية أخرى هو من يقرر مدى كفاءة الشخص أو الجهة التي تنوي تقديم الاستشارات في هذا المجال. فهو يراقب مدى انطباق أحكام القانون واللائحة وأحكامه على المعنيين، ومن ثم مدى استحقاقهم للحصول على الترخيص او التصريح اللازم لمزاولة النشاط للمرة الأولى، أو للاستمرار في مباشرته.

٩٨ - تنص المادة ٢٥ من قانون حماية البيانات الشخصية على أن: "للمركز بالتنسيق مع السلطات المختصة التعاون مع نظرائة بالبلاد الجنبية وذلك في إطار اتفاقيات التعاون الدولية والإقليمية والثنائية أو بروتوكولات التعاون المصدق عليها أو تطبيقًا لمبدأ المعاملة بالمثل بما من شأنه حماية البيانات الشخصية والتحقق من مدى الامتثال للقانون من قبل المتحكمين والمعالجين خارج الجمهورية، ويعمل المركز على تبادل البيانات والمعلومات بما من شأنه أن يكفل حماية البيانات الشخصية وعدم انتهاكها والمساعدة في التحقيق في الانتهاكات والجرائم ذات الصلة وتتبع مرتكبيها" .

وقد تعرضت النقاشات أثناء الورشة للسلطات القانونية التي يتمتع بها المركز حيث نجملها فيما يلى:

- السلطات اللائحية (مادة٢١): وضع قواعد عامة ومجردة يلزم بها جميع المتحكمين والمعالجين للبيانات.
- يصدر قرارات فردية (تراخيص - تصاريح - اعتماد).
- عقوبات إدارية على المتحكمين والمشغلين: وقف التراخيص جزئيا او كليا أو سحبها
- أخطر ما في العقوبات: إخضاع المتحكمين للإشراف الفني للمركز(مادة ٣١): يعني أن للمركز توجيه المتحكم بشكل مباشر لتنفيذ بعض الاشتراطات التي أخل بها.
- الغرامات المالية: ليست عقوبات إدارية وانما جنائية في هذا القانون ومخالف للائحة الأوروبية.

وتماشيًا مع هذه الدور، يقوم المركز أيضًا بتلقي الشكاوى والبلاغات المتعلقة بأحكام القانون، كما يملك فوق ذلك أن يصدر القرارات التي تتراءى له بصدد هذه الشكاوى والبلاغات، وقد دعم القانون ذلك بأن نص صراحةً حق المركز في الرقابة والتفتيش على المخاطبين بأحكام القانون واتخاذ الإجراءات القانونية اللازمة في مواجهتهم (م ١٩ من القانون).

وتتجلى سلطة المركز الرقابية كأوضح ما يكون في الأدوات التي منحه القانون إياها، فبخلاف الجزاءات المدنية والجنائية، ينص القانون على مجموعة من الجزاءات الإدارية التي يستطيع المركز توقيعها على المخالفين، والتي قد تصل إلى حد وقف نشاط الجهة المخالفة تمامًا، وفى هذا الصدد تقضي المادة (٣٠) أنه في حالة عدم امتثال المخالف للإنذار الموجه له بإزالة المخالفة وأسبابها أو آثارها خلال الفترة المحددة له بذلك، كان لمجلس إدارة المركز أن يصدر قراراً مسبباً بتوقيع الجزاءات التالية:

١- الإنذار بإيقاف الترخيص أو التصريح أو الاعتماد جزئيًا أو كليًا لمدة محددة.

٢- إيقاف الترخيص او التصريح أو الاعتماد جزئيًا أو كليًا. (الإيقاف قد يكون مؤقتًا، فقد يتم وقف الترخيص أو التصريح أو الاعتماد لمدة معينة من مدتهم الأصلية).

٣- سحب الترخيص أو التصريح أو الاعتماد أو إلغاؤه جزئيًا أو كليًا. (ونظرًا لجسامة جزاء إلغاء الترخيص أو التصريح أو الاعتماد فقط حدد القانون في المادة (٢٩) حالات محددة يقتصر عليها)[٩٩].

٤- نشر بيان بالمخالفات التي ثبت وقوعها في وسيلة إعلام أو أكثر واسعة الانتشار على نفقة المخالف.

وهذا قد يكبد المخالف خسائر فادحة، فهو يمس مباشرةً بسمعة المخالف، وتحديدًا معايير خصوصية بيانات المستخدمين لديه، ومدى أمانته عليها، فحتى وإن كان ذلك جزاءً تابعًا لإلغاء الترخيص أو التصريح أو الاعتماد بشكل كلي، فالشركات التي تمارس أكثر من نشاط ليس منها ما سيتضرر مباشرةً بهذا الإلغاء ستتأثر به سمعتها في العموم، وستتأثر بالتأكيد إذا كانت مؤسسة أو شركة متعددة الجنسيات، حيث سيطال نشر المخالفة من سمعتها في الدول الأخرى التي تمارس فيها نشاطها. ولا حاجة للإشارة لمدى حساسية مسألة خصوصية البيانات ليس فقط بالنسبة للمستخدمين بل والجهات الحكومية والشركاء.

٥- إخضاع المتحكم أو المعالج للإشراف الفني للمركز لتأمين حماية البيانات الشخصية على نفقتهما بحسب الأحوال.

ويُلاحظ هنا مدى قوة هذه التدابير التي يملكها المركز، فهي قد تصل لحد إيقاف أو سحب الترخيص أو التصريح من المخالف وهو ما قد يعني وقف نشاط الجهة المخالفة بصورة كلية. وذلك يعضد النظر بأن القانون قد أناط المركز بالتحكم في المعاملات المعنية بالبيانات الشخصية ومصير المخالفين على السواء، وهو ما يتماشى مع الاتجاه الأوروبي.

بيد أنه من الملاحظ أنه على خلاف معظم القوانين المقارنة، لم يعط القانون المركز سلطة توقيع أية جزاءات مالية على الخارجين على القانون. فالغرامات التي نصت عليها اللائحة العامة لحماية البيانات منوط بها الهيئات الرقابية وليس القضاء، وهي قد تصل إلى ٢٠ مليون يورو أو ٤٪ من إجمالي دخل المخالف.

ومن ثم فإن الغرامات المنصوص عليها في هذه القوانين هي غرامات إدراية، إلا أن نظيرتها في القانون المصري تعتبر غرامات جنائية، يختص بها القضاء وحده ممثلًا في المحكمة الاقتصادية بحسبما نص عليه القانون.

يضاف إلى الجزاءات الإدارية أن القانون قد منح العاملين بالمركز الذين يصدر بهم قرار من وزير العدل صفة الضبطية القضائية وذلك في إثبات الجرائم التي تقع بالمخالفة لأحكام هذا القانون، لذا يحق لهم التقصي والتحري والحصول على

٩٩ - تشمل الحالات الواردة فى المادة ٢٩ من قانون حماية البيانات الشخصية:
مخالفة شروط الترخيص أو التصريح أو الاعتماد.
عدم سداد رسوم تجديد الترخيص أو التصريح أو الاعتماد.
تكرار عدم الامتثال لقرارات المركز.
التنازل عن الترخيص أو التصريح أو الاعتماد للغير دون موافقة المركز.
صدور حكم بإفلاس المتحكم أو المعالج.

الأدلة التي تؤيد إدانة المخالف، بينما يتم مباشرة إجراءات القبض والتفتيش وغيرها من إجراءات التحقيق بمعرفة النيابة العامة.

وقد أوضحت النقاشات بالورشة والاجتماعات اللاحقة أن المشرع المصري قد خالف اللائحة الأوروبية GDPR في فرض التراخيص - حيث إن فرض التراخيص الإدارية هو من سلطات الضبط الإداري - وتطبيقه في نطاق هذا القانون أمر في غاية الصعوبة.

٣- التحديات التى تواجه عمل مركز حماية البيانات الشخصية

■ - وجود الكفاءات اللازمة:

سيحتاج الأمر إلي تدريبات ودورات مكثفة للحصول على الكفاءات القادرة على تطبيق القانون تقنيًا، نظرًا لحداثة نصوص القانون برمته، وكذلك تعتبر التطبيقات الدقيقة لحماية البيانات الشخصية جديدة على الكثير من المؤسسات خاصةً تلك التي تمارس نشاطها على المستوى المحلي.

أيضًا، سيواجه المركز تحديات كبيرة في تغطية احتياجاته من ذوي الكفاءة، ليس فقط على مستوى التمكن التقني، ولكن أيضًا على مستوى الأعداد بحيث يستطيع تغطية احتياجات السوق المصري بالكامل، وهو سوق كبير، ومستمر في النمو، خاصةً مع توجه الدولة إلى تشجيع الأنشطة الصغيرة والمتوسطة، وهو ما يعني بالتبعية زيادة المؤسسات المتعاملة في البيانات الشخصية. يدعم ذلك أن القانون الجديد يوجب على جميع المتعاملين في البيانات الشخصية الالتزام بأحكامه، بصرف النظر عن حجم نشاطهم. ويتضح ذلك بشدة في الالتزام بالحصول على التراخيص والتصاريح، والذي يعتبره القانون التزامًا عامًا يوقع على كل من ينصب نشاطه على التعامل في البيانات، أو بتعبير أدق كل من يقع تحت تعريف المتحكم أو المعالج، وهو ما يشمل كل المتعاملين في البيانات تقريبًا وذلك لعموم التعريفين.

وسيواجه المركز أيضًا مشكلة حث الشركات والمؤسسات على الامتثال لأحكامه دون التمادي والمبالغة في استخدام الجزاءات الإدارية التي خوله القانون إياها، كما أن الندرة في المتخصصين بهذا المجال ستنعكس أيضًا على التزام الشركات والمؤسسات، خاصةً وأن هناك البعض منها لا يمتلك بالضرورة القدرة على الوفاء بالأعباء المالية لقانون حماية البيانات، وعلى رأسهم الشركات الصغيرة.

وقد أوصت الورشة في هذا الصدد بضرورة الإستعانة بالكفاءات التقنية ضمن تشكيل وإدارة المركز لضمان فاعلية تطبيق أحكم القانون ولائحته التنفيذية.

■ موارد المركز:

في سياق آخر، صمت القانون عن الإمكانيات التي يتوجب توفيرها للمركز ليتمكن من ممارسة عمله، ويُفترض هنا أن المركز سيتكفل بتدبير احتياجاته المالية باعتباره هيئة اقتصادية كما نص القانون، إلا أن الأخير لم يحدد الوضع بالنسبة لميزانية المركز، وما إذا كانت مستقلة، أم تابعة لوزارة الاتصالات. بيد أنه بالرجوع لقانون الهيئات العامة نجد أن الأصل في الهيئات العامة أن يكون لها ميزانية خاصة، يصدق عليها رئيس مجلس إدارتها ويتم إقرارها بواسطة الجهة الإدارية المختصة، وهي وزارة الاتصالات في هذه الحالة. ولما كان وزير الاتصالات هو نفسه رئيس مجلس إدارة المركز، فيصبح في يده وضع الميزانية وإقرارها[١٠٠].

وبالنسبة للاتحاد الأوروبي، فإن السلطات الرقابية يفترض أن يكون لها ميزانية مستقلة[١٠١]، كما يفترض بالدول أن توفر للسلطات الرقابية فيها الموارد المالية والبشرية، والبنية التحتية اللازمة لاضطلاع السلطة بدورها[١٠٢].

■ استقلال المركز:

حرصت اللائحة الأوروبية على إنفاذ مبدأ الاستقلال فيما يتعلق بالجهات المنوطة بالرقابة على حماية البيانات(مسئول حماية البيانات والهيئة الرقابية، ويفترض وفقًا للائحة الاتحاد الأوروبي أن تتمتع السلطة الرقابية باستقلال تام في ممارسة نشاطها، وأن يراعي ذلك في تشكيلها وكذلك في مواردها (م ٥٢ من اللائحة الأوروبية).

وفي المقابل، لم يسلك القانون المصري السبيل نفسه، ونجد مظاهر ذلك واضحة للعيان فى تشكيل مركز حماية البيانات الشخصية، إذ يترأس المركز وزير الاتصالات نفسه، ويشمل مجلس إدارته عضوية ممثلين عن جهات حكومية متعددة، ومن ذلك ممثل عن (وزارة الدفاع - وزارة الداخلية - المخابرات العامة - هيئة الرقابة الإدارية.. إلخ) [١٠٣]، وقد ينعكس هذا التشكيل على مدى استقلالية المركز عن السلطة التنفيذية، وبالتالي على فعالية حماية البيانات، بالنظر إلى حجم السلطات الممنوحة للمركز في سياق البيانات الشخصية.

١٠٠ - راجع: المادة (١٥) من القانون رقم ٦١ لسنة ١٩٦٣ بشأن إصدار قانون الهيئات العامة.

١٠١ - الإرشاد (١٢٠)، فقرة (٢)، لائحة الاتحاد الأوروبي لحماية البيانات العامة.

١٠٢ - الإرشاد (١٢٠)، فقرة (١)، لائحة الاتحاد الأوروبي لحماية البيانات العامة؛ المادة (٥٢)، فقرة (٤)، لائحة الاتحاد الأوروبي لحماية البيانات العامة

١٠٣ - راجع: المادة ٢٠ من قانون حماية البيانات الشخصية المعنية بتشكيل مجلس إدارة المركز.

ثانياً

الإطار العقابي لقانون حماية البيانات الشخصية

اتجه المشرع إلى تنويع أدواته العقابية في ظل القانون الجديد ليضمن لنفسه مرونةً في مواجهة الاحتمالات المختلفة لانتهاكات البيانات الشخصية[١٠٤]. لذلك نص الفصل الرابع عشر الخاص بالجرائم والعقوبات على نوعين من العقوبات على اختلاف الجرائم: عقوبات مالية تتمثل في الغرامات متفاوتة المقدار، والعقوبات السالبة للحرية وصورتها الحبس، وجعل المحكمة المختصة بهذا القانون هي المحكمة الاقتصادية.

وباستقراء نصوص قانون حماية البيانات يتبدى أن المشرع قد اتخذ من العقوبات المالية وتحديدًا الغرامات سلاحًا أساسيًا للتعامل مع تهديدات البيانات الشخصية، فالنصوص العقابية، الممتدة من المادة (٣٥) إلى المادة (٤٨) من القانون، قد جعلت من الغرامات عاملًا مشتركًا بينها، إذ تم النص على الغرامات كخيار أساسي أو وحيد في كل المواد.

ووفقًا للقانون فإن الحد الأدنى للغرامة في القانون مائة ألف جنيه والحد الأقصى خمسة ملايين جنيه بحسب الجريمة، والقانون في ذلك يكون قد ساير التشريعات المقارنة وعلى رأسها اللائحة الأوروبية لحماية البيانات (GDPR) والتي تعتمد بشكل أساسي على الغرامات.

وقد تبنت اللائحة الأوروبية (المادة ٨٣ بند ٤) تقسيمًا وحيدًا للغرامات، ووفقًا لهذا التقسيم يكون الحد الأقصى للغرامة هو عشرة ملايين يورو أو ٢٪ من الدخل السنوي الإجمالي للجهة في حالات معينة، وترتفع الغرامة في حالات أخرى لتصل إلى ٢٠ مليون يورو أو ٤٪ من الدخل الإجمالي كحد أقصى (م ٨٣ بند ٥). أما بالنسبة للقانون المصري فقد آثر المشرع أن يكون أكثر تفصيلًا في هذا الصدد، فجعل نطاق العقوبة يتفاوت بحسب كل فعل أو مجموعة أفعال دون أن يجعل نطاقًا عامًا لكافة الانتهاكات.

وفي هذا الصدد نتناول انعكاس التمييز بين البيانات الشخصية العادية والحساسة على المعاملة العقابية، ونطاق الغرامات ومدى فعاليتها في العموم، ثم نتعرض لظاهرة إزدواج نصوص التجريم في القانون.

١٠٤ – حسام محمد نبيل الشنراقي: حماية البيانات الشخصية عبر الإنترنت التحديات والحلول، المجلة العربية للإدارة، محلق العدد الثاني، المجلد ٣٨، ٢٠١٨، ص ٤٨.

١- التمييز بين البيانات الشخصية العادية والحساسة من حيث المعاملة العقابية

أشارت الدراسة إلى أن المشرع يعني كثيرًا باضفاء مزيدٍ من الحماية على البيانات الشخصية الحساسة، فهو لم يكتف بوضع قيود أكثر على عمليات المعالجة التي تتضمن بيانات شخصية حساسة فحسب، بل وقام بمد هذه الحماية لتشمل عقوبات أكثر غلظة على الانتهاكات المتعلقة بها. فبينما أقر القانون عقوبة تتراوح بين ١٠٠ ألف ومليون جنيه للانتهاكات الواقعة على البيانات الشخصية العادية، فقد قفز بهذه العقوبة إلى خمسة أضعاف فيما يتعلق بالبيانات الشخصية الحساسة، فنص على نطاق غرامة بين ٥٠٠ ألف و ٥ ملايين جنيه، ذلك علمًا بأن ذلك هو الحد الأقصى للعقوبات المالية المنصوص عليها في القانون كما تمت الإشارةُ سلفًا[١٠٥].

كذلك، بالنسبة للبيانات الشخصية العادية، قام المشرع بالتمييز بين حالة التعامل غير المشروع على البيانات الشخصية العادية – المذكور سلفًا – الذي يتم بغرض على مقابل مادي أو أدبي، أو لتعريض الشخص للخطر أو الضرر، وحالة التعامل الذي يتم لغير ذلك من الأغراض. ذلك أن القانون قد ضاعف الحدين الأدنى والأقصى للغرامة على انتهاك خصوصية البيانات العادية إذا كان ذلك الانتهاك مقابل منفعة مادية أو معنوية، أو كان الانتهاك للإضرار بالشخص المعني بالبيانات أو تعريضه للخطر، لتصبح الغرامة من ٢٠٠ ألف جنيه إلى ٢ مليون جنيه، و/أو الحبس لمدة لا تقل عن ستة أشهر.

هذا التمييز له أهمية كبرى، لأنه يعالج أحد أكبر التهديدات التي تواجه البيانات الشخصية، ألا وهو الإتجار في البيانات، وبالمثل يواجه الأغراض الخبيثة لمعالجة البيانات الشخصية كالتعريض للخطر أو الإضرار.

ويعتبر التصدي لذلك السلوك أحد الأهداف التي صيغ القانون من أجلها في المقام الأول؛ فهو إن كان يستهدف حماية البيانات الشخصية في العموم، فهو يبتغي حمايتها من التحديات التي تطرحها التكنولوجيا تحديدًا والتي جعلت تداول تلك البيانات والولوج إليها أسهل بكثير، وبالتالي أصبحت فرص الاستفادة من تلك البيانات واستغلالها أكبر من ذي قبل، وصارت مادة خام وجاذبة للإتجار فيها والتعامل عليها لأهداف مختلفة.

لذا كان من الضروري أن يكون للمشرع موقف أكثر شدة من مسألة المعالجة غير المشروعة للبيانات الشخصية التي تتم بهدف الحصول على مقابل فلا تصبح تلك البيانات سلعة قابلة للتداول. والمجالات التي قد تعتمد على البيانات الشخصية وبالتالي تستدعي التعامل على هذه البيانات متنوعة للغاية

١٠٥ – منى الأشقر، محمود جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، مرجع سابق، ص ٨١.

بحيث لا يتسع لعرضها المقام، إلا أنه وعلى سبيل المثال فإن البيانات الشخصية تعتبر سلعة قيمة جدًا في مجال التسويق التجاري بحيث قد تدفع مقابلها مبالغ طائلة. والأمر كذلك فيما يتعلق باستخدام البيانات للأغراض السياسية ومحاولة فهم الساحة السياسية والتأثير عليها، ومثال ذلك قضية كامبريدج أناليتيكا الشهيرة التي استخدمت فيها البيانات الشخصية لمستخدمي تطبيق الفيس بوك لتصميم الحملة الانتخابية الرئاسية لأحد المرشحين بحيث تتناسب مع توجهات قاعدة الناخبين[١٠٦].

أما وإن كان التمييز بين التعدي على البيانات بحسب الغرض خطوةً محمودةً إلا أن تحديد الحد الأقصى للغرامة بمبلغ ٢ مليون جنيه قد لا يفي بالغرض بعد كل شيء، حتى مع القول بأن الغرامة ليست الجزاء المالي الوحيد الذي يمكن توقيعه على المعتدي على البيانات، وأنه يمكن تغريمه بتعويض لصالح المتضرر بجوار الغرامة. ذلك أن تحديد ملبغ التعويض يكون بناءً على معيار شخصي بخلاف الغرامة، أي أنه يتحدد بناءً على ما لحق بالشخص المعنى بالبيانات من ضرر أو فاته من كسب جراء تلك المعاملة غير المشروعة. فالغرض من التعويض إذًا هو جبر الضرر الذي خلفه الفعل غير المشروع للمضرور. ولكن بالنسبة للغرامة فالغرض منها يمتد لتحقيق الردع، ولذا فيتوقع أن تتجاوز قيمتها ما يمكن تحقيقه من مكسب من وراء الإتجار في البيانات أو على أقل تقدير أن تتساوى مع ذلك المكسب بحيث تسلب انتهاك البيانات كل قيمة له، ويجد المتعدي المحتمل على البيانات أنه يعرض نفسه لمخاطرة بدون مقابل مجزٍ عندما يحسب تكلفة الفرصة البديلة قبل الإقدام على فعله.

وبالنظر على ما يقتضيه ذلك على أرض الواقع نجد أن شراء بعض قواعد البيانات الشخصية قد يتجاوز سعره المليوني جنيه بكثير، بل وقد يتجاوز الحد الأقصى للقانون ككل: الخمسة ملايين جنيه. فكما أشرنا للتو، فإن سوق البيانات الشخصية نشط للغاية وهناك العديد من المجالات والتطبيقات التي تعني بهذا النوع من البيانات وهي على استعداد لدفع مبالغ تتجاوز المليوني جنيه فيه.

هذا التمييز في العقوبة المبني على الغرض من انتهاك البيانات لم يطبق على البيانات الحساسة، فالعقوبة، أو نطاق العقوبة بالأدق، واحد بصرف النظر عما إذا كانت تلك المعالجة غير المشروعة تمت بمقابل منفعة أو بغرض تعريض شخص للخطر، أو الضرر أم لا. أي أن أي تعدي على البيانات الشخصية الحساسة يقابله جزاء واحد أيًا كانت نية المتعامل في تلك البيانات، ألا وهو الحبس الذي لا يقل عن ستة أشهر و/أو الغرامة التي تتراوح بين ٥٠٠ ألف و٥ ملايين جنيه.

وبالنظر إلى أن ذلك هو أعلى حد أقصى وحد أدنى لغرامةٍ في القانون، فإن المشرع يكون قد أراد أن يمنح البيانات الحساسة أعلى مستوى من الحماية في كل أطوارها؛ فآثر التعميم بدلًا من أن ينص على حد أقل من (٥٠٠ ألف - ٥ مليون جنيه) لحالات الانتهاك.

وبالتالي يكون ذلك التنويع في المعاملة بين البيانات الشخصية العادية والحساسة مؤديًا للغرض منه؛ فهناك حدين للغرامة في البيانات العادية بحسب الغرض من الانتهاك، وهو ما يتناسب مع كونها بطبيعة الحال الأكثر انتشارًا والأكثر استخدامًا وتداولًا، وهناك حدٌ واحدٌ للغرامة على انتهاك البيانات الشخصية الحساسة لتحصينها بالكامل وبشكل أكثر صرامة.

ونطاق الغرامة ليس هو الضمانة العقابية الوحيدة التي ألحقها القانون بالبيانات الشخصية الحساسة، بل زاد على ذلك بأن وسع النطاق الموضوعي للأفعال المجرمة والتي تمثل انتهاكًا للبيانات الشخصية الحساسة؛ إذ أنه بالنسبة للبيانات الشخصية العادية قد تم تجريم عمليات "الجمع، والمعالجة، والإفشاء، والإتاحة، والتداول" في غير الأحوال المصرح بها قانونًا وبغير موافقة الشخص المعنى بالبيانات (م ٣٦ من القانون). أما بالنسبة للبيانات الشخصية الحساسة فقد أُضيفت إلى تلك الأفعال عمليات أخرى تشمل "التخزين، والنقل، والحفظ" (م ٤١ من القانون).

وهذا ما يثير التساؤل؛ فالمفترض في نطاق حماية البيانات أن كافة أنواع البيانات الشخصية تتمتع بالحماية ضد كل العمليات التي تشكل تهديدًا لأمنها، ولا اختلاف في ذلك بناءً على نوع البيانات إن كانت عادية أو حساسة، والاختلاف يكون فقط في ضمانات الحصول على هذه البيانات والعقوبات الموقعة جزاءً لانتهاكها، بحيث يتم كفالة مستوى أعلى من الحماية للبيانات الشخصية الحساسة، لكن التهديدات ينبغي النظر إليها بعين واحدة.

لذا حين يعتبر المشرع بعض العمليات (التخزين، والنقل، والحفظ) محظورة فقط في سياق البيانات الحساسة دون العادية، فإن ذلك يعوزه التبرير، ولا يغني فيه فكرة أنه محاولة لمنح حماية أكبر، لأنه كما أوضحنا سلفًا فإن مجال زيادة الحماية يكون في العقوبات وشروط جمع البيانات وموافقة الشخص المعنى بالبيانات، وليس طبيعة العمليات الواقعة على البيانات.

ومما يعضد ذلك النظر هو أن القانون الجديد، شأنه في ذلك شأن المعايير القياسية العالمية، قد اعترف في المواد (٤) و(٥) بالحق في النسيان دون تمييز بين البيانات الشخصية العادية والحساسة، وهو ما يعني أن عمليات التخزين والحفظ

106 - Final Order of the Federal Trade Commission of the United Stated of America in the matter of Cambridge Analytica, LLC, a corporation, docket no. 9383, issued at November 25, 2019; available at [https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf]

– والنقل بطبيعة الحال– يجب أن يكونوا مشروعين في كل الأحوال، إذن، وهو ما يطرح التساؤل حول الحكمة من وراء اختصاص البيانات الشخصية الحساسة بحماية خاصة فى هذه العمليات الثلاث.

ومن حيث النطاق الشخصي، يُرى أن المشرع قد ساوى بين البيانات الشخصية العادية والحساسة بأن جعل من الحائز والمتحكم والمعالج، كلهم مخاطبين بكلا النصين: الخاصين بالبيانات الشخصية العادية والحساسة.

وبذلك يكون القانون قد أحاط البيانات الشخصية الحساسة بسياج عقابي شديد، في اعتراف منه بمدى حساسية ذلك النوع من البيانات؛ حيث أن سوء استخدامه والتعدي عليه يسبب أضرارًا أكثر جسامة من مجرد التعرف على الشخص أو التوصل إليه، وقد يساء استخدامه بما يضر بالأمن القومي والفردي، حيث إن التعرف على التوجهات الدينية والسياسية والبيانات الحيوية للأفراد، قد يستخدم في توجيه الأفراد، أو استغلالهم، أو الترصد بهم وتقييد حريتهم في التعبير، أو حتى ابتزازهم.

٢- نطاق الغرامات وفعاليتها

أشارت الدراسة إلى أن قانون حماية البيانات الشخصية الجديد قد تبنى نطاقًا للغرامات، حده الأدنى ١٠٠ ألف جنيه والأقصى ٥ مليون جنيه، بحسب اختلاف الجرائم.

ومن خلال تتبع نهج المشرع لدى وضع الحدين الأدنى والأقصى لكل فعل من الأفعال، يمكن أن نستنتج ترتيب أولويات المشرع والاعتبارات الأكثر حاجةً للحماية في نظره والأقل. فبالنظر في خريطة العقوبات المالية للقانون يتضح أن القانون قد قسم الغرامات إلى أربع فئات رئيسية: الجرائم فئة المليون جنيه كحد أقصى، وفئة المليونين، وفئة الثلاثة ملايين، والخمسة ملايين وهي الأكبر.

فالمخالفات الأكثر خطورة في نظر المشرع كانت ثلاث: أولها الانتهاكات التي تنصب على البيانات الحساسة التي نص في المادة (٤١) على العقاب عليها بالحبس ما لا يقل عن ٣ أشهر و/أو الغرامة التي تتراوح بين ٥٠٠ ألف و٥ ملايين جنيه والتي تخاطب كل من الحائز والمتحكم والمعالج وتحظر عليهم جمع أو إتاحة أو تداول أو معالجة أو إفشاء أو تخزين أو نقل أو حفظ البيانات الشخصية الحساسة بدون موافقة الشخص المعنى بالبيانات أو في الأحوال المصرح بها قانونًا.

كذلك اعتبر المشرع مخالفة أحكام التراخيص والتصاريح والاعتماد أحد المخالفات التي تستحق الفئة الأعلى من الغرامات أيًا كان المخالف وهو ما يشمل بطبيعة الأمر الحائز والمتحكم والمعالج، وكذلك من يمارس نشاط تقديم الاستشارات في مجال حماية البيانات.

أما الحالة الثالثة فتشمل مخالفة أحكام حركة البيانات العابرة للحدود المذكورة في المواد (١٤) و (١٥) و(١٦). وتلك الحالة، وإن كان المشرع لم يخاطب بها شخص معين، فنطاقها الشخصي المنطقي يمتد إما للمتحكم أو للمعالج لأنهم هم من يملكون تمرير البيانات عبر الحدود.

وعلى صعيد آخر، يتم توقيع الفئة الأقل من الغرامات (من ١٠٠ ألف إلى مليون جنيه) على الحائز والمتحكم والمعالج الذين يتخلفون عن الحصول على موافقة الشخص المعنى بالبيانات للقيام بالمعالجة، أو حال قيامهم بها دون الحالات المصرح بها قانونًا.

ووفقًا للمادة (٣٧) تنصب ذات الغرامة على نفس الأشخاص إذا ما أعاقوا الشخص المعنى بالبيانات من ممارسة حقوقه[١٠٧]. وبالإجمال يمكن القول بأن الشريحة الأقل من العقوبات خص بها المشرع الانتهاكات المتعلقة بحقوق الشخص المعنى بالبيانات. بينما تقع في المنتصف العقوبات المتعلقة بالتزامات المتحكم والمعالج، والعاملين بالمركز، ومسئول حماية البيانات، والمخالفات التي تتعلق بأحكام التسويق الالكتروني.

هذا التدرج في الغرامات والذي يعكس ترتيب الأولويات بالنسبة للمشرع المصري لم يكن هو ذاته الذي تبنته اللائحة العامة لحماية البيانات GDPR. فوفقًا للمادة (٨٣) من تلك اللائحة، تم تقسيم الغرامات إلى فئتين فقط: أما الفئة الأولى فتوقع حد أقصى للغرامة يتمثل في الأعلى قيمة بين ١٠ ملايين يورو أو ٢٪ من الدخل العالمي الإجمالي الشركة أو المؤسسة، بينما تشمل الفئة الثانية الأعلى قيمةً الغرامة بين ٢٠ مليون يورو أو ٤٪ من حجم أعمالها، ودون أن يكون لأي منهم حدود دنيا، وهو ما يعطي مرونة أكثر للجهة المختصة بتوقيع العقوبة.

وعلى خلاف القانون المصري، فإن الفئة الثانية للغرامات وهي الأعلى تشمل انتهاك حقوق الشخص المعنى بالبيانات، ومبادئ المعالجة وعلى رأسها موافقة الشخص المعنى بالبيانات، أما مخالفات التراخيص فقد تم ادخالها في الفئة الأولى وكذلك التزامات المتحكم والمعالج.

بوجه عام، قام المشرع باتباع النهج العالمي في العقاب على انتهاكات البيانات الشخصية بأن تبنى نطاقًا كبيرًا للغرامات، فحتى وإن كانت قيمة الغرامات في القانون المصري تبدو منخفضة مقارنةً باللائحة الأوروبية، فذلك لا يمنع أنها تعتبر مرتفعة إذا ما قورنت بمعدل الغرامات في القوانين المصرية

١٠٧ – أشارت هذه المادة لحقوق الشخص المعنى بالبيانات المذكورة في المادة ٢، تحديدًا: العلم والاطلاع، والعدول، والتصحيح والتعديل، وتخصيص المعالجة، والعلم بالخرق، والحق في الاعتراض.

الأخرى، وتحديدًا القوانين المتعلقة بالتكنولوجيا[١٠٨]. على سبيل المثال يقل متوسط الغرامات المنصوص عليها في قانون جرائم تقنية المعلومات عن ٥٠٠ ألف، والحد الأقصى للغرامات في ذلك القانون هو مليون جنيه – إلا في حالة امتناع مقدم خدمة عن الامتثال لحكم محكمة وأن يترتب عليه الإضرار بالأمن القومي أو وفاة أحد الأشخاص فتصبح الغرامة بين ٣ ملايين و٢٠ مليون جنيه (م ٣٠ قانون جرائم تقنية المعلومات).

بيد أنه متى كان التزام المتحكم أو المعالج أو الحائز يتعلق بعدم الاحتفاظ بالبيانات لمدة أطول من اللازم للوفاء بالغرض المحدد لها[١٠٩]، وكانت العقوبة التي توقع جراء عدم التقيد بذلك هي الغرامة التي تتراوح بين ٢٠٠ ألف و ٢ مليون جنيه، فإن مقدم الخدمة – سواء أكان متحكم أو معالج أو حائز– يقع عليه التزام قانوني مقابل بالاحتفاظ بالبيانات لمدة معينة، فوفقًا لقانون جرائم تقنية المعلومات يتوجب على مقدم الخدمة أن يحتفظ بالبيانات التي تمكن من التعرف على مستخدم الخدمة (الشخص المعنى بالبيانات) لمدة مائة وثمانين يومًا متصلة. وقد قرر ذلك القانون غرامة تتراوح بين ٥ ملايين و ١٠ ملايين جنيه في حالة عدم الامتثال، وتضاعف في حالة العود (مادة ٢ من قانون جرائم تقنية المعلومات).

وبالتالي يصبح هناك استثناء على الحق في النسيان والالتزام بعدم الاحتفاظ الواقعين على المتحكمين والمعالجين، وهو استثناء غير تقديري، أي يلتزم به مقدم الخدمة بشكل مطلق أيًا كانت طبيعة البيانات المحتَفظ بها، دون الوقوف على إرادته أو إرادة الشخص المعنى بالبيانات، وجزاء عدم الانصياع له يتجاوز حتى الحد الأقصى للغرامة في قانون حماية البيانات الشخصية ككل.

وفي إطار تحديد نطاق الغرامات يلاحظ أن القانون قد أغفل ذكر معايير لتحديد قيمة الغرامة، فترك الأمر لسطلة القاضي والتفريد قضائي للعقوبة دون إعطاءه معايير يسترشد بها، وهو مسلك يخالف ما ذهبت إليه اللائحة الأوروبية(GDPR) فى المادة ٨٣ منها، إذ تحدد مجموعة عوامل تساعد على تقدير الغرامة بحسب طبيعة وجسامة الانتهاك الواقع، وما إذا كان عمديًا، ومحاولات المتحكم أو المعالج لتدراك الخرق وغيرها[١١٠].

كذلك لم يميز القانون في المعاملة العقابية بين المؤسسات الكبيرة والصغيرة، فلم يمنح الأخيرة أية إعفاءات أو وضع أحكام مخففة أو نطاق غرامات أقل. وعلى ذلك يكون قد ترك أمر التدرج بالعقوبة للقاضي ولما تأتي به اللائحة التنفيذية أيضًا[١١١].

٣- ازدواج نصوص التجريم

باستقراء النصوص العقابية في قانون حماية البيانات يتبدى بعض الالتباس بخصوص بعض الأفعال المجرمة، فقد تناول المشرع مثلًا فعل "جمع" البيانات غير المشروع الصادر عن المتحكم بالتجريم في موضعين مختلفين دون اختلاف ظاهر في شروط التطبيق مع اختلاف العقوبة.

فالمادة (٣٦) من القانون تنص على أن "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع... بيانات شخصية... في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعنى بالبيانات". وفي المادة (٣٨) يعود المشرع فيخاطب المتحكم أو المعالج مرةً أخرى بالعقاب "بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه" إذا لم يلتزم بواجباته المنصوص عليها في المادة (٤)، وتنص الأخيرة بدورها على أن "يلتزم المتحكم بالحصول على البيانات الشخصية أو تلقيها من الحائز أو المتحكم أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعنى بالبيانات أو في الأحوال المصرح بها قانونًا". والالتزام هنا يدخل أيضًا تحت مفهوم جمع البيانات أيضًا، ليصبح هناك وحدة في الموضوع والشخص واختلاف في العقوبة وهو ما يمثل إزدواجًا في نصوص التجريم والعقوبة على السواء.

وقد تكرر الأمر ذاته بالنسبة لإتاحة البيانات وإفشائها، فذات المادتين (٣٦) و(٣٨) يوقعان نفس العقوبات سالفة الذكر على فعل إفشاء البيانات الشخصية، بيد أن المادة (٣٦) تشير إليه بوصف إفشاء البيانات، بينما تشير المواد (٤) و(٥) المحال إليهما من المادة (٣٨) بوصف "القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات"، وهو ما لا يتصور اختلافه في المضمون عن الإفشاء، وبالتي نكون مرةً أخرى أمام وحدة موضوع (الإفشاء)، ووحدة أشخاص (المتحكم والمعالج)، مع اختلاف العقوبة.

---

١٠٨ – يلاحظ أن الغرامات التي نص عليها قانون حماية البيانات الشخصية تختلف من حيث طبيعتها عن تلك التي تتضمنها اللائحة الأوروبية، حيث أن الغرامة في مصر تعتبر عقوبة جنائية بينما هي غرامة إدارية وفقًا للائحة الأوروبية، وهو ما يترتب عليه اختلاف الاختصاص بتوقيع الغرامة في كل من النظامين. ففي أوروبا تختص مراكز حماية البيانات بتقدير الغرامة وتوقيعها وتخفيفها، بينما ينصرف ذلك الاختصاص للمحكمة وحدها في مصر. ويعني ذلك أيضًا خضوع الغرامات في مصر باعتبارها غرامات جنائية لكافة قواعد العقوبات الجنائية؛ فهي تخضع لمبدأ الشرعية، ولمبدأ شخصية العقوبة، وتتعدد بتعدد الفاعلين، وهو ما يعني إمكانية خضوع أكثر من متحكم أو حائز للغرامة كل على حدة عن نفس الفعل؛ مادة (٤٤)، قانون العقوبات المصري.

١٠٩ – راجع المادة ٣ من قانون حماية البيانات الشخصية

١١٠ – كذلك ذهبت بعض الدول إلى أبعد من ذلك، فتبنت الهيئة المعنية بالتنسيق بين السلطات الرقابية على حماية البيانات في ألمانيا (DSK) آلية لحسابة قيمة الغرامات المفترض توقيعها على المخالفين.

https://iapp.org/news/a/german-dpas-push-model-for-higher-gdpr-fines/

111 - Paul Lambert, 'Data Protection, Data Loss and Penalties' (2012) 4 IBLQ 22, p 26; recital 13, GDPR.

ومن المواضع التي قد تثير اللبس أيضًا العقوبات على مخالفة التراخيص والتصاريح، إذ توقع المادة (٣٨) جزاءً عامًا على مخالفة المتحكم لمجموع التزاماته المذكورة في المادة (٤) ومخالفة المعالج لمجموع التزاماته المذكورة في المادة (٥)، ومن بين هذه الالتزامات الالتزام "بالحصول" على التراخيص والتصرايح، بينما توقع المادة (٤٥) عقوبة الغرامة التي تتراوح بين ٥٠٠ ألف جنيه و ٥ مليون جنيه في حالة "مخالفة أحكام التراخيص والتصاريح". إلا أن المادة الأخيرة لا تخص المتحكم والمعالج وإنما تخاطب كل من يخالف أحكام التراخيص والتصاريح. وذلك النطاق الشخصي وإن كان أوسع فإنه من غير المتصور أن يقتصر على المتحكم والمعالج باعتبار أنهما المخاطبين الرئيسيين بالتزامات التراخيص والتصاريح.

"تم بحمد الله تعالى وتوفيقه"

مع تحيات كلية القانون بالجامعة البريطانية

التعديلات المقترحة
لمواد قانون حماية البيانات الشخصية

١ - التعديلات المقترحة لمواد قانون حماية البيانات الشخصية

رقم المادة	المادة الأولى (قانون الإصدار)
موضوع المادة	نطاق تطبيق قانون حماية البيانات الشخصية (من حيث طبيعة البيانات - من حيث الأشخاص)
التعليق	يقتصر نطاق تطبيق القانون على: (١) البيانات المعالجة إلكترونيًا فقط، ولا يمتد نطاقه إلى معالجة البيانات المكتوبة أو المخزنة ورقيًا بصورة كاملة (اليدوية). (٢) الأشخاص الطبيعيين دون الأشخاص الاعتبارية
نص القانون الحالي	يُعمل بأحكام هذا القانون والقانون والمُرافق في شأن حماية البيانات الشخصية المعالجة إلكترونيًا جزئيًا أو كليًا لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة للأشخاص الطبيعيين
ما يقابله في الـ GDPR	Art. 2 (Material scope): "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
التعليق على نص القانون	يكاد يتطابق النص المصري الذي سار على درب اللائحة، التي تنطبق على معالجة البيانات الشخصية كليًا أو جزئيًا بوسائل آلية وعلى المعالجة بخلاف الوسائل الآلية للبيانات الشخصية التي تشكل جزءًا من نظام حفظ الملفات، أو يُقصد بها أن تشكل جزءًا من نظام حفظ الملفات. كما حصرت المادة ٤ الخاصة بالتعريفات (تعريف البيانات) نطاقه في بيانات الشخص الطبيعي
المقترح	إيراد مبادئ حماية البيانات الشفافية والمشروعية، على غرار الفصل الثاني من اللائحة الأوروبية (م٥)

رقم المادة	المادة الثانية (قانون الإصدار)
موضوع المادة	النطاق الإقليمي لتطبيق قانون حماية البيانات الشخصية
التعليق	لم يركز القانون على البيانات، وانما أخذ بمبدأ الاقليمية مدعمًا بمبدأ شخصية القوانين
نص القانون الحالي	على كل من ارتكب إحدى الجرائم المنصوص عليها في القانون المرافق متى كان الجاني: - من المصريين داخل الجمهورية أو خارجها. - أو كان من غير المصريين المقيمين داخل الجمهورية. - من غير المصريين خارج الجمهورية إذا كان الفعل معاقبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية.
التعليق على نص القانون	الأخذ بمعيار موطن المعالج أو المتحكم في البيانات بصرف النظر عما إذا كانت المعالجة تتم في الاتحاد الأوروبي أم لا، كما تنطبق اللائحة على البيانات المتداولة داخل الاتحاد رغم وجود المعالج أو المتحكم خارج الاتحاد
التساؤلات التي يثيرها النص في القانون المصري	أين نطاق انطباقها على المنازعات التجارية والمدنية أو أي مسائل أخرى تثار بصدد تطبيق القانون؟ فلا يفترض دائمًا وقوع جريمة حال معالجة البيانات
المقترح	ضبط نطاق تطبيق القانون وفقًا لمعالجة البيانات

رقم المادة	المادة الثالثة (قانون الإصدار)
موضوع المادة	البيانات المستبعدة من نطاق تطبيق القانون
التعليق	توسع القانون في البيانات المستبعدة من نطاق تطبيق القانون مما يؤدي الى خروج عدد كبير من البيانات من نطاق التطبيق وخاصة بيانات البنك المركزي حيث يجب إدراجها لما فيها من خطورة إن لم تشمل بالحماية، وبالرجوع لقانون البنك المركزي الصادر مؤخرًا لم تفرد الحماية الكاملة لبيانات العملاء في نطاق القانون الصادر مؤخرًا
نص القانون الحالي	لا تسري أحكام القانون المرافق على ما يلي: البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي. البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني. البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخدم في أغراض أخرى، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام. البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية. البيانات الشخصية لدى جهات الأمن القومي وما تقدره لاعتبارات أخرى. ويجب على المركز- بناءً على طلب من جهات الأمن القومي- إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية خلال مدة زمنية محددة، وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به. البيانات الشخصية لدى البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه عدا شركات تحويل الأموال وشركات الصرافة، على أن يراعى في شأنهما القواعد المقررة من البنك المركزي المصري بشأن التعامل مع البيانات الشخصية
ما يقابله في الـ GDPR	art. 2 /2 This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. 3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 452001/ applies. Regulation (EC) No 452001/ and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98. 4. This Regulation shall be without prejudice to the application of Directive 200031//EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

التعليق على نص القانون

حرصت اللائحة على أن يكون الاستبعاد محدودًا للغاية، وقصره على البيانات المعالجة خارج الاتحاد، وهذا أمر طبيعي، والبيانات المعالجة في سياق نشاط شخصي أو منزلي أو لأغراض الضبط الإداري أو القضائي

التساؤلات التي يثيرها النص في القانون المصري

لماذا التوسع في طائفة البيانات المستبعدة؟ ما فائدة القانون إذاً؟

المقترح

إلغاء استبعاد البيانات الشخصية لدى البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه. كذلك البيانات الشخصية لدى جهات الأمن القومي وما تقدره لاعتبارات أخرى، فضفاضة ويخضع لتقدير بحت لهذه الجهات، حيث أن القانون توسع في تحديد هذه الجهات على إطلاقها (وزارة الداخلية.. وزارة الدفاع ...)

رقم المادة	الخامسة (قانون الإصدار)
موضوع المادة	اختصاص المحاكم الاقتصادية بنظر الجرائم التي ترتكب بالمخالفة للقانون
التعليق	أن يشمل اختصاص المحكمة للمنازعات الناشئة عن القانون
نص القانون الحالي	أن المحاكم الاقتصادية تختص بنظر الجرائم التي ترتكب بالمخالفة لأحكام القانون المرافق
التساؤلات التي يثيرها النص في القانون المصري	أهمية اختصاص المحاكم الاقتصادية بنظر أي منازعة متعلقة به، جنائية أو تجارية أو مدنية
المقترح	امتداد اختصاص المحاكم الاقتصادية بنظر المنازعات الناشئة عن تطبيق هذا القانون

رقم المادة	السادسة (قانون الإصدار)
موضوع المادة	التزام المخاطبين بأحكام القانون بتوفيق أوضاعهم خلال سنة
نص القانون الحالي	يلتزم المخاطبون بأحكام هذا القانون بتوفيق أوضاعهم طبقًا لأحكام القانون المرافق ولائحته التنفيذية، وذلك خلال سنة من تاريخ صدور هذه اللائحة
التعليق على نص القانون	أحال النص بشكل واضح للائحة
التساؤلات التي يثيرها النص في القانون المصري	ما هي حدود التوفيق وما هو المقبول بالنسبة للعمليات التي تمت في الماضي من معالجة ولها أثرها في المستقبل ؟؟؟

رقم المادة	مادة ١ فصل ١
موضوع المادة	التعريفات التي أوردها القانون
التعليق	بشأن تعريف البيانات الشخصية
نص القانون الحالي	أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية.
ما يقابله في الـ GDPR	م ٤ لائحة رقم ٦٧٩/٢٠١٦: "means any information relating to an identified or identifiable natural person ('data subject') ; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"
التعليق على نص القانون	يختلف نص اللائحة اختلافًا جوهريًا في تعريف البيانات الشخصية. ويتجلى هذا الاختلاف في استخدام القانون مصطلح "بالربط" واستخدام اللائحة مصطلح "By Reference" والذي يعني "بالإشارة" وليس "بالربط". وتبدو أهمية الفرق بين المصطلحين في أن مصطلح الربط يفهم منه بسهولة أنه لابد من ارتباط بيانين معًا لكي يصبح البيان شخصي بالمعنى الذي يقصده ويحميه القانون. بينما استخدام لفظ "بالإشارة" في اللائحة يوسع من نطاق الشخصية التي قد يشملها القانون بحمايته بجعلها قائمة بذاتها كبيان شخصي من دون الحاجة إلى ربطها ببيان أخر.
المقترح	تعديل نص المادة باستبدال لفظ "بالإشارة" بدلاً من لفظ "بالربط"

رقم المادة	مادة ١ فصل ١
موضوع المادة	التعريفات التي أوردها القانون
التعليق	بشأن تعريف البيانات الشخصية الحساسة
نص القانون الحالي	هي البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية " أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة .
ما يقابله في الـ GDPR	لم تفرد اللائحة تعريفًا خاصًا بالبيانات الشخصية الحساسة
التعليق على نص القانون	بعض البيانات التي عرفها القانون المصري بأنها بيانات حساسة أفرد لها المشرع الأوروبي تعريفًا مستقل بذاته مثل تعريف البيانات البايومترية
التساؤلات التي يثيرها النص في القانون المصري	س١: ما المقصود بالبيانات التالية التي ذكرتها المادة؟ ١. بيانات القياسات الحيوية "البيو مترية "، "البيانات المالية" س٢: هل هناك قوانين أخرى تعرف هذه البيانات؟ أم كان من المفترض أن يعرفها هذا القانون اقتداءً باللائحة الأوروبية؟ س٣: هل تعريف تلك المصطلحات متروك للائحة التنفيذية؟ لماذا لم يذكر النص إحالة تحديد تلك البيانات للائحة التنفيذية؟
المقترح	تعديل القانون بإضافة مواد لتعريف البيانات السابقة الذكر التي أغفل تعريفها تعديل تعريف البيانات الحساسة بإضافة إحالة للائحة التنفيذية لتقوم بتعريف البيانات التي تم تصنيفها على أنها بيانات شخصية حساسة في هذه المادة تعديل النص بإضافة تعريف شامل للبيانات الشخصية الحساسة مع إعطاء أمثلة لها

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف البيانات التي تفصح عن الصحة
نص القانون الحالي	لم يفرد القانون تعريفًا خاصًا بالبيانات التي تفصح عن الحالة الصحية للشخص
ما يقابله في الـ GDPR	‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
التعليق على نص القانون	رغم أن القانون المصري لم يفرد تعريفًا خاصًا بالبيانات التي تفصح عن الحالة الصحية للشخص إلا أنه ذكر تعريف البيانات الشخصية الحساسة حين حدد أن البيانات المتعلقة بالحالة الصحية هي تلك المتعلقة بالحالة العقلية أو البدنية للشخص الطبيعي، وهو ما يقابل تعريف تلك البيانات في لائحة الاتحاد الأوروبي. وإن كان المشرع المصري قد استزاد عن تعريف اللائحة بذكر البيانات التي تدل على الحالة الصحية النفسية وحسنًا فعل في حين لم تذكرها اللائحة. والجدير بالذكر أن تعريف اللائحة قد استرسل في تعريف البيانات المتعلقة بالحالة الصحية عن طريق الإشارة إلى بعض الحالات التي تندرج بها وهذه زيادة لم يوردها المشرع المصرى وإن كانت لا تنتقص من النص شئ.
المقترح	لا حاجة لإضافة تعريف للبيانات التي تفصح عن الحالة الصحية للشخص بناء على التعليق السابق ذكره

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف البيانات الجينية
نص القانون الحالي	لم يفرد القانون تعريفًا للبيانات الجينية
ما يقابله في الـ GDPR	genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
التعليق على نص القانون	عدم وجود نص يعرف المقصود بالبيانات الجينية يترك مجالًا واسعًا للتوسيع أو التضييق من نطاق تلك البيانات مما قد يؤدي إلى ظهور مشاكل في التطبيق، ويخل بقدرة المتحكم/المعالج في توقع نتيجة معالجته لبعض البيانات؛ وذلك لصعوبة توقع ما إذا كانت تلك البيانات شخصية حساسة أم لا.
المقترح	تعديل النص بإضافة تعريف للبيانات الجينية، أو تعديله بالإحالة إلى اللائحة التنفيذية لتقوم بذلك.

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف البيانات المالية
نص القانون الحالي	لم يفرد القانون تعريفًا للبيانات المالية
ما يقابله في الـ GDPR	لم تفرد اللائحة تعريفًا خاصًا بالبيانات المالية
التعليق على نص القانون	عدم وجود نص يعرف المقصود بالبيانات المالية يترك مجالًا واسعًا للتوسيع أو التضييق من نطاق تلك البيانات مما قد يؤدي إلى ظهور مشاكل في التطبيق، ويخل بقدرة المتحكم/المعالج في توقع نتيجة معالجته لبعض البيانات، وذلك لصعوبة توقع ما إذا كانت تلك البيانات شخصية حساسة أم لا ترتبط هذه النوعية من البيانات عادةً بالبنوك، الأمر المستثنى من نطاق تطبيق القانون، مما يشكل قصورًا، ويعد المصدر الأساسي للبيانات المالية خاصة في ظل التطور الرقمي.
المقترح	تعديل النص بإضافة تعريف للبيانات المالية التي تعد من قبيل البيانات المالية أو تعديله بالإحالة إلى اللائحة التنفيذية لتقوم بذلك

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف البيانات البيو مترية
نص القانون الحالي	لم يفرد القانون تعريفًا للبيانات البيو مترية
ما يقابله في الـ GDPR	‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
التعليق على نص القانون	يعد هذا المصطلح حديث الاستخدام نسبيًا مما كان يستدعي من المشرع إضافة تعريف له
التساؤلات التي يثيرها النص في القانون المصري	ما المقصود بالبيانات البيو مترية؟
المقترح	تعديل النص بإضافة تعريف للبيانات البيو مترية أو تعديله بالإحالة إلى اللائحة التنفيذية لتقوم بذلك

رقم المادة	مادة١ / فصل ١
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف الشخص المعنى بالبيانات
نص القانون الحالي	هو أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونيًا تدل عليه قانونًا أو فعلًا، وتمكن من تمييزه عن غيره.
ما يقابله في الـ GDPR	المادة رقم ٤
التعليق على نص القانون	عرفت المادة ٤ من اللائحة الأوروبية "صاحب البيانات Data subject" بأنه "الشخص الطبيعي الذي يمكن التعرف عليه، أو يمكن تحديده بشكل مباشر أو غير مباشر، وخاصة بالرجوع إلى رقم الهوية أو إلى عامل أو أكثر من العوامل المحددة لهويته البدنية أو الفسيولوجية أو العقلية أو الاقتصادية أو الاجتماعية
المقترح	يجب إضافة تعريف الشخص المعنى بالبيانات وبشكل واضح

رقم المادة	مادة١ / فصل ١
موضوع المادة	التعريفات التي أوردها القانون
التعليق	بشأن تعريف المعالجة
نص القانون الحالي	هو 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 جزئيًا أو كليًا .
ما يقابله في الـ GDPR	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
التعليق على نص القانون	يعد الفرق الجلي بين لائحة الاتحاد الأوروبي والقانون المصري هو ذكر الأفعال التي تعد من قبيل المعالجة في القانون على سبيل الحصر بينما أوردتها اللائحة على سبيل المثال. وإن كان تعداد الأفعال يكاد يبدو كافيًا من الوهلة الأولى للاطلاع على النص، إلا أنه ربما كان لابد أن يقتدي المشرع المصري بنظيره الأوروبي في هذا الشأن، وذلك ليترك مجال لأفعال أخرى ربما يخلقها التطور المستمر في التعامل مع البيانات باستخدام التكنولوجيا.
التساؤلات التي يثيرها النص في القانون المصري	ما الفرق بين التجميع والتسجيل؟ ما الفرق بين التخزين والحفظ؟ ما الفرق بين تعديل وتغيير؟ وما المقصود بتحليل؟
المقترح	تعديل القانون بإضافة تعريفات دقيقة لتلك الأفعال، أو تعديله بإضافة إحالة إلى اللائحة التنفيذية لتقوم بذلك.

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف التنميط Profiling
نص القانون الحالي	لم يفرد لها القانون تعريفًا
ما يقابله في الـ GDPR	profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
المقترح	يجب أن يورد القانون تعريفًا واضحًا للتنميط أو أن يُعهد للائحة بذلك.

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف التسمية المستعارة pseudonymization
نص القانون الحالي	لم يفرد لها القانون تعريفًا
ما يقابله في الـ GDPR	pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
المقترح	لابد أن يشار إلى "التعمية" إن صح التعبير في اللائحة التنفيذية والأطر التقنية المستخدمة في هذا الشأن.

رقم المادة	N/A
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف نظام الإيداع filing system
نص القانون الحالي	لم يفرد لها القانون تعريفًا
ما يقابله في الـ GDPR	filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
المقترح	يجب أن يورد القانون تعريفًا واضحًا لنظام الإيداع، أو أن يُعهد للائحة بذلك.

رقم المادة	مادة١ / فصل ١
موضوع المادة	التعريفات التي أوردها القانون
التعليق	بشأن تعريف الحائز
نص القانون الحالي	هو أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليا ببيانات شخصية في أي صورة من الصور، أو على أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة
ما يقابله في الـ GDPR	لم تفرد اللائحة تعريفًا مستقلًا للحائز
التعليق على نص القانون	حسنًا فعل المشرع حين أورد تعريفًا للحائز، وإن كان لابد أن يصيغ النص بما يظهر فرقًا بينه وبين المصطلحات الأخرى مثل المتحكم والمعالج؛ وذلك لأن النص بصياغته الحالية يفهم منه أن الحائز يمكن أيضًا أن يصبح أو يتحول لمعالج أو لمتحكم اذا بدأ بإجراء عمليات أخرى على سبيل المعالجة على البيانات التي يحوزها. لم يذكر المشرع للحائز أيًا من الالتزامات التالية، كما أفرد للمتحكم أو المعالج، وليس له دور واضح وربما يكون من الأفضل أن يحذف التعريف لما يسببه من خلط. الحائز لم يرد له ذكر في اللائحة الأوروبية والحقيقة إن تبرير وضعه في القانون بسبب التسويق الإلكتروني هو تبرير غير مقنع وليس له سند علمي بالعكس هو أعطى مبرر قانوني للحيازة حتى لو كانت بشكل غير قانوني.
التساؤلات التي يثيرها النص في القانون المصري	هل يمكن أن يتحول الحائز إلى معالج أو متحكم؟ وإذا كانت الإجابة نعم: لماذا أفرد المشرع تعريفًا خاصًا به في حين أن تعريف المتحكم ربما كان من الممكن أن يجبه؟ هناك تساؤل حول خصوصية مفهوم الحائز في القانون المصري، فلم نجد له مقابل في القوانين المقارنة المطروحة. وما هي طبيعة العلاقة بين الحائز والمعالج؟ وهل هناك تداخل بين مفهوم الحائز ومفهوم المعالج؟ حيث أن كلاهما يدخل في إطار تعريفه الاحتفاظ بالبيانات الشخصية؟
المقترح	تعديل صياغة النص بإضافة ما يفهم منه الفرق بين الحائز وغيره

رقم المادة	مادة١ / فصل ١
موضوع المادة	التعريفات التي أغفلها القانون
التعليق	بشأن تعريف المتلقي Recipient
نص القانون الحالي	لم يفرد القانون تعريفاً للمتلقي
ما يقابله في الـ GDPR	‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
التعليق على نص القانون	عند النظر بدايةً لكلٍ من لفظ الحائز الذي أورده القانون المصري، ولفظ المتلقي الذي أوردته اللائحة يمكن أن يفهَم أن كلاهما يتعلق بنفس الشخص. ولكن بعد قراءات أخرى يستنتج أنَّ لفظ الحائز ربما يكون أوسع من لفظ المتلقي؛ من حيث أنه يستهدف كل من وقعت البيانات في حيازته بينما لفظ المتلقي يضيق نطاق شموله على الأشخاص الذين تصل البيانات إليهم عن طريق التسريب
المقترح	إضافة تعريف للمتلقي وبشكل واضح لما في ذلك من أهمية في حالات الانتهاك والخرق.

رقم المادة	مادة١ / فصل ١
موضوع المادة	التعريفات التي أوردها القانون
التعليق	بشأن تعريف المتحكم
نص القانون الحالي	هو 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 طبقًا للغرض المحدد أو نشاطه.
ما يقابله في الـ GDPR	controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
التعليق على نص القانون	يعتبر الاختلاف الرئيسي بين كلا النصين أنَّ اللائحة أحالت إلى القوانين الوطنية بشأن تحديد الخصائص واجبة التوافر لكي يسمي الشخص الطبيعي أو الاعتباري معالج، بينما لم يورد المشرع المصري مثل هذه الخصائص التفصيلية، ولا أحال في شأنها إلى اللائحة التنفيذية
المقترح	إما تعديل النص ليكون أكثر تفصيلًا، ويحدد صفات تمكن من إلحاق صفة المعالج بالشخص الطبيعي أو الاعتباري، أو تعديل النص بالإحالة التنفيذية إلى اللائحة لتقوم بذلك.

رقم المادة	مادة١ / فصل ١
موضوع المادة	التعريفات التي أوردها القانون
التعليق	بشأن تعريف المعالج
نص القانون الحالي	هو أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته.
ما يقابله في الـ GDPR	‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
التعليق على نص القانون	الفرق بين القانون ولائحة الاتحاد -والذي ربما أفقد تعريف القانون معناه - هو ذكر القانون أن المعالج هو من يعالج البيانات لصالحه أو للمتحكم بينما ركزت لائحة الاتحاد على أنه يقوم بذلك لمصلحه المتحكم فقط وليس لمصلحته. وهذه الاستزادة من جانب المشرع المصري ربما تجعل التفرقة بين كل من مصطلحي المعالج والمتحكم غير واضحة.
التساؤلات التي يثيرها النص في القانون المصري	هل هناك سبب وراء إضافة لفظ "لصالحة" لتعريف المعالج؟ ويختلف القانون المصري عن اللائحة الأوروبية فيسمح للمعالج بأن يقوم "بعملية المعالجة" لصالحه وليس لصالح المتحكم. ويثار في هذا الشأن تساؤل حول مسؤولية المعالج في حالة قيامه بعملية المعالجة لصالحه، وليس بناءً على تعليمات المتحكم، وحول قصد المشرع المصري من إضافة إمكانية المعالجة لصالح المعالج، وهل يعني ذلك أنه لا يتحول لصفة متحكم تلقائيًا إن كان هو الذي يقوم بالمعالجة لصالح نفسه؟
المقترح	تعديل النص بحذف لفظ "لصالحه"

رقم المادة	N/A
موضوع المادة	تعريفات أغفلها القانون
التعليق	تعريف مسئول حماية البيانات
التعليق على نص القانون	التزامات مسئول حماية البيانات كبيرة جدًا، ومتداخلة مع وظائف أخرى مثل أمن المعلومات، وهناك فرق كبير بين أمن المعلومات وحماية البيانات الشخصية
المقترح	يجب تعريف مسئول حماية البيانات بشكل واضح لما له من دور محوري في تنفيذ القانون

رقم المادة	مادة١ / فصل ١
موضوع المادة	تعريفات أوردها القانون
التعليق	تعريف التصريح والترخيص
نص القانون الحالي	الترخيص: 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 المرخص له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية لهذا القانون وذلك لمدة ثلاث سنوات قابلة للتجديد لمدد أخرى. التصريح: وثيقة رسمية تصدر عن المركز للشخص الطبيعي أو الاعتباري تمنحه من خلالها الحق في ممارسة نشاط جمع البيانات الشخصية الإلكترونية، أو تخزينها، أو نقلها، أو معالجتها، أو القيام بأنشطة التسويق الإلكتروني، أو كل ما سبق، والتعامل عليها بأي صورة، او 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.
التعليق على نص القانون	لم يوضح القانون الفرق بين الترخيص والتصريح، وحالات استصدار كل منهما
المقترح	توضيح الفرق بين الترخيص والتصريح وحالات استصدار كل منهما

رقم المادة	مادة ١ /٢ فصل ٢
موضوع المادة	ضرورة موافقة الشخص المعنى بالبيانات
التعليق	استلزم المشرع ضرورة الموافقة الصريحة على أي عمليات تجري على البيانات (جمع – معالجة ...) ولكن لا تشترط الموافقة في الأحوال المصرح بها قانونًا
نص القانون الحالي	لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعنى بالبيانات أو في الأحوال المصرح بها قانوناً
ما يقابله في الـ GDPR.	المادة ٦
التعليق على نص القانون	عرفت المادة ١١/٤ من اللائحة الأوروبية "موافقة" صاحب البيانات "consent" of the data subject بأنها تعني أي إشارة صريحة ومحددة وواضحة لا لبس فيها، تدل على رضا صاحب البيانات والتي يشير من خلالها إلى الموافقة على معالجة البيانات الشخصية المتعلقة به أو بها، من خلال بيان أو بعمل إيجابي واضح.
التساؤلات التي يثيرها النص في القانون المصري	قصر المشرع المصري من طرق الموافقة على حالات جمع البيانات، على انه استلزم الموافقة الصريحة فقط او في الحالات المصرح بها قانونا، إلا أن اللائحة كانت متوسعة في حالات جمع البيانات. ويلاحظ أن المشرع لم يحدد صورة الموافقة الصريحة، هل تشترط الكتابة أم تكفي الموافقة شفاهه؟
المقترح	يجب أن يحدد المشرع شكل الموافقة المطلوبة (كتابةً) من الشخص المعنى بالبيانات. أيضًا

رقم المادة	مادة ٢
موضوع المادة	بيان حقوق الشخص المعنى بالبيانات
التعليق	أورد المشرع بعض حقوق الشخص المعنى بالبيانات على سبيل المثال لا الحصر.. ولم يتضمن الحق في نقل البيانات
نص القانون الحالي	ويكون للشخص المعنى بالبيانات الحقوق الآتية: العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها. العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها. التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية. تخصيص المعالجة في نطاق محدد. العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية. الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات. وباستثناء البند (٥) من الفقرة السابقة، يؤدي الشخص المعنى بالبيانات مقابل تكلفة الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه، ويتولى المركز إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه.
ما يقابله في الـ GDPR	خصصت اللائحة الفصل الثالث كله لحقوق صاحب البيانات، واشارت في المبحث الأول للشفافية والوسائل، تناول فيه شفافية المعلومات والاتصالات ووسائل ممارسة حقوق صاحب البيانات (م١٢). وأشار المبحث الثاني إلى المعلومات وحق الوصول إلى البيانات الشخصية(م١٥)، وتضمن المبحث الثالث الحق في التصحيح م ١٦ والحق في المحو (الحق في النسيان) م ١٧. والحق في تقييد المعالجة م ١٨ ، والحق في نقل البيانات م ٢٠ والحق في الاعتراض٢١
التعليق على نص القانون	تميزت اللائحة بوضع ضوابط ممارسة كل حق في صلب اللائحة، على عكس القانون المصري الذى نص على الحق نفسه وترك تحديد كيفية ممارسته إلى تنظيم اللائحة التنفيذية. كذلك لم تربط اللائحة تقديم الخدمات المرتبطة بممارسة الحق بمقابل مادي كما فعل المشرع المصري
التساؤلات التي يثيرها النص في القانون المصري	ما هو السبب في عدم ذكر المشرع لضوابط ممارسة كل حق؟
المقترح	إلغاء المقابل المادي لأداء خدمات مقابل ممارسة حقوق الشخص. تعديل القانون بإضافة قواعد ممارسة كل حق قرين النص الذى يقرره إضافة حق الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

رقم المادة	مادة ٣ / فصل ٢
موضوع المادة	شروط جمع البيانات الشخصية ومعالجتها والاحتفاظ بها
نص القانون الحالي	يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية: أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعنى. أن تكون صحيحة وسليمة ومؤمنة. أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها. ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها. وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات.
التعليق على نص القانون	يعتبر الشرط الاول "معلنة للشخص المعنى"، ليس له قواعد تحدده. فقد تجمع البيانات وتعالج ويحتفظ بها دون معرفة الشخص المعنى بالبيانات نص المشرع على أهمية التخلص من البيانات بعد انتفاء الغرض المحدد له، إلا أنه نص في المادة ٤ من الفصل الثالث للمتحكم بالاحتفاظ بالمعلومات مع ضرورة محو بياناته الشخصية أي أن تكون في صورة لا تسمح بتحديد هوية الشخص. هناك خلط بين ضروه إمساك الدفاتر والمحو للبيانات.
المقترح	يجب إيضاح صورة الإبقاء على البيانات في السجلات وكيفية محوها بما يسمح بتتبع أثر المعالجة

رقم المادة	مادة ٤
موضوع المادة	التزامات المتحكم
التعليق	لم يحدد القانون طريقة أو كيفية العلم هل سيكون إبلاغ أو مسئولية على المتحكم أن يتحرى، ولم يقم المشرع بالإحالة للائحة التنفيذية في ذلك
نص القانون الحالي	تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به
التعليق على نص القانون	بخلاف ال GDPR، و إن كان المشرع الأوروبي تعرض بإيجاز شديد لوجوب تحديد المسؤولية بين المتحكمين المشتركين، لم يشر المشرع المصري لأي شروط خاصة بالتحكم المشترك ولم ينص على إمكانية تعيين نقطة اتصال لتسهيل الوصول للمتحكم بدل من وضع هذا العبء على الشخص المعنى البيانات.
التساؤلات التي يثيرها النص في القانون المصري	ماذا عن اشتراط وجود عقد أو اتفاقية مفصلة؟ ما هي طرق العلم والإبلاغ؟
المقترح	أن يحدد القانون وسائل العلم وطرق الإبلاغ أو يتم تحديد ذلك في اللائحة

رقم المادة	مادة ٥
موضوع المادة	التزامات المعالج
نص القانون الحالي	الفقرات ٥ و٧ و ٩
المقترح	يجب توضيح طبيعة السجل ما إذا كان إلكترونيًا أو ورقيًا عدم إشراك معالج اخر دون إذن كتابي مسبق من المتحكم عدم إجراء أية معالجة للبيانات الشخصية تتعارض مع غرض أو نشاط المتحكم فيها إلا إذا كانت البيانات الشخصية لغرض إحصائي أو تعليمي أو لا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة، وفي جميع الاحوال يجب أن تكون تلك البيانات مجهلة وفي حالة وجود أكثر من معالج، يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون فضلاً عن الالتزامات المنصوص عليها في العقود المبرمة بينهم.....

رقم المادة	مادة ٦
موضوع المادة	شروط المعالجة
نص القانون الحالي	تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، مالم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.
التعليق على نص القانون	ذكر القانون تمكين المتحكم فقط، ولم يذكر تمكين المعالج وهو نص غير واضح يشوبه الغموض وفتح الباب للتلاعب.
المقترح	يجب أن يلحق بتقييد أو موافقة الشخص المعنى بالبيانات ضرورة وجود عقد مكتوب بين المتحكم والمعالج ينبغي على اللائحة التنفيذية أن تدير علاقة المتحكم بالمعالج من خلال الالتزامات التعاقدية حتى تكون تلك العلاقة مبنية على التزامات مكتوبة وبالتالي يمكن ربط المعالج بالقانون من خلال آلية متابعة التنفيذ في العقود. إضافة فقرة خامسة: (٥) أن تكون المعالجة ضرورية لحماية المصالح الحيوية للشخص المعنى بالبيانات أو لأجل المصلحة العامة

رقم المادة	مادة ٨
موضوع المادة	تعيين مسئول حماية البيانات
نص القانون الحالي	ينشأ بالمركز سجل لقيد مسئولي حماية البيانات الشخصية، وتحدد اللائحة التنفيذية لهذا القانون شروط القيد وإجراءاته وآليات التسجيل. ويلتزم الممثل القانوني للشخص الاعتباري لأي متحكم أو معالج بأن يعين داخل كيانه القانوني وهيكله الوظيفي موظفًا مختصًا مسئولًا عن حماية البيانات الشخصية، وذلك بقيده في سجل مسئولي حماية البيانات الشخصية بالمركز، ويعلن عن ذلك. ويكون الشخص الطبيعي المتحكم أو المعالج هو المسئول عن تطبيق أحكام هذا القانون.
المقترح	صياغة معيبة، حيث يكون المتحكم أو المعالج (الشخص الطبيعي هو المسئول عن تطبيق القانون) إذن ما هي وظيفة مسئول حماية البيانات؟ وما هو التصرف حال لم يكن المتحكم أو المعالج شخص طبيعي؟ النص من تقرير اللجنة المشتركة: يلتزم الممثل القانون للشخص الاعتباري، لأي متحكم أو معالج بما يلي: تعيين موظف مختص مسئول عن حماية البيانات الشخصية داخل كيانه القانوني وهيكله الوظيفي بما يضمن استقلاليته وعدم التأثير على قراراته المتعلقة بالتزاماته الواردة في المادة رقم ٩. قيد الموظف المسئول عن حماية البيانات الشخصية في سجل مسئولي حماية البيانات الشخصية بالمركز، والإعلان عن ذلك. توفير الإمكانيات اللازمة لممارسة مسئول حماية البيانات الشخصية اختصاصاته وفقاً لمقتضيات وظيفته. ويكون الشخص الطبيعي المتحكم أو المعالج هو المسئول عن تطبيق أحكام هذا القانون. وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد وآليات التسجيل.

رقم المادة	مادة ١١
موضوع المادة	الدليل الرقمي
نص القانون الحالي	يكون للدليل الرقمي المستمد من البيانات الشخصية طبقًا لأحكام هذا القانون ذات الحجية في الإثبات المقررة للأدلة المستمدة من البيانات والمعلومات الخطية متى استوفت المعايير والشروط الفنية الواردة باللائحة التنفيذية لهذا القانون.
التعليق على نص القانون	لم يحدد القانون علاقة الدليل الرقمي بالبيانات الشخصية فليست كل بيانات تصلح أن تكون دليلًا رقميًا. وأحال نص المادة إلى اللائحة التنفيذية كما ذكرت المادة نصًا كمادة الدليل الرقمي رقم ١١ في قانون مكافحة جرائم تقنية المعلومات ١٧٥ لعام ٢٠١٨
المقترح	يجب أن يعمم الإثبات والتوقيع والتوثيق والموافقات الرقمية على كل جوانب القانون ويفرد لذلك بندًا في التعريفات ويلحق بالمواد المرتبطة تحقيقًا لفكرة الرقمنة وللوصول لنتائج أكثر فاعليه.

رقم المادة	مادة ١٢
موضوع المادة	البيانات الشخصية الحساسة
نص القانون الحالي	.... وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر.
التعليق على نص القانون	ألزم المشرع موافقة ولي الأمر في حالة إجراء أي عملية تتعلق ببيانات الطفل ولم يذكر الوصي. لم يحدد المشرع طبيعة موافقة ولي الأمر ولا شكلها لم يحدد المشرع الطفل ولم يضع له معيار سني؛ فلم يفرق بين من هو عمره ٥ سنوات و ١٩ واعتبرهم أطفال.
المقترح	تحديد شكل الموافقة المطلوبة من ولي الأمر ضرورة تحديد شكل الموافقة ومعرفة طبيعتها (مكتوبة أم إلكترونية) يجب وضع معيار لتحديد الطفل ورد بمقترح اللجنة المشتركة تحديد سن الطفل بـ ١٦ سنة

رقم المادة	مادة ١٦
موضوع المادة	نقل البيانات عبر الحدود دون موافقة الشخص المعنى بالبيانات
التعليق	أجاز المشرع للمتحكم أو المعالج إتاحة البيانات لمتحكم آخر خارج مصر بترخيص من المركز، ولم يشترط موافقة الشخص المعنى، وهو ما يتعارض مع أهم حقوقه
نص القانون الحالي	يجوز للمتحكم أو المعالج، بحسب الأحوال، إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية بترخيص من المركز متى توافرت الشروط الآتية...
تساؤلات يثيرها القانون	التخوف من الإضرار بمصالح الشخص المعنى بالبيانات
المقترح	اشتراط الحصول على الموافقة على إتاحة البيانات عبر الحدود

رقم المادة	مادة ١٧
موضوع المادة	التسويق الإلكتروني المباشر
التعليق	مثال غير موفق
التعليق على نص القانون	تضيق النطاق بشكل غير فعال
التساؤلات التي يثيرها القانون	لماذا أفرد المشرع نصًا للتسويق الإلكتروني المباشر؟
المقترح	كان من الأجدى والأنسب وضع إطار عام للمعاملات الرقمية في التعامل مع البيانات لأغراض تجارية. أضاف مشروع اللجنة المشتركة للشرط الأول ما يلي: "إذا كان الاتصال الإلكتروني يتسق مع غرض ونشاط المتحكم في التسويق لمنتجاته وخدماته دون الإخلال بمصالح وحقوق الشخص المعنى بالبيانات"

رقم المادة	مادة ٢٠
موضوع المادة	تشكيل مجلس إدارة المركز
نص القانون الحالي	يكون للمركز مجلس إدارة يشكل برئاسة الوزير المختص وعضوية كل من: ١- ممثل عن وزارة الدفاع....٢- ممثل عن وزارة الداخلية ..
التعليق على نص القانون	تضمن التشكيل ممثلي جهات الأمن القومي الواردة في التعريف في المادة الأولى، ولكنه لم يشر لممثل رئاسة الجمهورية ... كما نص على وجود ثلاثة أشخاص من ذوي الخبرة يختارهم الوزير المختص، دون أن يحدد مجال تخصصهم أو خبرتهم
المقترح	إضافة ممثل لرئاسة الجمهورية ضمن أعضاء المجلس، وتحدد نوع الخبرة المطلوبة في الأشخاص ذوي الخبرة الذين يختارهم الوزير

التشريعات المصرية
المنظمة لحماية البيانات

٢- التشريعات المصرية المنظمة لحماية البيانات

تسلسل	القانون	المواد المرتبطة بقانون حماية البيانات الشخصية
١	قانون التوقيع الإلكتروني (٢٠٠٤/١٥) ولائحته التنفيذية	القانون: ٢٠ و٢١
		اللائحة: ١
٢	قانون الجرائم الإلكترونية (٢٠١٨/١٧٥) ولائحته التنفيذية	القانون: ٢٥
		القانون: ٢٩
		القانون: ٣٥
٣	قانون البنك المركزي (١٩٤ / ٢٠٢٠)	مادة ١٦
٤	قانون التأمين الصحي (٢ / ٢٠١٨)	مادة ٤٧
٥	قانون الطفل (١٢ / ١٩٩٦)	مادة ١١٦ مكرر / ب
٦	قانون العقوبات (٥٨ / ١٩٣٧)	مادة ٣٠٩ مكرر
٧	قانون حماية المستهلك (١٨١ / ٢٠١٨)	مادة ٢٩
٨	قانون الأحوال المدنية (٩٤/٤٤٣)	مادة ١٣
٩	قانون تنظيم الاتصالات (١٠ / ٢٠٠٣)	مادة ٣/٢٨
		مادة ٢٩
		مادة ٥٨
		مادة ٦٤

موضوع المواد
بيانات التوقيع الإلكتروني والوسائط الإلكترونية
تعريفات
انتهاك الخصوصية ومشاركة البيانات الشخصية دون موافقة صاحب الشأن (م ٤١ من قانون حماية البيانات الشخصية)
مسئولية القائم على إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي عن تعريض أي منها لإحدى الجرائم المنصوص عليها في القانون (م ٤٠ من قانون حماية البيانات الشخصية)
مسئولية القائم على إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي عن الإبلاغ عن تعرض أي مما سبق لأحد الجرائم المنصوص عليها في القانون (م ٧ و٤٧ من قانون حماية البيانات الشخصية)
إنشاء نظام لتسجيل بيانات العملاء لإعداد الدراسات اللازمة لتعزيز الشمول المالي والخدمات المصرفية، طبقًا للضوابط والإجراءات التي يحددها مجلس الإدارة مع مراعاة المحافظة على سريتها
بشأن التزام كافة الجهات العامة والخاصة بتزويد هيئة الاعتماد والرقابة بكافة البيانات الشخصية الخاصة بالمنتفعين بنظام التأمين الصحي الشامل
عقوبة نشر بيانات الأطفال المعرضين للخطر أو المخالفين للقانون
عقوبة انتهاك حرمة الحياة الخاصة
إفشاء البيانات الخاصة بالمستهلك
سرية البيانات والمعلومات الخاصة بالأحوال المدنية
بشأن البيانات التي يفصح عنها مقدم الخدمة لإثبات تضرره من فعل أحد مشتركي الشبكة الخاصة بمقدم خدمة اخر
بشأن سلطة الجهاز القومي لتنظيم الاتصالات في طلب أي بيانات متعلقة بنزاع منظور أمامه
بشأن جمع وحفظ وحماية بيانات مستخدمي الطيف الترددي
بشأن التزام مقدمي خدمات الاتصالات ووكلائهم بالحصول على بيانات دقيقة عن مستخدميها من المواطنين.


A1
INNOVATION
INNOVATION
DATA
Data-A

المواد التي أحال فيها قانون حماية البيانات إلى لائحته التنفيذية مع المعايير التقنية المقترحة

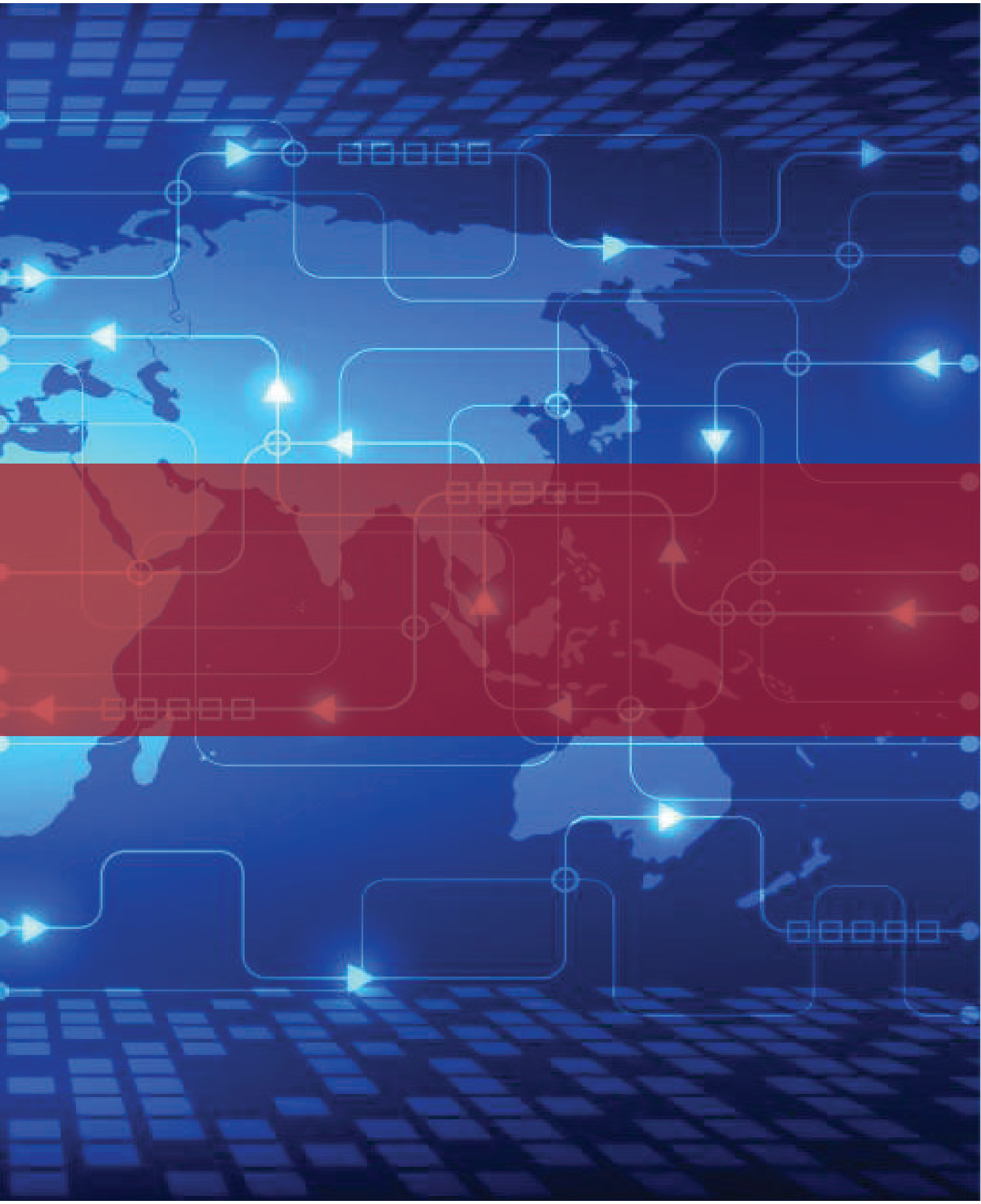
٣- المـواد التـي أحـال فيـهـا قـانـون حمـايـة البيـانـات إلى لائحته التنفيذية مع المعايير التقنية المقترحة

رقم المادة	الموضوع	التكليف
٤ (قانون الإصدار)	موعد صدور اللائحة التنفيذية	صدور اللائحة خلال ستة أشهر من تاريخ العمل بالقانون
٣	شروط جمع ومعالجة والاحتفاظ بالبيانات الشخصية	تحديد السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين للبيانات الشخصية
٤	التزامات المتحكم	تحديد السياسات والإجراءات والضوابط والمعايير الفنية لتلك الالتزامات
٥	التزامات المعالج	تحديد السياسات والإجراءات والضوابط والشروط والتعليمات والمعايير القياسية لالتزامات المعالج
٧	الالتزام بالإخطار والإبلاغ	تحديد الإجراءات الخاصة بالإبلاغ والإخطار

	المعايير التقنية المقترحة
	• BS 10012 Personal Information Management System • ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework • ISO/IEC 29101:2013 Information technology — Security techniques — Privacy architecture framework • ISO/IEC 27701:2019 • Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines • ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT • ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors • NIST Cybersecurity Standards • PCI DSS في حالة وجود معلومات مالية
	نفس المعايير
	نفس التوصيات السابقة

رقم المادة	الموضوع	التكليف
٨	سجل قيد مسئولي حماية البيانات الشخصية	شروط القيد وإجراءاته وآليات التسجيل
٩	التزامات مسئول حماية البيانات الشخصية	تحديد الالتزامات والإجراءات والمهام التي يجب على مسئول حماية البيانات القيام بها ولم ترد بهذه المادة
١١	حجية الدليل الرقمي المستمد من البيانات الشخصية	تحديد المعايير والشروط الفنية التي يجب أن تستوفيها البيانات الشخصية حتى يعد للدليل الرقمي المستمد منها نفس حجية الإثبات لنظيره الخطي.
١٢	البيانات الشخصية الحساسة	تحديد معايير وضوابط معالجة والتحكم في البيانات الشخصية الحساسة بما فيها بيانات الأطفال
١٤	البيانات الشخصية عبر الحدود	تحديد السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود
١٦	الترخيص للمتحكم أو المعالج بإتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية	تحديد الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لإتاحة تلك البيانات خارج حدود جمهورية مصر العربية
١٨	التسويق الإلكتروني المباشر	تحديد القواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر

	المعايير التقنية المقترحة
	• ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence • NIST Digital Forensics Framework • NIST SP 80086- Guide to Integrating Forensic Techniques into Incident Response • NIST SP 80088- Guidelines for Media Sanitization • SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence • ENISA Digital Forensics Guides • Guides for Handling Digital Evidence, National Institute of Justice, USA • ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence

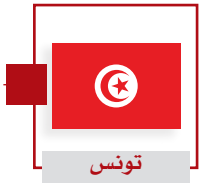



خريطة لنماذج قوانين حماية
البيانات الشخصية حول العالم

خريطة

لنماذج قوانين حماية البيانات الشخصية حول العالم

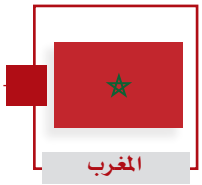
شمال إفريقيا والشرق الأوسط:



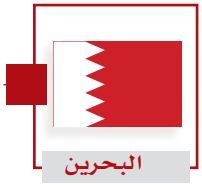
قانون ٦٣ لسنة ٢٠٠٤ بشأن حماية البيانات الشخصية.

المواد ٥٦ و ٦١ و ٧٥ من قانون مكافحة الإرهاب وجرائم غسيل الأموال، تعالج مسألة الشخص المعنى بالبيانات وحالات السماح باستخدام البيانات الشخصية.

في عام ٢٠١٨ تم تقديم مسودة لقانون جديد لحماية البيانات الشخصية يتوافق مع اللائحة الأوروبية لحماية البيانات (GDPR) إلى البرلمان التونسي.

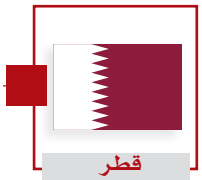


قانون رقم ٠٩-٠٨ لسنة ٢٠٠٩ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية، مع المرسوم التنفيذي رقم ٢-٠٩-١٦٥ لسنة ٢٠٠٩، يمثلان معًا قانون حماية البيانات في المغرب.



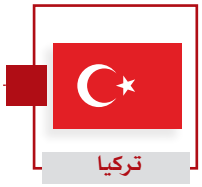
قانون رقم ٣٠ لسنة ٢٠١٨ لحماية البيانات الشخصية PDPL

دخل حيز النفاذ في أغسطس ٢٠١٩



قانون رقم ١٣ لسنة ٢٠١٦

دخل القانون حيز النفاذ في عام ٢٠١٧ إلا أن لوائحه التنفيذية لم تصدر بعد، ومن المتوقع صدورها خلال العام الجاري ٢٠٢٠.



قانون رقم ٦٦٩٨ لسنة ٢٠١٦، القائم على التوجيه الأوروبي رقم EC/46/95

اللائحة المتعلقة بمحو، وتدمير، وإخفاء البيانات الشخصية رقم ٣٠٢٢٤ لعام ٢٠١٧.

لائحة إجراءات ومبادئ مجلس حماية البيانات الشخصية، رقم ٣٠٢٤٢ لسنة ٢٠١٧.

لائحة سجل المتحكمين في البيانات، رقم ٣٠٢٨٦ لسنة ٢٠١٧.

لائحة تنظيم هيئة حماية البيانات الشخصية، رقم ٣٠٤٠٣ لسنة ٢٠١٨.

قرار مجلس حماية البيانات الصادر بتاريخ ٣١ يناير ٢٠١٨، برقم ١٠ / ٢٠١٨، بشأن التدابير المطلوب اتخاذها من قِبَل المتحكمين بالبيانات في معالجتهم للفئات الخاصة من البيانات الشخصية.

إفـــريقـــيـــــا:

- قانون حماية المعلومات الشخصية رقم ٤ لسنة ٢٠١٣، POPIA.
- سيدخل القانون حيز النفاذ بشكل كامل فـ ي ٣٠ / ٦ / ٢٠٢١.
- هناك بعض بنود هذا القانون دخلت وحدها دون بقية القانون حيز النفاذ منذ ١ / ٧ / ٢٠٢٠ منها:
  - الحالات الثمانية للمعالجة القانونية.
  - القيود على معالجة البيانات الشخصية ذات الطابع الخاص والبيانات الشخصية المتعلقة بالأطفال.
  - الأحكام الخاصة بالاستثناءات.
  - المتطلبات الخاصة بالتصاريح المسبقة.
  - الأحكام الخاصة بإنفاذ القانون، وبالجرائم والعقوبات.
  - أحكام عامة متعلقة بالرسوم، وبالتدابير الانتقالية.

- قانون حماية البيانات، رقم ١١/٢٢، لسنة ٢٠١١.
- قانون حماية النظم المعلوماتية والشبكات، رقم ١٧/٧، لسنة ٢٠١٧.

- قانون رقم ٨٤٣ لسنة ٢٠١٢
- القانون لم يدخل حيز النفاذ بعد، ومن المتوقع أن يُنشر بالجريدة الرسمية وينفذ خلال العام الجاري.

آســـيـــــــا:

كازاخستان

قانون رقم ١٣ لسنة ٢٠١٦

تركمانستان

قانون رقم ٥١٦-V لسنة ٢٠١٧.

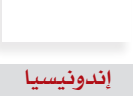
كوريا الجنوبية

قانون حماية البيانات PIPA الصار في عام ٢٠١١.

اليابان

قانون حماية البيانات، رقم ١١/٢٢، لسنة ٢٠١١.

قانون حماية النظم المعلوماتية والشبكات، رقم ١٧/٧، لسنة ٢٠١٧.



إندونيسيا

قانون رقم ١١ لسنة ٢٠٠٨ بشأن المعاملات والمعلومات الإلكترونية EIT Law والمعدل بالقانون رقم ١٩ لسنة ٢٠١٦.

القرار رقم ٧١ لسنة ٢٠١٩ بشأن أحكام المعاملات والنظم الإلكترونية، ولائحته التنفيذية.

لائحة وزير الاتصالات والمعلومات رقم ٢٠ لسنة ٢٠١٦ بشأن حماية البيانات الشخصية في النظم الإلكترونية.

نماذج من أهم قضايا حماية البيانات الشخصية حول العالم

نماذج من أهم قضايا حماية البيانات الشخصية حول العالم

قضية ليندكفيست Lindqvist v Åklagarkammaren i Jönköping (٢٠٠٣)

أوضحت محكمة العدل الأوروبية أن نشر بيانات شخصية على صفحة إنترنت يعد من قبيل المعالجة التى تجعلها فى هذة الحالة مشمولة بالحماية التى تكفلها توجيهات الاتحاد الأوروبي.

ديوران ضد هيئة الخدمات المالية Durant v. Financial Services Authority (٢٠٠٣)

قضت المحكمة فى صدد تعريف البيانات الشخصية بأن مجرد ذكر شخص صاحب بيانات بوثيقة لدى المتحكم لا يعد –بالضرورة– من قبيل البيانات الشخصية، وأن البيان لا يعتبر شخصي إلا إذا كان من شأنه أن يؤثر على حق صاحبه فى الخصوصية فى أى من جوانب حياته سواء الشخصية أو العملية.

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia (٢٠٠٨)

حكمت محكمة العدل الأوروبية أن جمع البيانات الشخصية ونشرها ونقلها على قرص مضغوط عن طريق الرسائل النصية كلها أشكال لمعالجة البيانات الشخصية بغض النظر عن ما إذا كانت البيانات التى تم نشرها قد تم تعديلها أم لا.

مركز حماية البيانات وحرية المعلومات ضد بافارين ليجر Commission v. Bavarian Lager (٢٠٠٨)

قضت محكمة العدل الأوروبية برفض اعتبار التحليل القانونى الذى تقوم به جهة ما للرد على طلب تقدم به صاحب البيانات لها من قبيل البيانات الشخصية إلا أن ذلك لا يتعارض مع أن يكون تسليم بيانات شخصية استجابةً لطلب حصول على تلك بيانات يعد من قبيل أعمال المعالجة.

شوارز ضد بوشام SCHWARZ V. BOCHUM (٢٠١٤)

تقدم المدعى بالطلب إلى Stadt Bochum للحصول على جواز سفر، لكنه رفض أخذ بصمات أصابعه، وبالتالي رفض Stadt طلبه. ورفع دعوى أمام محكمة الإحالة لاستخراج جواز سفر دون أخذ بصماته. فى هذا الصدد، قضت المحكمة بأن بصمات الأصابع تشكل بيانات شخصية، لأنها تحتوي بشكل موضوعي على معلومات فريدة عن الأفراد مما يسمح بتحديد هويتهم بدقة.

ماكس شريمز ضد مركز حماية البيانات الأيرلندي Max Schrems v. Data Protection Commissioner (مارس ٢٠١٥)

قضية نُظرت أمام محكمة العدل الأوروبية بناءً على شكوى قدمها محامي يُدعى ماكس شريمز إلى مركز حماية البيانات بأيرلندا ضد فيسبوك حيث قامت الأخيرة بنقل بيانات الشاكي وبيانات مواطني الاتحاد الأوروبي بشكل عام من أوروبا إلى الولايات المتحدة الأمريكية. أدت هذه القضية إلى إلغاء محكمة العدل الأوروبية العمل باتفاقية "Safe Harbor" المنظمة لنقل البيانات بين الاتحاد الأوروبي والولايات المتحدة الأمريكية.

جوجل إسبانيا ضد مركز حماية البيانات الإسباني Google Spain v. Data Protection Commissioner (فبراير ٢٠١٣)

صرحت المحكمة بأن تعديل أو تغيير (Alternation) البيانات الشخصية يعد فى حد ذاته من قبيل أعمال المعالجة إلا أنه يمكن أن تنشأ عمليات معالجة أخرى للبيانات دون أن يتم تعديلها. وأشارت المحكمة إلى أن قدرة محرك البحث على "إتاحة" بيانات خاصة بتاريخ وتفاصيل البحث الذى قد يقوم به شخص تعد من قبيل المعالجة، كما هو الحال بالنسبة لكل العمليات السابقة على الإتاحة، مثل قيام محرك البحث بجمع وتسجيل وتنظيم وتخزين تلك البيانات بصورة تلقائية ومستمرة وممنهجة.

نواك ضد مركز حماية البيانات وحرية المعلومات Nowak v. Data Protection Commissioner (٢٠١٧)

اعتبرت محكمة العدل الأوروبية أن الإجابات المكتوبة التي قدمها الممتحن وأي تعليقات أدلى بها الفاحص فيما يتعلق بهذه الإجابات تشكل بيانات شخصية تتعلق بذلك الممتحن. ذكرت المحكمة أن الحكم بخلاف ذلك سيؤثر في استبعاد تلك المعلومات تمامًا من الالتزام بالامتثال لمبادئ حماية البيانات والضمانات، وحقوق الحصول والتصحيح وموضوع البيانات.

قضية برير Breyer Case (٢٠١٦)

أكدت المحكمة أنه وفقًا لقانون الاتحاد الأوروبي، فإن معالجة البيانات الشخصية تعتبر قانونية، من بين أمور أخرى، إذا كانت كذلك ضرورية لتحقيق هدف مشروع يسعى إليه المتحكم أو الطرف الثالث التي يتم نقل البيانات، بشرط أن تكون المصلحة أو الحقوق والحريات الأساسية موضوع البيانات لا يتجاوز هذا الهدف.

ZXC v. Bloomberg LP (٢٠١٩)

قضية تم رفعها على أساس أن الأشخاص الذين تم التحقيق معهم من قبل جهات إنفاذ القانون لهم الحق في الخصوصية بشكل عام. ذكرت صحيفة اسم المدعي في سياق الاستشهاد بمعلومات سرية تم الحصول عليها من وكالة إنفاذ القانون في المملكة المتحدة. نجح المدعي في الحصول على ٢٥٠٠٠ جنيه إسترليني.

Google LLC v. CNIL (٢٠١٩)

وجدت محكمة العدل أن النطاق الإقليمي للحق في النسيان كان محدودًا من الناحية القضائية، وبالتالي لا يمكن تطبيقه على أسماء النطاقات العالمية.

GC & Others v. CNIL (٢٠١٩)

تم طرح عدد من الأسئلة على المحكمة، كلها تتعلق بشكل عام بمسألة كيفية تطبيق الحظر على معالجة البيانات الشخصية الحساسة بموجب التوجيه على محركات البحث. أراد المدعون الحصول على نتائج مختلفة من عمليات البحث عن أسمائهم التي تم حذفها من نتائج بحث Google. وخلصت المحكمة إلى أنه لا يوجد حظر شامل على معالجة البيانات الشخصية الحساسة بواسطة محركات البحث بموجب توجيه حماية البيانات، وبالتالي رفض فرض إلغاء مرجعية للنتائج.

شركة H&M ضد مركز حماية البيانات وحرية المعلومات بهامبورج H&M v. Data Protection Commissioner of Hamburg (٢٠٢٠)

لقد كلف عدم التزام شركة H&M (Hennes & Mauritz) باتباع الإجراءات القانونية اللازمة عند إجراء عمليات المعالجة وتحديدًا التنميط والإيداع مبالغ طائلة مؤخرًا فى أكتوبر من هذا العام (٢٠٢٠)، حيث فرض مفوض هامبورج لحماية البيانات الشخصية وحرية المعلومات غرامة قدرها ٣٥,٣ مليون يورو على الشركة بسبب انتهاكاتها للبيانات الشخصية لموظفيها؛ حيث جمعت الشركة واحتفظت بتسجيلات لموظفيها تحتوي بيانات على مستوى عال من الخصوصية، ولفترات زمنية طويلة. كما تم استخدام تلك البيانات فى تقييم أداء العاملين، وعمل ملفات تعريفية مفصلة لهم، تستخدم وتؤثر فى اتخاذ قرارات تجاههم. والجدير بالذكر أن الموظفين لم تكن لديهم أدنى فكرة عن ذلك إلا حين حدث خطأ فني في أنظمة حواسيب الشركة مما جعل هذه البيانات متاحة لعدة ساعات فى أكتوبر من العام الماضي.

CLETs
Centre for Law & Emerging Technologies

مركـز بحـوث القانون والتكنولوجيا

مركز بحوث القانون والتكنولوجيا يعد أول مركز بحوث قانوني في مصر والشرق الأوسـط متخصص في دراسة الموضوعـات المتعلقة بتنظيـم التكنولوجيا وما يتعلق بها من أمـور ومسائل قانونيـة.

www.clets.org

THE BRITISH UNIVERSITY IN EGYPT

JOLETS

Journal of Law and Emerging Technologies

مجلــة بحـوث
القانون والتكنولوجيا

مجلة بحوث "**القانون والتكنولوجيا**" أول مجلة بحوث قانونيــة متخصصة دورية علمية محكمة نصف سنوية تصدر عن كلية القانون بالجامعة البريطانية.

www.jolets.org

2021

The British University in Egypt
EL Sherouk City, Suez Desert Road, Cairo11837 - P.O. Box 43

19283, +202 26890000, +202 26300013 / 14 / 15/ 16 /17 /18

https://www.bue.edu.eg/index.php/law-home

www.facebook.com/BUE.Faculty.of.law

twitter.com/buefacultyoflaw