مسار
TECHNOLOGY & LAW COMMUNITY

# قانون حماية البيانات الشخصية

## تعزيز للحق في الخصوصية أم إيهام بتحسين البيئة التشريعية ؟

## قانون حماية البيانات الشخصية

# تعزيز للحق في الخصوصية أم إيهام بتحسين البيئة التشريعية ؟

المحتويات

## المقدمة

يواجه المصريون ضعفًا في الحماية القانونية لحقهم في الخصوصية على مستويات عديدة، فمن البيانات التي تحصل عليها الجهات الحكومية من الأفراد أثناء إجراء المعاملات الإدارية اليومية، إلى المعلومات التي تجمعها شركات القطاع الخاص عن عملائها، توجد ثغرات تشريعية كثيرة تُعرِّض الحياة الخاصة لأصحاب هذه البيانات والمعلومات للإفشاء دون إرادتهم. وفي ضوء هذا النقص التشريعي لحماية البيانات الشخصية للأفراد، طالب المجتمع المدني المصري على مدار العقدين الماضيين بضرورة التدخل التشريعي لملء هذا الفراغ. وقد تبنت السلطات المصرية أخيرًا حزمة تشريعات تتعلق بتنظيم استخدام تكنولوجيا المعلومات، إلا أن التدخل التشريعي للسلطات في هذا المجال لم يأتِ بهدف حماية حقوق الأفراد في الخصوصية، بقدر ما جاء لتمكين السلطات من السيطرة على الفضاء الرقمي. فبعد ما يقرب من عامين ونصف العام قضتهم لجنة الاتصالات بمجلس النواب المصري في مُناقشة مشروع قانون حماية البيانات الشخصية، وافق المجلس أخيرًا على تمرير القانون، ثم قام رئيس الجمهورية بالتصديق عليه في شهر يوليو من العام الحالي[1]. وقد شهدت عملية وضع القانون مشاركة واسعة للشركات العاملة في قطاع الاتصالات ومشاركة محدودة لمنظمات المجتمع المدني المصري. ومن المثير للاهتمام اقتصار قانون حماية البيانات الشخصية على وضع أطر تنظيمية لحماية البيانات المُعالجة إلكترونيًا فقط، في الوقت الذي تنطوي أغلب التعاملات اليومية، سواء مع القطاع الحكومي أو غير الحكومي، على الإفصاح عن بيانات شخصية غير معالجة إلكترونيًا بشكل روتيني. ولا توجد تشريعات أخرى تعالج حماية البيانات غير الإلكترونية أو تنظم مشاركتها مع أطراف مُختلفة. وهو ما يؤكد أن إصدار قانون حماية البيانات لم يكن غرضه الحقيقي حماية خصوصية الأفراد، وإنما استخدام هذا التشريع في مخاطبة المجتمع الدولي بأن مصر لديها بيئة قانونية مهيئة للاستثمار تمكنها من عقد شراكات مع أطراف المجتمع الدولي في مجال تكنولوجيا المعلومات.

اعتمد المُشرِّع المصري عند وضع قانون حماية البيانات الشخصية، على الأخذ بالقواعد المنصوص عليها باللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي (GDPR)، إلا أن المُشرِّع قد أدخل تعديلات على هذه القواعد أدت إلى صياغة بعض نصوص القانون بشكل مقتضب، خاصة فيما يتعلق بحقوق الأفراد الذين تتم مشاركة بياناتهم الشخصية مع أطراف مختلفة وضمانات حماية الحق في الخصوصية لأصحاب البيانات.

كما أحال القانون عددًا كبيرًا من الإجراءات المتعلقة بتفعيل قانون حماية البيانات إلى اللائحة التنفيذية للقانون والتي لم تصدر حتى الآن، ورغم ذلك يُعتبر القانون خطوة تشريعية هامة، تحتاج جهودًا كبيرة لإنفاذها على أرض الواقع.

---

١ - قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ والمنشور بالجريدة الرسمية بالعدد ٢٨ مُكرر هـ بتاريخ ١٥ يوليو ٢٠٢٠.

ومن أهم الخطوات التي ترى "مسار" أنها مصيرية لجعل قانون حماية البيانات أداة فعالة لحماية خصوصية الأفراد، هي فلسفة التشريع ذاته. فإقدام السلطات المصرية على تنظيم عملية مشاركة البيانات الشخصية يجب أن ينطلق من إيمان حقيقي بحق الأفراد في الخصوصية وليس من مجرد رغبة السلطات في تهيئة بيئة الاستثمار. لكن بقراءة متمعنة في نصوص قانون حماية البيانات الشخصية، نجد أن الحق في الخصوصية لم يكن الدافع الرئيسي لتبني هذا القانون، وإنما استهداف توفير مناخ تشريعي جاذب لحزم المساعدات المالية بصورها المختلفة. وبالرغم من مشروعية هذا الهدف، فإنه لا ينبغي ألا يأتي على حساب حق الأفراد في الخصوصية المحمي بموجب كلٍّ من القانون الدولي والدستور المصري.

## وقد عَرَّف قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ 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 بالاسم، أو بالصوت، أو بالصورة، أو برقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية."

إلا أن قانون حماية البيانات الشخصية استثنى بعض الجهات من الخضوع لأحكامه بشكل مجمل. وتضم الجهات الخارجة عن نطاق سريان القانون، على سبيل المثال، المؤسسات الخاضعة للبنك المركزي وجهات الأمن القومي. وكان يجب على السلطات التشريعية استثناء بعض أنواع البيانات التي تحوزها هذه الجهات بمناسبة ممارستها لوظائفها من الخضوع لأحكام القانون وليس إعفاء كافة ما تحوزه هذه الجهات من بيانات ومعلومات من الخضوع لأحكامه، وذلك لانتهاك هذا التوسع لمبدإ سيادة القانون. حيث يجب أن تخضع هذه الجهات أيضًا للالتزام القانوني بحماية خصوصية الأفراد..

تأتي هذه الورقة في ظل سياق تشريعي وإجرائي غير مُكتمل، حيث تعمل الحكومة المصرية الآن على وضع اللائحة التنفيذية لقانون حماية البيانات، كما أن الفترة المُقبلة قد تشهد إنشاء المفوضية المُتعلقة بحماية البيانات (مركز حماية البيانات الشخصية) ولجانه المُختلفة، إذا ما قُدِّر لهذا القانون الدخول في حيز النفاذ. لذلك تهدف الورقة إلى تحليل أهم الأحكام التي ذكرها قانون حماية البيانات الشخصية، بالإضافة إلى وضع بعض التعليقات على الصياغات التشريعية، كما تُحاول الورقة إلقاء نظرة عامة على الأوضاع التشريعية التي تم خلالها إقرار القانون، وكذلك فهم الأهداف التي دفعت المُشرِّع إلى إصداره في هذا التوقيت.

تعتمد الورقة على القراءة المُباشرة لنصوص قانون حماية البيانات الشخصية، في ضوء التقارير البرلمانية الصادرة عن لجنة الاتصالات أثناء مُناقشة مشروع القانون، وعلى ما جاء بالمذكرة الإيضاحية المُرفقة بمشروع القانون المُقترح من الحكومة المصرية، بالإضافة إلى المعايير المُتعلقة بصياغة قوانين حماية البيانات المنصوص عليها بـ"دليل المُشرِّع لقانون حماية البيانات الشخصية" الصادر عن مُنظمة "أكسس ناو" [٢].

## المخاطبون بأحكام القانون

يضع قانون حماية البيانات الشخصية التزامات أساسية على الأفراد والجهات التي قد تحوز البيانات الشخصية للمُستخدمين، سواء كانت حيازة البيانات لأسباب تتعلق بطبيعة عملها أو لأي سبب آخر. ويُفرق القانون بين هذه الالتزامات حسب طبيعة الأشخاص الذين يتعاملون في البيانات الشخصية. وبالرغم من تركيز القانون على توضيح الصور المختلفة للتعامل مع البيانات الشخصية، كالحيازة، والتحكم في، والمعالجات المختلفة للبيانات الشخصية، والالتزامات القانونية الواقعة على الحائز أو المعالج أو المتحكم، لم يتطرق القانون بشكل تفصيلي وكافٍ للحقوق المكفولة محل الحماية، والإجراءات التي يمكنهم اتخاذها في حال انتهاك حقوقهم بل ركزت صياغة القانون على التزامات الأطراف الحائزة للبيانات.

وقد عرّف القانون الحائز للبيانات:

"أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليًا ببيانات شخصية في أي صورة من الصور، أو على أي وسيلة تخزين سواء أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة" [٣].

ثم فرّق القانون بين الجهات المُختلفة التي تحوز البيانات بسبب عملها حيث يضع تعريفًا لـ"المتحكم" في البيانات بأنه:

"أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقًا للغرض المحدد أو نشاطه" [٤].

وأخيرًا يُعرِّف القانون "المعالج" للبيانات بأنه:

"أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته" [٥].

---

٢ - الدليل الصادر عن مُنظمة أكسس ناو بعنوان: "إنشاء إطار المعطيات الشخصية:
دليل للمشرعين حول ما يجب فعله واجتنابه، دروس مُقتبسة من القانون العام للاتحاد الأوروبي".

## الهدف من إقرار قانون حماية البيانات الشخصية

لم تكن هناك سياسة تشريعية واضحة تتعلق بقطاع الاتصالات وتكنولوجيا المعلومات يُمكن من خلالها فهم الاحتياجات التشريعية التي تفرض نفسها على جدول أعمال المُشرِّع المصري، أو فهم ترتيب الأولويات المُتعلقة بإصدار بعض التشريعات، لذلك اعتمدت الورقة على التصريحات الصحفية الصادرة عن أعضاء لجنة الاتصالات بمجلس النواب، ومحاولة استنتاج الهدف من إقرار قانون حماية البيانات من خلال قراءة مذكرته الإيضاحية والتقارير البرلمانية ذات الصلة بهذا القانون.

خلال الدورة البرلمانية الماضية الممتدة من أكتوبر ٢٠١٥ وحتى سبتمبر ٢٠٢٠، صدر عن لجنة الاتصالات بمجلس النواب المصري العديد من التصريحات التي أفادت بعمل المجلس على إقرار ثلاثة قوانين رئيسية، أولها كان قانون الجرائم الإلكترونية والذي صدر في الربع الثالث من عام ٢٠١٨ تحت عنوان قانون "مُكافحة جرائم تقنية المعلومات"، وثانيها قانون حماية البيانات الشخصية، والذي صدر في منتصف عام ٢٠٢٠، تحت عنوان قانون: "حماية البيانات الشخصية"، وأخيرًا قانون حرية تداول المعلومات، الذي أُرسلت مسودته إلى البرلمان في منتصف عام ٢٠١٨، ورغم بدء مُناقشة المسودة النهائية للقانون فإنه لم يُصدَر حتى انتهاء الدورة البرلمانية.

أشارت التصريحات والنقاشات البرلمانية إلى أن هناك ارتباطًا بين التشريعات الثلاثة، وأن هناك حاجة عاجلة إلى إقرار هذه القوانين. لم تكن هناك عقبات أمام إقرار قانون الجريمة الإلكترونية، حيث جاء هذا القانون ليَبسُط يد جهات إنفاذ القانون على الساحة الافتراضية عبر تقنين مُمارسات معادية لحقوق الإنسان والحريات الأساسية مثل حجب المواقع، وتجريم صور التعبير على الإنترنت، وأصبحت قواعده فيما بعد أساسًا لتوجيه الاتهامات الجنائية الفضفاضة في جرائم الرأي، بينما تأخر إصدار قانون حماية البيانات الشخصية، الذي قد يضع قيودًا على الجهات الحكومية في استخدام البيانات الشخصية للأفراد، وتم إرجاء إصدار قانون حرية تداول المعلومات لأسباب غير معروفة ولأجل غير معلوم.

---

٣ - المادة رقم ١ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.
٤ - المادة رقم ١ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.
٥ - المادة رقم ١ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

لم تكن الحاجة المُجتمعية إلى إقرار قانون توفّر قواعده الحماية اللازمة للبيانات الشخصية للمواطنين هي الهدف الرئيسي، حيث أن النقاشات البرلمانية والحكومية السابقة على إقرار القانون ذكرت أهدافًا مُختلفة، من بينها أن إقرار القانون سيسهم في رفع تصنيف مصر في مؤشر حقوق الإنسان[٦]، بينما تُشير المذكرة الإيضاحية المُرفقة بمشروع قانون حماية البيانات الشخصية إلى أهداف تتعلق بالعائد الاقتصادي من إقرار القانون، حيث تنتهي المذكرة إلى أن معرفة القيمة الاقتصادية للبيانات الشخصية تأتي بشكل أساسي من خلال عمليات التحليل الضخمة لهذه البيانات، كما تساهم حمايتها في تطوير وتنمية صناعة التعهيد (outsourcing) ، وصناعة مراكز البيانات، بما يحقق وفرة اقتصادية كبيرة تسهم في خلق مزيد من فرص العمل، وتشجع على جذب الاستثمارات في قطاعات الدولة المُختلفة. كما يؤكد على نفس المعنى ما ورد بالتقرير البرلماني المُشترك بين لجنة الاتصالات ولجنة الأمن القومي بالبرلمان المصري، والذي جاء به أن اهتمام الدولة بتشجيع الاستثمارات في مجال صناعة مراكز البيانات العملاقة سوف يساعد مصر على أن تصبح "ممر رقمي عالمي"، ولمّا كان ذلك يتطلب وجود بيئة تشريعية مُناسبة، جاء القانون ليهيئ المناخ الاستثماري في مصر ويساهم في تحسين سمعة الأداء الحكومي على المستوى الدولي. كما بينت هذه النقاشات أن المشروع يهدف إلى "التواكب مع المعيار العالمي الخاص بحماية البيانات الشخصية حاليًا في العالم".

فالمعيار الأساسي وهو اللائحة العامة لحماية البيانات الشخصية (GDPR) "وهي القواعد الذهبية الموجودة في العالم لحماية البيانات الشخصية للمُستخدمين"، كما يضمن القانون "حماية الاستثمارات الوطنية وخاصة المُتعاملة مع الاتحاد الأوروبي". ومن خلال هذه التصريحات يمكن القول بأن الهدف من إقرار قانون حماية البيانات الشخصية هو إعطاء انطباع للمجتمع الدولي حول وجود حماية قانونية لخصوصية الأفراد كأحد مؤشرات نجاح بيئة الاستثمار وليس حماية خصوصية الأفراد كهدف في حد ذاته.

---

٦ - تصريح صادر من النائب نضال السعيد رئيس لجنة الاتصالات وتكنولوجيا المعلومات بالبرلمان المصري البوابة الإلكترونية لجريدة الأهرام بتاريخ ٨ أكتوبر ٢٠١٨.

## استثناءات واسعة على حماية البيانات الشخصية

جاء إصدار قانون حماية البيانات متأخرًا في نهاية الدور التشريعي الأخير، حيث بدأت النقاشات حول مسودة القانون منذ نهاية عام ٢٠١٧، واستمرت المُناقشات البرلمانية حتى تمت الموافقة النهائية على القانون من البرلمان في بداية عام ٢٠٢٠ وإصداره من رئيس الجمهورية في منتصف عام ٢٠٢٠.

يرجع التأخير في إصدار القانون إلى الاعتراضات التي أُبديت من جهات إدارية مُختلفة، من بينها وزارة الداخلية المصرية، حيث عقدت لجنة الاتصالات وتكنولوجيا المعلومات، اجتماعًا في بداية عام ٢٠١٨، مع عدد من ممثلي وزارات "الداخلية" و"الدفاع" و"الخارجية"، لحسم المواد المتعلقة بالأمن القومي، المنصوص عليها بقانون حماية البيانات الشخصية المُقترح من ٦٠ نائبًا، وقد انتهت اللجنة إلى عدم سريان أحكام هذا القانون علي وزارتي الدفاع والداخلية، وذلك بعد تخوفهم من سريان أحكام القانون علي البيانات والمعلومات التي تجمعها وزارة الداخلية، ومنها التحريات بشكل عام، وبشكل خاص المعلومات المتعلقة بقضايا المخدرات والإرهاب، وكذلك المعلومات المتعلقة بالسجناء والمعلومات الخاصة بالطوائف وأصحاب العقائد والتركيبة الديمغرافية للسكان [٧].

ورغم الاستجابة لبعض طلبات جهات الأمن القومي واستثناء هذه الجهات من الخضوع لأحكامه، فإنه لم يُكتب لهذا المشروع الاستمرار، حيث تقدمت الحكومة بمشروع قانون آخر، وقد رُوعي في المشروع الذي تقدمت به الحكومة المصرية الاستثناءات على البيانات المُرتبطة بالأمن القومي، إلا أن الاعتراضات ظلت تُلاحق المشروع المُقدّم من الحكومة المصرية، حيث أرسل البنك المركزي في شهر يونيو ٢٠١٩ خطابًا إلى رئيس مجلس النواب، يُطالب فيه بعدم سريان أحكام القانون على البيانات الشخصية لعملاء الجهات الخاضعة لإشراف البنك المركزي تفاديًا لتداخل الاختصاصات بين البنك المركز المصري ومركز حماية البيانات الشخصية، وأسوة بالاستثناءات التي تم إقرارها، مثل البيانات الإحصائية الرسمية أو البيانات التي لدى جهات الأمن القومي [٨].

وقد انتهى البرلمان إلى إقرار عدد من الاستثناءات التي تسمح بعدم خضوع بعض البيانات أو البيانات التي تتحكم بها بعض الجهات الإدارية لقانون حماية البيانات الشخصية، وقد حددت مواد الإصدار سريان أحكام هذا القانون في شأن حماية البيانات الشخصية المعالجة إلكترونيًا جزئيًا أو كليًا لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة إلى الأشخاص الطبيعيين، وقد وضعت المادة الثالثة من مواد الإصدار عدم سريان أحكام القانون في بعض الحالات على النحو الآتي:

---

٧ - خبر بعنوان: اجتماع موسع بـ"لجنة اتصالات" البرلمان لإنهاء مواد "الأمن القومي" بقانون حماية البيانات
البوابة الإلكترونية لجريدة أخبار اليوم بتاريخ ١٣ يناير ٢٠١٨ .

٨ - خطاب مُحافظ البنك المركزي المُرسل إلى رئيس مجلس النواب المصري بتاريخ ٣٠ مايو ٢٠١٩ (مُرفق).

(المادة الثالثة)

لا تسري أحكام القانون المرافق على ما يأتي:

أولًا: البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير ويتم معالجتها للاستخدام الشخصي.

ثانيًا: البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني.

ثالثًا: البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألّا تستخدم في أغراض أخرى وذلك بدون الإخلال بالتشريعات المنظمة للصحافة والإعلام.

رابعًا: البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية.

خامسًا: البيانات الشخصية لدى جهات الأمن القومي وما تقدره لاعتبارات أخرى. ويجب على المركز، بناءً على طلبٍ من جهات الأمن القومي، إخطار المتحكِّم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية خلال مدة زمنية محددة، وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكِّم أو المعالِج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحدّدة به.

سادسًا: 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.

الاستثناءات التي تم النص عليها بقانون حماية البيانات اعتمدت معيارين مُختلفين لعدم الخضوع للضوابط المُتعلقة بحماية البيانات، المعيار الأول هو طبيعة البيانات، على سبيل المثال، البيانات الإحصائية التي يجمعها الجهاز المركزي للتعبئة العامة والإحصاء، أو البيانات التي يتم معالجتها للاستخدام الشخصي، وهذا النوع من البيانات قد يكون له مُبرر من الواقع، مثل جمع البيات بهدف المصلحة العامة أو أغراض البحث العلمي، أما المعيار الثاني فيستبعد بعض الجهات الإدارية من الخضوع بالكامل لأحكام القانون دون ضوابط مُحددة أو معايير يُمكن فهمها، فالقانون يُعطي صلاحيات غير مُحددة لحيازة البيانات ومُعالجتها مع غياب كامل للرقابة القضائية على هذه الإجراءات، وهو أمر لا يُمكن تصوره بشكل مُطلق دون وجود مُحددات تشريعية ترتبط بطبيعة البيانات التي تتحكم بها جهات مثل جهات الأمن القومي.

من المفهوم بالضرورة أن هناك بعض البيانات التي تتم مُعالجتها من هذه الجهات يصعب استخلاصها بحيث تكون خاضعة لأحكام القانون، ولكن يجب أن يكون ذلك في نطاق مُحدد، وإن كانت هناك بعض المُبررات التي يُمكن أن تسوقها جهات الأمن القومي لاستثناء بعض جوانب عملها من الخضوع للقانون، فإن هذا لا يعني عدم الخضوع بالكامل دون تحديد لأوجه الاستثناءات وبيان الأسباب التي تُبرر هذا الاستثناء.

القانون لم يستبعد جهات الأمن القومي فقط، ولكن امتد هذا الاستثناء إلى جهات أخرى، مثل استبعاد خضوع البنك المركزي والجهات الخاضعة لإشرافه من أحكام هذا القانون، وهو أمر لا يُمكن فهمه ويُفرِّغ القانون من مضمونه بشكل كبير، فاستبعاد القطاع المصرفي المصري بالكامل من الخضوع لأحكام القانون لا يتعارض فقط مع الحقوق الأساسية المنصوص عليها بالمادة ٥٧ من الدستور المصري والتي تحمي حق الأفراد في الخصوصية، بل إن هذا الاستثناء يتعارض مع الأهداف التي تبنّاها المُشرِّع فيما يتعلق بفلسفة وهدف القانون لجذب الاستثمار.

## ضمانات وحقوق المُستخدمين أثناء جمع ومعالجة البيانات

وضع قانون حماية البيانات الشخصية عددًا من الضمانات المُتعلقة بحقوق المستخدم، والتي أسماها القانون: "الشخص المعني بالبيانات"، وتعتبر هذه الضمانات هي القواعد الأساسية التي يجب الالتزام بها أثناء عملية جمع ومُعالجة البيانات الشخصية، ورغم أهمية هذه الضمانات والتي تُعتبر الهدف الأساسي لإصدار قانون حماية البيانات الشخصية، فإنها جاءت في صياغات مُقتضبة جدًا، لتنص على أصل الحق دون بيان مُفصل أو تعريفات للمفاهيم الأساسية المُتعلقة به، كما أن نصوص القانون قد وزّعت هذه الضمانات في صور مُختلفة، حيث أتت بشكل غير واضح في المادة الخاصة "بحقوق الشخص المعني بالبيانات وشروط جمع ومعالجة البيانات" وذُكر جزء منها في الالتزامات الواردة على المُتحكم أو المُعالج، كما أتت الأجزاء الأخيرة منها في صورة شروط وضوابط تتعلق بعملية جمع البيانات، وهو ما يُصعِّب على المخاطَبِين بالقانون فهم حقوقهم وإدراكها بشكل مُستساغ.

### مادة (٢):

لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشاؤها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا. ويكون للشخص المعني 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 في نطاق محدد.

٥- العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

٦- الاعتراض علي معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات. وباستثناء البند (٥) من الفقرة السابقة، يؤدي الشخص المعني 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.

بالإضافة إلى إشكالية صياغة الحقوق والضمانات المُتعلقة ببيانات المُستخدمين، هناك بعض الضمانات التي أغفلها النص الخاص بتنظيم حقوق المُستخدمين، من بين هذه الحقوق:

## الحق في العلم بأي خرق أو انتهاك :

أشار نص المادة ٢ من قانون حماية البيانات إلى حق المُستخدم في العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية، إلا أن النص لم يتحدث عن آلية الإبلاغ أو المدى الزمني الذي يجب أن يتم خلاله إخطار مَن وقع في حقه الانتهاك، ورغم أن نص المادة ٧ المُتعلقة بالتزامات المُتحكم والمُعالج قد نظمت عملية الإبلاغ عن أي خرق أو انتهاك للبيانات الشخصية التي يحوزانها، فإن النص اقتصر على أن يتم إبلاغ مركز حماية البيانات فقط، وليس صاحب البيانات، خلال اثنتين وسبعين ساعة، وفي حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فوريًا إلى مركز حماية البيانات، وعلى المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فورًا، دون ذكر لأي إطار زمني يتعلق بإبلاغ الأشخاص أصحاب البيانات التي يتم اختراقها.

## الحق في معرفة الهدف من جمع البيانات وأسباب المُعالجة :

اكتفى نص المادة ٢ من قانون حماية البيانات الشخصية بتنظيم حق المُستخدم في العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج البيانات والاطلاع عليها والوصول إليها أو الحصول عليها

، إلا أن النص أغفل حق المُستخدمين في الاستفسار عن الهدف من جمع البيانات، وجعل القانون هذا الحق مُجرد شرط من ضمن الشروط التي يجب توافرها أثناء عملية جمع البيانات في المرة الأولى، حيث أشارت المادة ٣ من قانون حماية البيانات إلى أن من ضمن شروط جمع البيانات، أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني، هذه الصياغة لها أثر هام، أن شروط جمع المعلومات جاءت بصياغة غير واضحة مُكتفية باستخدام عبارة: "أن يكون الهدف لسبب مشروع ومُعلن للشخص المعني"، وهو ما يعني أن عملية إخطار المُستخدم بالهدف من جمع البيانات سوف تكون في صورة إخطار واحد عند الموافقة الأولى على جمع البيانات، وهنا يظهر الفارق بين النص على الهدف من جمع البيانات بين كونه شرطًا على المُتحكم أو حقًا للمُستخدم، حيث أن تنظيم الهدف من جمع البيانات ومعالجتها كحق للمُستخدم يعني القدرة على الاستفسار الدائم والمُستمر في أي مرحلة سواء كانت مرحلة جمع البيانات أو مُعالجتها، ولا يُمكن الاكتفاء في هذه الحالة بالموافقة الأولى، أو اعتبار الموافقة الأولى سارية على كافة البيانات التي يتم جمعها بعد الحصول عليها. فالهدف من المعرفة الدائمة والمُستمرة هو ضمانة أساسية يُمكن من خلالها مُمارسة الحق في الاعتراض أو العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

## ارتفاع الرسوم:

يضع القانون سقفًا للحد الأقصى لمقابل تكلفة الخدمة المقدمة إلى المُستخدم من المتحكم أو المعالج فيما يخص ممارسته لحقوقه، والتي من المُمكن أن تصل إلى عشرين ألف جنيه مصري، وتجب الإشارة هنا إلى أن هذا الرسم يُثير مخاوف حول ارتفاع تكلفة الحصول على خدمات تتعلق بحق المُستخدمين بالأساس، وهو ما قد يُصعِّب على المُستخدم مُمارسة حقوقه القانونية والدستورية المُتعلقة بالحفاظ على بياناته، إلا أن هذا الأمر يُمكن تداركه من خلال إصدار قرارات تحديد أسعار الخدمات التي سوف يُصدرها مركز حماية البيانات، حيث أن القانون لم يضع حدًا أدنى لتقديم هذه الخدمات، لذا يجب على مركز حماية البيانات عند وضع القواعد الخاصة بتسعير الخدمات، أن يُراعي فرض رسوم تتناسب مع التكاليف الإدارية لتوفير البيانات أو المعلومات، مع مُراعاة طبيعة البيانات المطلوبة والجُهد اللازم لاستخراجها ومدى تكرار طلب هذه البيانات.

## إجراءات إتاحة البيانات الشخصية

من الأهداف الرئيسية لقانون حماية البيانات، إتاحة وصول المُستخدم إلى البيانات التي يمتلكها كلّ من المُتحكم أو المُعالج أو الحائز، وهي خطوة أساسية لتفعيل حقوق المُستخدم المُختلفة، سواء برغبة المُستخدم في محو البيانات وتصحيحها أو تعديلها، لذا يجب أن تتسم الضمانات المُتعلقة بإتاحة البيانات، ومن ثم الإجراءات المُرتبطة بذلك، بالوضوح وعدم اللبس والنص صراحة على القواعد والإجراءات الضامنة لذلك.

### مادة (١٠) :

يلتزم كل من المتحكم والمعالج والحائز عند طلب إتاحة البيانات الشخصية بالإجراءات الآتية:

١ - أن يكون بناءً علي طلب كتابي يقدم إليه من ذي صفة أو وفقًا لسند قانوني.

٢ - التحقق من توافر المستندات اللازمة لتنفيذ الإتاحة والاحتفاظ بها.

٣ - البت في الطلب ومستنداته خلال ستة أيام عمل من تاريخ تقديمه إليه، وعند صدور قرار بالرفض يجب أن يكون الرفض مسببًا، ويعتبر مضي المدة المشار إليها دون رد في حكم الرفض.

### ملاءمة الإتاحة :

لم يُحدد نص المادة ١٠ طريقة الرد على طلب الحصول على البيانات، حيث اكتفى النص بتحديد المواعيد التي يجب الرد خلالها فقط، ويحتاج النص إلى أن يكون أكثر وضوحًا، حول الطريقة التي تتم بها إتاحة البيانات المطلوبة، حيث يجب أن تتاح البيانات بلغة واضحة ومفهومة، وأن تُقدّم بالطريقة الأنسب التي يُحددها المُستخدم سواء كان ذلك كتابة أو بإحدى الوسائل الإلكترونية، وأن تتاح بصيغ تقنية شائعة وغير مُعقدة.

### الضوابط المُتعلقة بالبيانات المُتاحة :

لم يذكر نص المادة ١٠ الضوابط المُتعلقة بالرد على طلب إتاحة البيانات، فيجب على المُتحكم أو المُعالج أن يوضح في الرد على طلب الإتاحة حالة البيانات المطلوب إتاحتها، وما إذا تمت مُعالجتها، وما إذا تمت مُشاركة البيانات مع أطراف أخرى، وفترة تخزين البيانات، والأوجه التي تم من خلالها استخدام البيانات.

### غياب إجراءات تصحيح أو تعديل أو محو البيانات :

نظمت المادة ١٠ بعض الإجراءات المُتعلقة بإتاحة البيانات، إلا أن القانون قد أغفل الإجراءات المُنظمة لطلبات تصحيح أو تعديل أو محو البيانات الشخصية، مُكتفيًا بوضع التزام على المُتحكم أو المُعالج بنص المادة ١٢ التي تُلزم المُتحكم أو المُعالج بتصحيح أي خطإ بالبيانات الشخصية فور إبلاغه أو علمه به، ولكن لم يُنظم القانون الإجراءات المُتعلقة بـتقديم طلبات التصحيح أو المحو، والآلية التي تتم من خلالها.

## التزامات المُتحكم والمُعالج والحائز

يكفُل القانون عددًا من الضمانات التي تتعلق بحماية البيانات الشخصية للمُستخدمين، وتنعكس هذه الضمانات في صورة التزامات تقع على كل مُعالج أو مُتحكم أو حائز للبيانات، وقد فرّق القانون بين الالتزامات التي تقع على المُتحكم والمُعالج، بينما أغفل الالتزامات المُتعلقة بالحائز. فتنظم المادة ٤ من القانون الالتزامات التي تقع على المُتحكم، وتتنوع الالتزامات الواردة بالقانون ما بين التزامات تتعلق بحقوق المُستخدمين، مثل ضرورة موافقة الشخص المعني بالبيانات، للحصول علي البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها، وكذلك التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها، ومحو البيانات الشخصية لدى المُتحكم فور انقضاء الغرض المحدد منها، والتزام المُتحكم بتصحيح أي خطإٍ بالبيانات الشخصية فور إبلاغه أو علمه به.

كما أشار نص المادة ٤ إلى بعض الضوابط والشروط التي يجب أن يلتزم بها المُتحكم عند مُمارسة نشاطه، من بينها ضرورة الحصول علي ترخيص أو تصريح من مركز حماية البيانات للتعامل مع البيانات الشخصية، كذلك وضع طريقة وأسلوب ومعايير المعالجة طبقًا للغرض المحدد، التأكد من اتساق الغرض المحدد من جمع البيانات الشخصية مع أغراض معالجتها، وكذلك اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظًا علي سِرّيتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها من قِبَل أي إجراء غير مشروع، وكذلك إمساك سجل خاص للبيانات، يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم، وسنده والمُدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود، ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات، وتوفير الإمكانيات اللازمة لإثبات هذه الالتزامات، وتمكين المركز من التفتيش والرقابة للتأكد من ذلك.

وفيما يتعلق بالمُتحكم في البيانات خارج جمهورية مصر العربية، فقد وضع القانون نصًا إلزاميًا، بتعيين ممثل له في جمهورية مصر العربية، وقد أحال نص المادة ٤ السياسات والإجراءات والضوابط والمعايير الفنية التي يجب أن يلتزم بها المُتحكم إلى اللائحة التنفيذية للقانون والتي لم تصدر حتى الآن.

## غياب التزامات الحائز للبيانات :

لم يُعرِّف قانون حماية البيانات الحائز للبيانات تعريفًا واضحًا، كما لم يستطع القانون التمييز بين وظيفة الحائز ووظيفة المُتحكم أو المُعالج، حيث عُرِّف الحائز بأنه أي شخص طبيعي أو اعتباري يحوز ويحتفظ قانونيًا أو فعليًا ببيانات شخصية في أي صورة من الصور، كما وضع القانون إطارًا يُنظم من خلاله عملية إجراءات إتاحة البيانات من خلال الحائز والتي تم النص عليها بالمادة ١٠ من قانون حماية البيانات، ورغم ذلك جاء الفصل الثالث من قانون حماية البيانات الشخصية ليُنظم الالتزامات التي تقع على كلٍّ من المُتحكم والمُعالج فقط، دون ذكر لالتزامات حائز البيانات.

## الالتزامات الأساسية عند عملية جمع البيانات :

لم يُفرد قانون حماية البيانات فصلًا مستقلًا يُنظم من خلاله الضوابط المُتعلقة بالمعلومات الأساسية التي يجب أن يُحاط بها المُستخدم عند جمع المعلومات، مُكتفيًا بوضع القواعد الأساسية التي يلتزم بها المُتحكم والمُعالج، المُتعلقة بإمساك سجل خاص للبيانات، على أن يتضمن هذا السجل وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها، وهو ما يعني أن الالتزامات التي تقع على كلٍّ من المُتحكم والمُعالج، تتم كأحد الإجراءات الإدارية الداخلية، أو لأهداف المُتابعة والتفتيش من مركز حماية البيانات، ولم يضع القانون أي التزامات إجرائية واضحة تتعلق بتفعيل حقوق المُستخدم (الشخص المعني بالبيانات)، عندما يتم جمع البيانات الشخصية، لذلك كان يجب أن يكون ضمن الالتزامات التي تقع على كلٍّ من المُتحكم والمُعالج، عند الحصول على/ جمع البيانات الشخصية، تزويد المُستخدم كتابة بالمعلومات التالية:

- بيانات الاتصال بمسؤول حماية البيانات لدى المُتحكم والمُعالج.
- أغراض المعالجة التي من المُمكن أن تتم على البيانات الشخصية.
- الأساس القانوني للمعالجة.
- الفترة التي سيتم خلالها تخزين البيانات الشخصية.
- الإجراءات اللازمة للحصول على نسخة من البيانات.
- الإجراءات المُتعلقة بتصحيح أو تعديل أو محو البيانات الشخصية أو تقييد المُعالجة المتعلقة بموضوع البيانات أو الاعتراض على المعالجة.
- إجراءات سحب الموافقة المُسبقة على عملية جمع البيانات.
- إجراءات الطعن على أيٍّ من قرارات تعديل أو محو أو تصحيح أو نقل البيانات والجهة التي تتم أمامها الإجراءات.
- مدى احتمالية أن تتم المُعالجة عبر أطراف أخرى غير خاضعة للقوانين المصرية.

## مُشاركة البيانات عبر الحدود

لم تَعُد عملية نقل ومشاركة البيانات أمرًا يقتصر على الجهات الحكومية أو الشركات الوطنية، وخاصة أن التعاملات التي تتم عبر الحدود التقليدية أصبحت أمرًا يوميًا، هذا بالإضافة إلى التطورات المُتعلقة بتوقيع اتفاقات أطرافها الدول تسمح بُمشاركة البيانات لأغراض مُتعددة، وهو ما يعني أن هناك مخاطر تتعلق باحتمالية حدوث انتهاكات تتعلق بالبيانات الشخصية، لم يضع قانون حماية البيانات الشخصية المصري معايير واضحة تمثل الحد الأدنى الذي يجب توافره خلال عملية مُشاركة البيانات عبر الحدود سواء تم ذلك مع أطراف حكومية أو شركات أو مُنظمات خارج مصر، لم يضع قانون حماية البيانات سوى شرطين يجب توافرهم عند مُشاركة أو إتاحة البيانات عبر الحدود، الأول: توفر مستوى حماية لا تقل عن مستوى الحماية المنصوص عليها بالقانون المصري، والثاني: أن يكون هناك ترخيص من مركز حماية البيانات لمُشاركة البيانات مع أطراف أجنبية.

### مادة (١٤):

يحظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوًى من الحماية لا يقل عن المستوى المنصوص عليه في هذا القانون، وبترخيص أو تصريح من المركز. وتحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها.

### مادة (١٥):

استثناءً من حكم المادة (١٤) من هذا القانون، يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلي دولة لا يتوفر فيها مستوى الحماية المشار إليها في المادة السابقة، وذلك في الحالات الآتية:

١- المحافظة على حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له.
٢- تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة أو الدفاع عنه.
٣- إبرام عقد، أو تنفيذ عقد مبرم بالفعل، أو سيتم إبرامه بين المسؤول عن المعالجة والغير، وذلك لمصلحة الشخص المعني بالبيانات.
٤- تنفيذ إجراء خاص بتعاون قضائي دولي.
٥- وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة. ٦ - إجراء تحويلات نقدية إلى دولة أخرى وفقًا لتشريعاتها المحددة والسارية.
٧- إذا كان النقل أو التداول يتم تنفيذًا لاتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفًا فيه.

## عدم كفاية القواعد المنصوص عليها بالقانون المصري لحماية البيانات عبر الحدود :

تناول قانون حماية البيانات القواعد المُتعلقة بمُشاركة البيانات بشكل مختصر، لم يذكر القانون أهم القواعد المُتعلقة بتحديد نطاق المسؤولية بين الأطراف المُختلفة، كما أن الشروط التي يتطلب قانون حماية البيانات الشخصية توفرها تقتصر فقط على توفر القواعد التشريعية المنصوص عليها في الدولة الأجنبية، بينما هناك معايير أخرى يجب الالتفات إليها، مثل: مدى احترام الدولة الأجنبية لقواعد حقوق الإنسان والحريات الأساسية، ووجود هيئة أو مفوضية مُستقلة تعمل على إنفاذ القانون بشكل صحيح، والضوابط المُتعلقة بالمُمارسات الفعلية وليست التشريعية فقط.

## الاستثناءات الواردة على عدم مُشاركة البيانات :

يُنظم القانون في المادة ١٥ الحالات المُستثناة التي لا تتقيد بالقواعد الواجب اتباعها عند مُشاركة أو إتاحة البيانات عبر الحدود، والاستثناءات تعتمد بالأساس على موافقة ورغبة المُستخدمين في مُشاركة بياناتهم مع أطراف لا تلتزم بالضرورة بالقواعد الخاصة بحماية البيانات الشخصية، لكن النص لم يضع التزامًا على مركز حماية البيانات يتعلق بضرورة إبلاغ المُستخدم بالمخاطر المُحتملة في حالة مُشاركة البيانات دون التقيد بالقواعد المنصوص عليها في قانون حماية البيانات المصري.

## غياب السياسات والمعايير والضوابط اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود :

أحال قانون حماية البيانات، القواعد المُتعلقة بالسياسات والمعايير اللازمة لإتاحة ومُشاركة البيانات عبر الحدود إلى اللائحة التنفيذية، وهو خطأ تشريعي يجب مُعالجته، فعملية حماية البيانات هي الهدف الرئيسي من إقرار القانون، وبالتالي لا يجب إحالة القواعد المُنظمة لها إلى السلطة التنفيذية، أو أن تخضع لمعايير مُتغيرة لا يُمكن للمُستخدم مُتابعة تطوراتها.

## دور مركز حماية البيانات في إحالة الشكاوى والمساعدة في التحقيق والاختصاص القضائي :

عملية مُشاركة وإتاحة البيانات عبر الحدود قد يترتب عليها انتهاكات تتعلق بإفشاء البيانات، وهو ما يستدعي اتخاذ الإجراءات القانونية المُتعلقة بتقديم الشكوى واللجوء إلى القضاء إذا لزم الأمر، وهو ما يستدعي توضيح الاختصاص القضائي عند حدوث نزاع، كما أن هذا الأمر يُثير إشكالية تطبيق الأحكام القضائية المصرية خارج الحدود المصرية لاختلاف الأنظمة القضائية من دولة إلى أخرى، وهو ما سكتت عنه نصوص القانون، ولم يوضح القانون دور مركز حماية البيانات في مُتابعة عملية تنفيذ الأحكام القضائية ذات الصلة.

### التحقيق :

كذلك لم يذكر القانون دور مركز حماية البيانات في عملية التحقيق في الشكاوى المُقدمة ضد أطراف خارج مصر تكون قد تمت مُشاركة البيانات الشخصية معها، أو طريقة تقديم المُساعدة للمُستخدمين، كما لم يتحدث القانون صراحة عن دور المركز في الإعلان الدائم عن قوائم الدول أو الشركات أو المُنظمات التي تلتزم بقواعد حماية البيانات الشخصية، وهو الأمر الذي يتطلب أن يكون من بين وظائف المركز مراقبة التطورات في البلدان والمنظمات الدولية.

## تشكيل واختصاصات مركز حماية البيانات

نظمت نصوص قانون حماية البيانات الشخصية تشكيل ودور الهيئة المنوط بها حماية البيانات الشخصية، وقد سُمي بمركز حماية البيانات الشخصية، وقد عُهد إلى هذا المركز القيام بكافة المهام المُتعلقة بمتابعة إنفاذ قانون حماية البيانات الشخصية، وقد نظمت نصوص القانون تشكيل واختصاصات مركز حماية البيانات الشخصية من خلال المادة ١٩ من قانون حماية البيانات، حيث يهدف المركز إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، وأفرد القانون للمركز عددًا من الاختصاصات لمُباشرة نشاطه، من بينها توحيد سياسات وخطط حماية ومعالجة البيانات الشخصية داخل الجمهورية، إصدار التراخيص أو التصاريح والموافقات والتدابير المختلفة المتعلقة بحماية البيانات الشخصية وتطبيق أحكام هذا القانون، اعتماد الجهات والأفراد، ومنحهم التصاريح اللازمة التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات الشخصية، التنسيق والتعاون مع جميع الجهات والأجهزة الحكومية وغير الحكومية في ضمان إجراءات حماية البيانات الشخصية، والتواصل مع جميع المبادرات ذات الصلة، ودعم تطوير كفاءة الكوادر البشرية العاملة في جميع الجهات الحكومية وغير الحكومية القائمة على حماية البيانات الشخصية.

كما يختص مركز حماية البيانات تلقي الشكاوى والبلاغات المُتعلقة بحماية البيانات، الرقابة والتفتيش على المخاطبين بأحكام هذا القانون واتخاذ الإجراءات القانونية اللازمة، والتحقق من شروط حركة البيانات عبر الحدود، وتقديم جميع أنواع الخبرة والاستشارات المتعلقة بحماية البيانات الشخصية، وعلى الأخص لجهات التحقيق والجهات القضائية، إبرام الاتفاقيات ومذكرات التفاهم والتنسيق والتعاون وتبادل الخبرات مع الجهات الدولية ذات الصلة بعمل المركز وفقًا للقواعد والإجراءات المقررة في هذا الشأن، إعداد وإصدار تقرير سنوي عن حالة حماية البيانات الشخصية في جمهورية مصر العربية.

## تشكيل مركز حماية البيانات واستقلاله :

اعتمد القانون على آلية اختيار أعضاء مجلس إدارة مركز حماية البيانات عن طريق الترشيح المُباشر من بعض الجهات الإدارية، دون ذكر للمعايير أو الخبرات المُتعلقة بالأعضاء، ويغلب على تشكيل مجلس إدارة المركز الطابع الإداري دون تمثيل لأصحاب المصالح أو لمُنظمات المجتمع المدني العاملة في مجال حماية البيانات، حيث تشكل الجهات الأمنية ما يقرب من نصف أعضاء المجلس تقريبًا، أربعة مُمثلين من أصل تسعة أعضاء مجلس إدارة المركز، وهو أمر لا يُمكن فهمه في ظل استثناء جهات الأمن القومي من الخضوع لأحكام قانون حماية البيانات الشخصية، كما أن نصوص القانون لم تتحدث صراحة عن المعايير الخاصة بضرورة عدم وجود تضارب للمصالح بين الوظائف الإدارية التي يتولاها أعضاء المجلس والمهام المُتعلقة بإدارة مركز حماية البيانات، كافة هذه المُلاحظات تجعل من مركز حماية البيانات هيئة غير مُستقلة، يصعب ضمان عدم حدوث تدخلات مُباشرة في إدارته لعملية هامة مثل حماية بيانات المُستخدمين .

## مادة (٢٠) :

يكون للمركز مجلس إدارة، يشكل برئاسة الوزير المختص، وعضوية كل من:

١- ممثل عن وزارة الدفاع يختاره وزير الدفاع.

٢- ممثل عن وزارة الداخلية يختاره وزير الداخلية.

٣- ممثل عن جهاز المخابرات العامة يختاره رئيس الجهاز.

٤- ممثل عن هيئة الرقابة الإدارية يختاره رئيس الهيئة.

٥- ممثل عن هيئة تنمية صناعة تكنولوجيا المعلومات يختاره رئيس مجلس إدارة الهيئة.

٦- ممثل عن الجهاز القومي لتنظيم الاتصالات يختاره رئيس مجلس إدارة الجهاز.

٧- الرئيس التنفيذي للمركز.

٨- ثلاثة من ذوي الخبرة يختارهم الوزير المختص. وتكون مدة عضوية مجلس الإدارة ثلاث سنوات قابلة للتجديد، ويصدر بتشكيله، وتحديد المعاملة المالية لأعضائه قرار من رئيس مجلس الوزراء.

ولمجلس الإدارة أن يشكل من بين أعضائه لجنة أو أكثر يعهد إليها بصفة مؤقتة ببعض المهام، وللمجلس أن يفوض رئيس مجلس الإدارة أو الرئيس التنفيذي للمركز في بعض اختصاصاته.

## خاتمة وتوصيات

إن إقرار قانون حماية البيانات الشخصية خطوة هامة لتوفير الحماية اللازمة لخصوصية المُستخدمين، وتتعاظم هذه الأهمية في ظل وجود بيئة تشريعية فقيرة تغيب عنها الضمانات المُتعلقة بخصوصية الأفراد بشكل عام، هذا بجانب غياب القواعد التنظيمية المُتعلقة بالقواعد والإجراءات اللازمة لحماية البيانات الشخصية، وعدم وضوح سُبل الإنصاف في حالة الاعتداء على الحياة الخاصة، وبناء على القراءة المتقدمة لنصوص القانون توصي "مسار" بالآتي:

- يجب على السلطات المصرية إجراء مُراجعة تشريعية واسعة لكافة القوانين الأخرى التي تنظم المُعاملات اليومية التي تتطلب مُشاركة بيانات الأفراد مع الغير، وذلك لجعل أحكام قانون حماية البيانات فعالة، حيث يعتبر هذا القانون هو القاعدة العامة المعنية بتنظيم وحماية كل ما يتعلق بتداول البيانات الشخصية.

- يجب على السلطات إعادة النظر في القواعد الإجرائية المنصوص عليها بقانون حماية البيانات الشخصية، على أن يتم تعديل القانون بإضافة كافة الضوابط المُتعلقة بحماية البيانات أو مُشاركتها مع أطراف أخرى، دون الإحالة إلى اللوائح والقرارات التنفيذية، حيث أحال قانون حماية البيانات الشخصية، تفصيلات إجرائية جوهرية إلى اللائحة التنفيذية، وهو ما يتعارض مع الطبيعة الخاصة لقانون حماية البيانات، فهو بطبيعته قانون ذو طابع إجرائي، ما يعني ضرورة أن تكون القواعد الإجرائية شاملة وكافية لتطبيقها بذاتها، وأن يتم النص عليها في القانون لضمان استقرارها، دون الإحالة إلى لوائح وقرارات تنفيذية تصدرها الجهات التنفيذية، وتستطيع تغييرها دون الرجوع إلى السلطة التشريعية.

- يجب على السلطات مُراعاة القواعد المُتعلقة بفرض رسوم لحصول الأفراد على بياناتهم الشخصية نظرًا إلى ارتفاع الحد الأقصى المنصوص عليه في القانون بشكل مبالغ فيه (عشرون ألف جنيه مصري). لذلك يجب أن تُراعي قرارات مركز حماية البيانات التكلفة الفعلية لاستخراج البيانات.

- يجب أن يتبع إصدار قانون حماية البيانات الشخصية تشكيل هيئات مُستقلة قادرة على مُتابعة الالتزامات القانونية للمُخاطَبين بالقانون ورفع وعي المُستخدمين والجهات، وفي هذا الشأن يجب تعديل النصوص الخاصة بتشكيل مجلس إدارة مركز حماية البيانات، بما يضمن تمثيل الأطراف المُختلفة من أصحاب المصالح والمُستخدمين.

- يجب تعديل القانون بإضافة نصوص إجرائية واضحة تُنظم الإجراءات المُتعلقة بمحو وتصحيح وتعديل البيانات الشخصية لدى الحائز أو المُتحكم أو المُعالج.

- تجب إعادة صياغة النصوص المُتعلقة بدور ومسؤوليات مركز حماية البيانات في حالة مُشاركة البيانات مع أطراف خارج الحدود المصرية، ومن أهم هذه الالتزامات، توضيح المخاطر المترتبة على مُشاركة البيانات مع أطراف خارج الحدود المصرية والتي لا تلتزم بالحد الأدنى من المعايير والإجراءات اللازمة لمُشاركة البيانات، كذلك توضيح دور مركز حماية البيانات في عملية تلقي ومُتابعة الشكاوى التي تتم في حالة تعرض البيانات الشخصية لأي انتهاك أثناء مُشاركتها مع أطراف خارج الحدود المصرية، مع ضرورة النص صراحة على السياسات والمعايير والضوابط اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود، حيث أن القانون قد أحال هذا الأمر إلى اللائحة التنفيذية، وهو أمر لا يستقيم مع أهمية هذه الإجراءات.

- يجب تعديل النصوص التي تتعلق بحقوق المُستخدم، لتشمل إلزام المُتحكم أو المُعالج بتقديم البيانات الشخصية التي يطلبها المُستخدم بطريقة مُلائمة يكون للمُستخدم الحق في تحديدها أو اختيارها من بين طرق وصيغ مُتعددة تتفق وحاجة المُستخدم، مع النص على آلية إبلاغ المُستخدم عن حدوث انتهاك للبيانات الشخصية الخاصة به والمدى الزمني الذي يجب أن يتم خلاله إخطار من وقع في حقه الانتهاك.

- يجب تعديل القانون بإضافة نصوص تُلزم الحائز أو المُتحكم، عند جمع البيانات بشكل مُباشر من المُستخدمين، أن يُسلم المُستخدمين قائمة تتضمن الحقوق الأساسية المُتعلقة بالبيانات التي تم جمعها أو مُعالجتها، على أن تتضمن هذه القائمة، أغراض المُعالجة، وسُبل الاتصال بالحائز أو المُتحكم أو المُعالج لمحو أو تعديل البيانات الشخصية.


https://masaar.net