مشكلات البنية التشريعية

لحماية البيانات الشخصية في مصر

مشكلات البنية التشريعية

لحماية البيانات الشخصية في مصر

إعداد:

الوحدة البحثية بالمركز الإقليمي للحقوق والحريات

تصميم الغلاف والتنسيق الداخلي:

الوحدة الإعلامية بالمركز الإقليمي للحقوق والحريات

الناشر:

المركز الإقليمي للحقوق و الحريات

www.rc-rl.org

the regional center for Rights & liberties

المركز الإقليمي للحقوق و الحريات

المحتويات

أولا: الملخص التنفيذي

في عام ٢٠٠٣، أُصدر أول قانون لتنظيم الاتصالات في مصر برقم ١٠ لسنة ٢٠٠٣. جاءت تلك الخطوة بعد ٥ سنوات من اقتحام الهواتف المحمولة سوق الاتصالات في مصر، ورغم أن القانون تم تشريعه لعدة أغراض منها تنظيم العلاقة بين مقدمي الخدمة (شركات الاتصالات العامة والخاصة) وبين المستخدم، لكنه أغفل الكثير من حقوق المستخدم، مما تسبب في وجود فراغ تشريعي حول هذه النقطة.

ومع تزايد رقعة مستخدمي الهواتف المحمولة والتطور التكنولوجي، بدأت مصر مؤخرا الاتجاه نحو الرقمنة، وهو ما تطلب استحداث بنية تشريعية متكاملة الأركان، فأصدر المشرعون قانون مُكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

تعددت أهداف القانون، وجاء من بينها حماية حرمة الحياة الخاصة، والبيانات والمعلومات الشخصية وكذلك الحكومية وتجريم انتهاكها استنادا إلى مواد الدستور المصري. لكن مواد القانون تضمنت بعض العبارات والكلمات الفضفاضة واسعة التفسير التي قد تسمح بتدخل الأهواء الشخصية، وهو ما يعد عوار تشريعي بالقانون.

وخلال العامين الماضيين، توجهت مصر نحو صناعة مراكز البيانات[1]، إحدى الصناعات التي تساهم في نمو الاقتصاد من خلال اجتذاب الاستثمارات العالمية في هذا المجال. ولذلك كان على الدولة أن تعمل على سد الفراغ التشريعي الخاص بحماية البيانات الشخصية من خلال إصدار قانون البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

تعددت أهداف قانون حماية البيانات الشخصية، وكان من أبرزها ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً. لكن القانون حتى الآن ما زال معطلا رغم مرور عام كامل من التصديق عليه ونشره في الجريدة الرسمية، نظرا لاعتماد أغلب نصوص القانون على اللائحة التنفيذية التي كان من المفترض أن تصدر خلال ستة أشهر وفقا لمواد القانون، حيث أحال القانون عددًا كبيرًا من الجوانب والضوابط والآليات الإجرائية إلى اللائحة التنفيذية، لكنها-وبالرغم من ذلك-لم تصدر حتى وقت إصدار هذه الورقة، وبالتالي لا يمكن سريان القانون وتطبيقه دون إقرارها.

تأتي هذه الورقة لتسلط الضوء على الأزمات والمشكلات التشريعية التي تواجه حماية البيانات الشخصية في مصر، وبالأخص في مرحلة جمع ومعالجة البيانات، ومدى خطورة تلك المشكلات على البيانات الشخصية، وكيفية حلها، للسير قدما نحو قوانين تحترم وتحمي حرمة الحياة الخاصة وكذلك البيانات الشخصية للمواطنين.

---

١ وزير الاتصالات: قانون حماية البيانات الشخصية يدعم صناعة مراكز المعلومات في مصر

ثانيا: مقدمة (الرقمنة والاستثمارات الرقمية في مصر)

في يوليو من عام ٢٠١٩، أعلن الرئيس المصري عبد الفتاح السيسي خلال جلسة «إطلاق مبادرة التحول الرقمي» ضمن فعاليات المؤتمر الوطني الدورى السابع للشباب بالعاصمة الإدارية الجديد- عما اسماه بـ «عقل جديد للدولة المصرية»، وهو منظومة من الخوادم والحواسيب مدفونة على عمق ١٤ مترا تحت سطح الأرض ومؤمنة بشكل كبير، هذا بالإضافة إلى عقل آخر تبادلي تعمل عليه الدولة منذ عامين وتكلف ٢٥ مليار جنيه، وذلك للتعامل مع قواعد بيانات المواطنين المصريين[2].

يهدف التحول الرقمي في مصر، والذي يعتبر جزءا من رؤية مصر ٢٠٣٠، إلى تحسين جودة حياة المواطن المصري عن طريق تعزيز الخدمات الرقمية في المصالح الحكومية، حتى يتمكن المواطن من إتمام المعاملات الحكومية بشكل أبسط وأسرع. وكذلك تحويل الحكومة إلى حكومة مترابطة رقميا وتحسين العمل داخل الجهاز الإداري للدولة. بالإضافة إلى تعزيز قيم الشفافية والمحاسبة والمراقبة وتمكين الدولة من الحوكمة الإلكترونية، وتوفير الدعم لعملية صناعة القرار، وإيجاد حلول للقضايا التي تهم المجتمع. كما أن هناك هدف آخر لاستراتيجية التحول الرقمي وهو جذب الاستثمارات الرقمية في قطاع البنية التحتية للاتصالات إلى مصر[3].

وتتعاون وزارة الاتصالات مع قطاعات ومؤسسات الدولة لتوفير الخدمات الحكومية للمواطنين رقميًا، وذلك حتى يتمكن المواطن من تلقي هذه الخدمات إلكترونيًا، وكذلك دفع رسوم الخدمة إلكترونيا عبر الإنترنت. فمن بين الهيئات التي طورت وأطلقت الخدمات المذكورة، هيئة إنفاذ القانون والتوثيق والأحوال الشخصية ومحاكم الأسرة والتموين والكهرباء والزراعة والمرور والشهر العقاري وصندوق الإسكان الاجتماعي ودعم التمويل العقاري والهيئة العامة للاستثمار والمناطق الحرة[4].

تطلب تنفيذ خطة التحول الرقمي العمل على محورين هامين، أولهما: البنية التحتية الرقمية، التي تضمنت خمسة منافذ، هي منصة مصر الرقمية وتطبيقات الهاتف المحمول ومراكز الاتصال (١٥٩٩٩) ومكاتب البريد ومراكز خدمة المواطنين. هذا بالإضافة إلى المشروعات التي تهدف إلى تحسين جودة وسرعة الإنترنت وخدمات الاتصالات، وكذا شبكات كابلات الألياف البصرية التي ستعمل على ربط المباني الحكومية ببعضها لتحسين الخدمات المقدمة.

أما المحور الثاني، فهو البنية التشريعية الرقمية أو الإطار التشريعي، الذي يتشكل من مجموعة من القوانين التي تحكم عملية الرقمنة في مصر. فهناك مجموعة من القوانين التي تم سنها بالفعل في وقت سابق مثل قانون تنظيم الاتصالات وقوانين الملكية الفكرية وحماية المستهلك وقانون التوقيع الإلكتروني، إلى جانب القوانين التي تم إقرارها مؤخرا مثل قانون مكافحة جرائم تقنية المعلومات ولائحته التنفيذية وقانون حماية البيانات الشخصية.

2 السيسي: «عقل الدولة المصرية» محفوظ تحت الأرض بعمق 14 مترًا

3 وزير الاتصالات يبحث مسؤوع التحول الرقمي مع سفير الدنمارك
وزير الاتصالات يبحث مع السفير الإيفواري التعاون في مجال التحول الرقمي

4 مصر الرقمية

القوانين المذكورة تعرضت لمسألة حماية البيانات الشخصية، الأمر الذي يعد حجر أساس نجاح استراتيجيات الرقمنة، فالتعامل مع قواعد بيانات مواطنين بهذه الضخامة يجب أن يخضع لقوانين صارمة وإلا فسوف تتحول حياة هؤلاء المواطنين إلى مادة خام للاستغلال، وهو ما قد يعرضهم أو يعرض ذويهم للمخاطر. إلا أن تلك القوانين قد شابها عوار تشريعي سوف سنتطرق له في هذه الورقة، ونختص بالتحليل قانون تنظيم الاتصالات وقانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات الشخصية، وذلك فيما يتعلق بمسألة معالجة البيانات.

ثالثا: مشكلات البنية التشريعية لقوانين حماية حرمة الحياة الخاصة والبيانات الشخصية

كفل الدستور المصري الصادر عام ٢٠١٤ للمواطنين حماية حرمة الحياة الخاصة في المادة ٥٧، والتي تطرقت بشكل خاص لحرمة وسائل الاتصال بكافة أشكالها وعدم جواز الاطلاع عليها أو مراقبتها إلا بإذن قضائي مسبب ولفترة محددة وفقا لما ينظمه القانون، كما وضعت المادة ذاتها التزام على الدولة. أما المادة ٩٩ من الدستور فقد جرمت الاعتداء على حرمة الحياة الخاصة للمواطنين، ولا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، ويعوض عنها من وقع عليه الاعتداء تعويضا عادلا[5].

أ- قانون تنظيم الاتصالات

صدر قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣[6] ليمنح الصلاحيات للجهاز القومي لتنظيم الاتصالات كونه الجهاز المختص بمراقبة قطاع الاتصالات في مصر وتحسين خدماتها وتوسيع نطاق استخداماتها.

ووضع القانون عدة تعريفات تقنية تتعلق بالاتصالات والشبكات، هذا بالإضافة إلى تعريف الجهاز القومي لتنظيم الاتصالات والوزير المختص. وحدد القانون تشكيل الجهاز واختصاصاته واختصاصات أعضائه، كما حدد شروط الحصول على تراخيص وتصاريح إنشاء وتشغيل الاتصالات.

كما ألزم مقدمو خدمات الاتصالات والمستثمرون بالامتثال للوائح والمعايير التي وضعها الجهاز حتى يمكنهم الدخول إلى السوق المصرية وإطلاق خدمات جديدة فيه. وأخيرا، سن القانون مجموعة من العقوبات التي تتعلق بالجرائم المتعلقة بالاتصالات والشبكات.

---

5 مادة ٥٧ من دستور مصر ٢٠١٤: "الحياة الخاصة حرمة، وهى مصونة لا تمس، وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها أو الإطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التى يبينها القانون».

مادة ٩٩ من دستور مصر ٢٠١٤: "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. وتكفل الدولة تعويضًا عادلاً لمن وقع عليه الاعتداء، وللمجلس القومى لحقوق الإنسان إبلاغ النيابة العامة عن أى انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضمًا إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون».

6 قانون تنظيم الاتصالات رقم 10 لسنة 2002

العوار التشريعي في قانون تنظيم الاتصالات:

ربط الدستور المصري الصادر عام ٢٠١٤ في مادته ٥٧ بين حماية الحياة الخاصة وبين حرية الاتصال ربطا وثيقا دون استثناء لأي جهة إلا بأمر قضائي مسبب ولمدة محددة. ورغم أن قانون تنظيم الاتصالات المعمول به من قبل وزارة الاتصالات إلى الآن نص على حقوق وواجبات شركات الاتصالات ومقدمي الخدمة، لكن القانون تناسي أن يضمن حقوق المستخدم.

والمقصود بالمستخدم وفقا لقانون الاتصالات[7]؛ هو أي شخص طبيعي أو اعتباري يستعمل خدمات الاتصالات أو يستفيد منها. وبالرغم من تعريف القانون بالمستخدم لكنه أغفل تعريف حقوق المستخدم والتي كان من المفترض أن تدرج في تعريفات القانون؛ وهي مجموعة من الضوابط والقواعد التي تضمن حماية بيانات المستخدمين من خطر الاختراق أو الانتهاك.

على سبيل المثال؛ حق المستخدم في الموافقة الصريحة والواضحة للشركات بالتصرف في بياناته الخاصة، بالإضافة إلى حقه في سحب الموافقة أثناء أي مرحلة من مراحل المعالجة، فضلاً عن حق المستخدم في الحصول على تأكيد من وحدة التحكم، عما إذا كان بياناته الشخصية تتعرض لمرحلة معالجة أم لا، وفي هذه الحالة يحق له الحصول على المعلومات الآتية (أغراض المعالجة، فئات البيانات المعنية، الفئات المستفيدة من المعالجة حيثما أمكن، الفترة الزمنية التي ستخزن فيها البيانات الشخصية وإن لم يكن المعايير المستخدمة لتحديد تلك الفترة).

وكذلك حق المستخدم في الشكوى؛ أن يحق للمستخدم تقديم شكوى لدى السلطة الإشرافية في حالة إذا لم يتم جمع البيانات الشخصية من صاحب البيانات، أو في حال حدوث أي انتهاك أو تسريب تتعرض له بيانات المستخدم. وغيرها من الحقوق التي كان من المفترض أن يحرص المشرع على تضمينها في القانون لضمان حقوق المستخدمين.

أيضا، نص البند الـ١٨ من المادة ٢٥ على وضع نظام لتلقى الشكاوى والتحقيق فيها، دون ذكر آليات تقديم الشكاوى والمدة المحددة للنظر فيها. فيما نص البند الـ١٩ من المادة ٢٥[8] من القانون المشار إليه، على ضمان سرية المكالمات وفقا للقواعد اللازمة، دون أن تنص المادة أو القانون في المواد اللاحقة عن تلك القواعد والضوابط التي يجب اتباعها، ما يعرض مكالمات واتصالات المستخدمين وكذلك بياناتهم لخطر التسريب. وهو ما حدث بالفعل من قبل أحد الإعلاميين في واقعة شهيرة عام ٢٠١٤[9]، إذ قام بإذاعة عدد من مكالمات بعض النشطاء التي تم تسريبها من بعض شركات الهواتف المحمولة متضمنة أسمائهم في حلقات برنامجه.

---

7 مادة ١ من قانون تنظيم الاتصالات: تطبيق أحكام هذا القانون بالمصطلحات التالية المعاني المبينة قرين كل منها.....المستخدم : أي شخص طبيعي أو اعتباري يستعمل خدمات الاتصالات أو يستفيد منها».

.

8 مادة ٢٥ من قانون تنظيم الاتصالات: "يحدد الترخيص الصادر التزامات المرخص له والتي تشمل الأخص ما يأتي.....

18-وضع نظام لتلقى الشكاوى والتحقيق فيها وإصلاح الأعطال بكفاءة .

19-ضمان سرية الاتصالات والمكالمات الخاصة بعملاء المرخص له ووضع القواعد اللازمة للتأكد من ذلك".

9 «القومي لحقوق الإنسان» يطالب بالتحقيق في «تسريب مكالمات النشطاء»

وتضمن الباب السابع العقوبات المتبعة في حالة الإخلال بنصوص القانون، فقد نصت المادة ٧٣[10] بمعاقبة الموظف أثناء تأدية وظيفته في مجال الاتصالات إذا قام بـ»إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات، أو إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه....». ويعرف الموظف أو (مقدم خدمة الاتصالات) وفقا لقانون تنظيم الاتصالات[11]: «أي شخص طبيعي أو اعتباري، مرخص له من الجهاز بتقديم خدمة أو أكثر من خدمات الاتصالات للغير».

لكن في المقابل لم تتضمن هذه المادة أو أي مادة أخرى في باب العقوبات أية عقوبة على شركات الاتصالات التي يقع الانتهاك بداخلها من قبل الموظف. فكان من الأولى أن تُقسّم المسؤولية الجنائية بين الموظف أو مقدم الخدمة وفقا لتعريف القانون، وبين الشركة التي يعمل بها الموظف أو مقدم الخدمة المذكور. وذلك لمنع شركات الاتصالات من الإفلات من المسؤولية والعقوبة، وضمان حماية بيانات المستخدمين وحياتهم الخاصة من خطر التسريب والافشاء.

وبالنظر لمواد القانون نجد أنه يحتاج لبعض التعديلات التشريعية لمواكبة التطور التكنولوجي والطفرة الرقمية التي حدثت في مجال الاتصالات خلال الـ١٨ عام الماضية - لتوفير مستوى أكثر دقة في «حماية البيانات الشخصية للمستخدمين أو العملاء».

ب- قانون مكافحة جرائم تقنية المعلومات ولائحته التنفيذية

جاء قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨[12]، حاملا فلسفة تتعلق بحماية البيانات والمعلومات الشخصية، من استغلالها استغلال يسيء إلى أصحابها، وخاصة في ظل عدم كفاية النصوص العقابية المتعلقة بحماية خصوصيات الأفراد وحرمة حياتهم الخاصة في مواجهة التهديدات والمخاطر المستحدثة لاستخدام تقنية المعلومات.

قانون مكافحة الجريمة الإلكترونية، هو قانون جزائي أو جنائي، أي أنه يحوي قواعد قانونية تبين الجرائم وتحدد العقوبات المقررة لها. واختص هذا القانون بالجرائم التي تُرتكب بواسطة شبكة الإنترنت أو تقنية المعلومات، وحدد لها عقوبات تتراوح بين الحبس والغرامة أو كلاهما.

---

10 مادة ٧٣ من قانون تنظيم الاتصالات: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسي ألف جنيه أو بإحدى هاتين العقوبتين ، كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية :

1- إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانوني في ذلك.

2- إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه.

3- الامتناع عمداً عن إرسال رسالة اتصالات بعد تكليفه بإرسالها.

4- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق.

11مادة 1:
تطبيق أحكام هذا القانون بالمصطلحات التالية المعاني المبينة قرين كل منها : ٧- مقدم خدمة الاتصالات : أي شخص طبيعي أو اعتباري ، مرخص له من الجهاز بتقديم خدمة أو أكثر من خدمات الاتصالات للغير .

12 قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

أما اللائحة التنفيذية للقانون[13]، فقد صدرت بقرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠ واحتوت على بعض التعريفات التقنية، بالإضافة إلى الالتزامات التقنية والتنظيمية والإجراءات الواجب على مقدمي خدمات تقنية المعلومات اتخاذها فيما يتعلق بتشفير وأمان البيانات، إلى جانب الإجراءات التقنية والتنظيمية الخاصة بالبنية التحتية المعلوماتية الحرجة. كما وضعت اللائحة شروطا يجب أن تتوفر في الأدلة الرقمية الجنائية للإثبات الجنائي.

و جاءت المصطلحات الواردة في القانون محددة بتعريفات واضحة لتحقيق التطبيق النافذ للقانون وهي :

- المعالجة الإلكترونية: أي عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا، كتابة، 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 استبدال للبيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى.

- تقنية المعلومات: أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا.

- مقدم الخدمة: أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.

- المستخدم: كل شخص طبيعي أو اعتباري، يستعمل خدمات تقنية المعلومات أو يستفيد منها بأى صورة كانت.

العوار التشريعي في قانون قانون مكافحة جرائم تقنية المعلومات

يتضح مما سبق أن الهدف التشريعي من هذا القانون هو تحديد ومكافحة الجرائم المتعلقة بالحاسبات وتقنية المعلومات، بالإضافة إلى حماية حرمة الحياة الخاصة التي أفرد لها القانون باب كامل جاء في الفصل الثالث بعنوان «الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع، وتحديدا في المادة ٢٥ من القانون[14] التي تطرقت إلى حرمة الحياة الخاصة.

13 اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

١٤ يعاقب بالحبس مدة لاتقل عن ستة أشهر، وبغرامة لاتقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو باحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الاسرية في المجتمع المصرى، أو انتهك حرمة الحياه الخاصة أو ارسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع اليكترونى لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو باحدى وسائل تقنية المعلومات، لمعلومات أو اخبار أو صور وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة ام غير صحيحة.

ووفقا لنص المادة، فقد حدد المشرع ٤ صورا لأشكال جرائم انتهاك حرمة الحياة الخاصة والحق في الخصوصية، وهما:

- كل من اعتدى على أيٍّ من المبادئ أو القيم الأسرية في المجتمع المصري

- أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته

- أو منح بيانات شخصية إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته

- أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة

وخلال المادة المذكورة أفرد المشرع في صور الانتهاكات التي قد تحدث في المستقبل مع التطور التكنولوجي، ولذلك شمل الجزء الأول من المادة صور عامة للاعتداء على حرمة الحياة الخاصة، ومن ثم أفرد في الجزء الثاني صور أخرى لهذا الاعتداء، من بينها نشر بيانات شخصية أو صورًا خاصة أو إرسال رسائل بكثافة دون موافقة، وغيرها من أشكال الاعتداء.

وتضمنت المادة عبارة "الاعتداء على المبادئ والقيم الأسرية"، اعتقادا من المشرع أن النص المُخصص قد يعزز من حماية الحق في الخصوصية، لكن النص حمل مصطلحات واسعة التفسير، حيث لم يحدد المشرع المصري في القانون أو لائحته التنفيذية معنى (المباديء والقيم الأسرية المحمية بموجب القانون)، ما يجعل من هذه المصطلحات نسبية، قد تستخدم وفقا للمعتقدات والأهواء الشخصية.

ورغم أهمية النص القانوني لما يتضمن من صور مختلفة لحماية الحياة الخاصة للمُستخدمين، لكنها أيضا تضمنت عوار تشريعي بسبب الصياغة المتداخلة وغير الواضحة لنص القانون، وإدخال فقرة «المبادئ والقيم الأسرية» على المادة دون دلالة قانونية أو تفسير واضح ومحدد لها. فيما تغافلت المادة الحديث عن آليات جمع الموافقة من المستخدمين من قبل مقدمي الخدمة، لجمع ونشر البيانات عن طريق الشبكة المعلوماتية.

والمقصود بالموافقة، أن يحصل كلا من (المتحكم أو المعالج) على موافقة صريحة من المستخدم قبل جمع بياناته وأيضًا قبل استخدامها في أي مرحلة من مراحل المعالجة، ويشترط أن تكون الموافقة واضحة ويتم إيصال الغرض للمُستخدم بلغة يفهمها دون أي خداع أو كلمات مطاطة تحمل أكثر من معنى ويخلو من المصطلحات التقنية المعقدة، كما لابد من توضيح سبب وجيه لأغراض المعالجة والأساس القانون لها، كما لابد أن يتضمن إقرار الموافقة على تفاصيل التواصل مع موظف حماية البيانات، فضلا عن معرفة الفئات المستفيدة من البيانات الشخصية.

أما عن آليات جمع الموافقة، فلم يحدد القانون ستكون موافقة كتابية يتم جمعها من المستخدم عن طريق الجهة المخزن لديها بياناته الشخصية، أم إلكترونية تتم عن طريق تطبيق مخصص أو استخدام التوقيع الإلكتروني على المستند الذي يُرسل للمستخدم عبر ايميله الشخصي أو أي وسيلة تواصل الكترونية، أو تكون الموافقة شفوية بشكل واضح وصريح.

ج- قانون حماية البيانات الشخصية

صدر قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠[15]، لتنظيم حيازة وجمع ومعالجة البيانات الشخصية سواء بشكل مباشر أو غير مباشر، أيًّ كان نوعها حتى ولو إلكترونية. وتضمن القانون مجموعة من المحاور، نذكر منها: «تعريفات المصطلحات الواردة به، حقوق الشخص المعني بالبيانات، شروط جمع ومعالجة البيانات، التزامات المتحكم والمعالج، وشروط المعالجة والالتزام بالإخطار والإبلاغ، إجراءات إتاحة البيانات الشخصية، أحكام حركة البيانات الشخصية الحساسة، أحكام التسويق الإلكتروني المباشر، اختصاصات مركز حماية البيانات الشخصية، والعقوبات في حالة مخالفة أحكام القانون».

سُن القانون ليتواكب مع اللائحة العامة لحماية البيانات الشخصية (GDPR)، ويضمن حماية الاستثمارات الوطنية وخاصة تلك التي ستتعامل فيها الدولة مع الاتحاد الأوروبي. جاء القانون أيضا لينظم عملية استخدام البيانات الشخصية في عمليات التسويق الإلكتروني، وكذلك عمليات نقل البيانات إلى خارج حدود الدولة.

ويختص الفصل الأول من القانون بالتعريفات التي أسس عليها، وعرفت البيانات الشخصية في القانون بـ «أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى مثل الأسم، أو الصوت، أو الصورة.. إلخ».

أما البيانات الشخصية الحساسة فهي «البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية، أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية... وتعد بيانات الأطفال من البيانات الشخصية الحساسة».

أما المعالجة، والتي نختص الحديث عنها في هذه الورقة، فعرفها القانون بأنها «أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها... أو استرجاعها أو تحليلها باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيًّا أو كليًّا».

العوار التشريعي في قانون حماية البيانات الشخصية في مصر

نهدف في هذه الفقرة الوقوف على مشكلات الصياغة التشريعية لبعض مواد قانون حماية البيانات الشخصية.

15 قانون حماية البيانات الشخصية رقم 151 لسنة 2020

أ- استثناء البنك المركزي من الخضوع لأحكام القانون

بالرغم من أن القانون الهدف منه هو حماية البيانات الشخصية وحماية خصوصية الأفراد التي يكفلها القانون الدولي والدستور المصري، لكن القانون في مادته الثالثة[16] استثنى بعض الجهات من الخضوع لأحكامه. جاءت من ضمن هذه الجهات البنك المركزي، دون تفسير تشريعي لهذا الاستثناء.

وينطبق على البنك المركزي ٣ مفاهيم مما تضمنه القانون فهو يعتبر (حائز ومتحكم ومعالج) للبيانات، وبالتالي استثنائه من أحكام القانون يعني انتهاك صريح للهدف الذي سن القانون لتحقيقه وهو حماية خصوصية الأفراد وبياناتهم الشخصية.

16المادة ٣ من قانون حماية البيانات الشخصية: «لا تسري أحكام القانون المرافق على ما يأتي:

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

2. البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية، أو تطبيقًا لنص قانوني.

3. البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية، بشرط أن تكون صحيحة ودقيقة، وألا تستخدم في أي أغراض أخرى، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام.

4. البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية.

5. البيانات الشخصية لدى جهات الأمن القومي، وما تقدره لاعتبارات أخرى.

يجب على المركز، بناءً على طلب 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

6. 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.

وكان الهدف من إقرار قانون حماية البيانات الشخصية هو أن يكون هناك مظلة واسعة تشمل جميع المؤسسات المصرية لحماية البيانات الشخصية، في محاولة لمواكبة المعيار العالمي الخاص بحماية البيانات الشخصية وهو GDPR (اللائحة العامة لحماية البيانات التي أصدرها البرلمان الأوروبي والمفوضية الأوروبية) والتي لم يستثنى منها سوى السلطات المختصة[17] لأغراض منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو مقاضاة مرتكبيها منع التهديدات التي يتعرض لها الأمن العام.

وبالتالي يصبح استثناء البنك المركزي في قانون حماية البيانات الشخصية في غير محله، فضلا عن أن القانون الهدف منه هو رفع تصنيف مؤشر مصر في مجال حقوق الإنسان، فلم يتم إقرار القانون للحاجة المجتمعية له فقط، وإنما تم إقراره لتشجيع الاستثمار في مجال صناعة مراكز البيانات، وبالتالي استبعاد بعض المؤسسات من مظلة الحماية التشريعية لأول تشريـع مصري مخصص لحماية البيانات الشخصية، يفرغ القانون الجديد من مضمونه.

17 اللائحة العامة لحماية البيانات GDPR

المادة ٢: نطاق تطبيق القانون

1. ينطبق هذا القانون على معالجة البيانات الشخصية كليا أو جزئيا بالوسائل الآلية والتجهيز بخلاف الوسائل الآلية للبيانات الشخصية التي تشكل جزءا من نظام حفظ الملفات أو يقصد منها أن تشكل جزءا من نظام حفظ الملفات.

2.لا ينطبق هذا القانون على معالجة البيانات الشخصية:

(أ) في سياق نشاط يقع خارج نطاق قانون الاتحاد؛

(ب) من قبل الدول الأعضاء عند القيام بأنشطة تقع ضمن الفصل 2 من الباب الخامس من TEU

(ج) من قبل شخص طبيعي في سياق نشاط شخصي أو منزلي بحت،

(د) من جانب السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو مقاضاة مرتكبيها أو تنفيذ العقوبات الجنائية، بما في ذلك صون ومنع التهديدات التي يتعرض لها الأمن العام.

1. لتجهيز البيانات الشخصية من قبل مؤسسات الاتحاد وهيئاته ومكاتبه ووكالاته تطبق اللائحة (EC) رقم

45/2001. ويجب تكييف اللائحة (EC) رقم 45/2001 والأفعال القانونية الأخرى للاتحاد التي تنطبق على معالجة البيانات الشخصية وفقا لمبادئ وقواعد هذه اللائحة وفقا للمادة ٩٨.

2.لا تمس هذه اللائحة تطبيق التوجيه EC/2000/31، ولا سيما قواعد المسئولية الخاصة بمقدمي خدمات الوساطة في المواد ١٢ إلى ١٥ من ذلك التوجيه.

ووفقا لقانون البنك المركزي رقم ١٩٤ لسنة ٢٠٢٠[18] فقد ألزمت المادتين (١٤٠، ١٤٢)[19] في الفصل التاسع بعنوان (سرية الحسابات) البنك المركزي بالحفاظ على سرية بيانات العملاء من إفشائها أو تسريبها أو استخدامها في غير محلها، وبالتالي فإن الاستثناء الذي حصل عليه البنك المركزي في قانون حماية البيانات الشخصية لا داعي له.

والجدير بالذكر أيضا، أن قانون حماية البيانات الشخصية في صياغته الأولى[20] الذي تم مناقشته داخل أروقة البرلمان، لم تحتوي مادته الثالثة على استثناء البنك المركزي من الخضوع لأحكام القانون، وتم إرجاء مناقشة هذه المادة داخل البرلمان حتى تنتهي الحكومة من مناقشتها مع البنك المركزي، وفي عام ٢٠٢٠ أُصدر القانون بإضافة استثناء البنك المركزي من الخضوع لأحكام قانون حماية البيانات الشخصية.

ب - حقوق المستخدمين (آليات الموافقة والإبلاغ وإتاحة البيانات)

عرف القانون المستخدم بأنه (الشخص المعني بالبيانات) وأفرد له المادة الثانية[21] من القانون لوضع ضمانات وإرساء حقوق المستخدمين، لكن المادة جاءت مقتضبة وغير دقيقة في تحديد هذه الحقوق. فقد أكدت المادة على عدم جواز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات (المستخدم)، دون أن توضح المادة عن آلية جمع الموافقة من المستخدمين.

وبالرغم من أن المادة تضمنت ضرورة الحصول على موافقة صريحة من المستخدم قبل جمع بياناته وأيضًا قبل استخدامها في أي مرحلة من مراحل المعالجة، لكنها أغفلت ضرورة أن يشترط لجمع الموافقة أن تكون واضحة ويتم إيصال الغرض للمُستخدم بلغة يفهمها دون أي خداع أو كلمات مطاطة تحمل أكثر من معنى

18 قانون رقم 194 لسنة 2020 بإصدار قانون البنك المركزي والجهاز المصرفي

19 تنص المادة (١٤٠) في هذا الفصل، 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. وتحظر المادة (١٤٢) على كل من يتلقى أو يطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر أو غير مباشر على معلومات أو بيانات عن العملاء أو حساباتهم أو ودائعهم، أو الأمانات أو الخزائن الخاصة بهم أو معاملاتهم إنشاؤها أو تمكين الغير من الاطلاع عليها وذلك في غير الحالات المرخص بها بمقتضى أحكام هذا القانون، ويستمر هذا الحظر بعد تركهم للعمل.

20 تعرف على مواد مسؤوع قانون «حماية البيانات الشخصية» الذي يناقشه مجلس النواب

21 المادة ٢ من قانون حماية البيانات الشخصية: "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:
1 – العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

2 – العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

3 – التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية.

4 – تخصيص المعالجة في نطاق محدد.

5 – العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

6 – الاعتراض على معالجة البيانات الشخصية أو نتائجها متى 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.

وتخلو من المصطلحات التقنية المعقدة، كما لابد من توضيح سبب وجيه لأغراض المعالجة والأساس القانون لها، فضلا عن ضرورة أن يتضمن إقرار الموافقة على تفاصيل التواصل مع موظف حماية البيانات، وكذلك معرفة الفئات المستفيدة من البيانات الشخصية.

كما أغفل القانون الحديث أو الإشارة إلى آليات جمع الموافقة؛ فلم يحدد القانون هل ستكون موافقة كتابية يتم جمعها من المستخدم عن طريق الجهة المخزن لديها بياناته الشخصية، أم إلكترونية تتم عن طريق تطبيق مخصص أو استخدام التوقيع الإلكتروني على المستند الذي يرسل للمستخدم عبر ايميله الشخصي أو أي وسيلة تواصل الكترونية، أو تكون الموافقة شفوية بشكل واضح وصريح.

وكذلك أشارت المادة إلى حق المستخدم في علمه وإبلاغه بأي خرق أو انتهاك حدث لبياناته الشخصية، دون أن تشير المادة إلى آلية إبلاغ المستخدمين. وهو ما يجعل المادة غير مكتملة ويشوبها الغموض. فعلى سبيل المثال؛ أفردت المادتين (٣٣، ٣٤) من اللائحة العامة لحماية البيانات الشخصية GDPR، آليات للابلاغ عن خرق البيانات الشخصية للجهة المختصة وكذلك لصاحب البيانات.

- حيث تضمنت المادة ٣٣ من اللائحة أنه:

١- في حالة خرق البيانات الشخصية يجب على المعالج أو المتحكم دون تأخير لا داعي له وحيثما كان ذلك ممكن في موعد لا يتجاوز ٧٢ ساعة، بعد علمه إخطار خرق البيانات الشخصية إلى الجهة الإشرافية المختصة، ما لم يكن خرق البيانات الشخصية من المرجح أن يؤدي إلى خطر على حقوق وحريات الأشخاص الطبيعيين، وفي حالة عدم إرسال الإخطار إلى السلطة الإشرافية خلال ٧٢ ساعة فأن ذلك يجب أن يكون مصحوبا، بأسباب التأخير.

٢- على المعالج إخطار جهاز التحكم دون تأخير غير مبرر بعد أن يصبح على دراية بخرق البيانات الشخصية.

٣- يكون الإخطار المشار إليه في الفقرة ١ على الأقل :

أ- وصف طبيعة خرق البيانات الشخصية بما في ذلك حيثما أمكن الفئات والعدد التقريبي لأصحاب البيانات المعنية والفئات والعدد التقريبي لسجلات البيانات الشخصية المعنية.

ب- إبلاغ الأسم وتفاصيل الاتصال لموظف حماية البيانات أو أي نقطة اتصال أخرى يمكن الحصول منها على مزيد من المعلومات.

ج- وصف النتائج المحتملة لخرق البيانات الشخصية.

د- وصف التدابير المتخذة أو المقترح أن يتخذها المراقب لمعالجة خرق البيانات الشخصية بما في ذلك عند الاقتضاء تدابير للتخفيف من آثاره الضارة المحتملة.

هـ- حيث أنه لا يمكن توفير المعلومات في نفس الوقت يمكن تقديم المعلومات على مراحل دون المزيد من التأخير غير المبرر

و- يجب على المراقب أن يوثق أي خروقات للبيانات الشخصية بما في ذلك الحقائق المتعلقة بخرق البيانات الشخصية وتأثيراتها والإجراءات التصحيحية المتخذة، ويجب أن تمكن هذه الوثائق السلطة الاشرافية من التحقق من الامتثال لهذه المادة.

أما المادة ٣٤ والخاصة بالتواصل مع الشخص المعني بالبيانات التي تم انتهاكها جاءت في اللائحة كالتالي:

١- عندما يكون خرق البيانات الشخصية من المرجح أن يؤدي إلى مخاطر عالية على حقوق وحريات الأشخاص الطبيعيين، يجب على المراقب أن يشرح خرق البيانات الشخصية لصاحب البيانات دون تأخير غير مبرر.

٢- يجب أن يوضح البلاغ المقدم إلى صاحب البيانات المشار إليه في الفقرة ١ من هذه المادة بصورة واضحة طبيعي خرق البيانات الشخصية ويحتوي على الأقل على المعلومات والتدابير التي تم اتخاذها ومشار إليها في النقاط (ب- ج-د) من المادة ٣٣ الفقرة الثالثة.

٣- لا يلزم ارسال البلاغ إلى صاحب البيانات المشار إليه في الفقرة ١ إذا تم استيفاء أي من الشروط التالية:

أ- نفذت وحدة التحكم تدابير الحماية الفنية والتنظيمية المناسبة، وتم تطبيق تلك التدابير على البيانات الشخصية المتأثرة بعملية الانتهاك، ولا سيما تلك التي تجعل البيانات الشخصية غير مفهومة لأي شخص غير مخول بالوصول إليها مثل التشفير.

ب- اتخذ المراقب تدابير لاحقة تضمن أنه من غير المحتمل أن تتجسد المخاطر المرتفعة على حقوق وحريات الأشخاص المعنيين بالبيانات المشار إليها في الفقرة ١.

ج- قد يتطلب الأمر جهدا غير متناسب وفي هذه الحالية يجب أن يكون هناك اتصال عام أو إجراء مماثل يتم من خلاله إعلام الأشخاص المعنيين بالبيانات بطريقة فعالة وسريعة على قدم المساواة.

٤- إذا لم تقم وحدة التحكم بالفعل بنقل خرق البيانات الشخصية إلى صاحب البيانات فإن السلطة الإشرافية المختصة بعد أن تنظر في احتمال حدوث خرق للبيانات يؤدي الى مخاطر عالية قد تطلب تلك السلطة من وحدة التحكم التواصل مع المعني بالبيانات وإبلاغه، أو قد تقرر أن أيا من الشروط المشار إليها في الفقرة ٣ تم استيفائها.

فيما نظمت المادة العاشرة[22] من القانون حق المستخدم في الحصول على بياناته الشخصية من (المتحكم والمعالج والحائز) عند طلبه، وفقا لضوابط محددة، وأعطت المادة الحق لـ(المتحكم أو المعالج) قرار برفض إتاحة البيانات، دون أن توضح المادة آلية الرد بالرفض، بالإضافة إلى أن القانون نص على إتاحة بيانات المستخدم ومساعدته في الحصول عليها أو تصحيحها أو محوها، وهو ما حاولت المادة تنظيمه، لكنها ظلت غامضة وغير واضحة فيما يخص حق المتحكم والمعالج في رفض الطلب المقدم من المستخدم لإتاحة بياناته، فالأصل في البيانات الشخصية هو إتاحتها للمستخدم أو من ذي صفة إذا توافرت المستندات اللازمة، وبالتالي حالة الرفض هنا في غير محلها، وتحرم المستخدم من حق إتاحه له القانون، فضلا عن أن المادة لم تأتي على ذكر الأسباب التي قد تكون السبب في رفض إتاحة البيانات.

ج- تأثير تأخر صدور اللائحة التنفيذية

وفقا للمادة الرابعة[23] من الديباجة الخاصة بالقانون، كان من المفترض أن تصدر لائحته التنفيذية خلال ستة أشهر من تصديق رئيس الجمهورية عبد الفتاح السيسي على قانون حماية البيانات الشخصية[24]، ورغم مرور عام إلا أن اللائحة التنفيذية لم تصدر حتى الآن[25]، مما يجعل العمل بالقانون معطل وفقا للمادة السادسة من ديباجته التي ربطت العمل بالقانون وتوفيق الأوضاع بصدور اللائحة التنفيذية[26].

كما حدد القانون في مادته الثالثة في باب (حقوق الشخص المعني بالبيانات وشروط جمع ومعالجة البيانات)[27]، الشروط اللازم توافرها أثناء معالجة البيانات، لكنها جاءت مقتضبة غير واضحة، حيث أسند المشرع للائحة التنفيذية تحديد السياسات والإجراءات والضوابط والمعايير. وهو ما يجعل عمليات المعالجة حتى الآن ورغم صدور القانون تتم دون سند أو تنظيم تشريعي.

---

22 المادة ١٠ من قانون حماية البيانات الشخصية: "يلتزم كل من المتحكم والمعالج والحائز عند طلب إتاحة البيانات الشخصية بالإجراءات الآتية:
1 – أن يكون بناءً على طلب كتابي يقدم إليه من ذي صفة أو وفقًا لسند قانوني.
2 – التحقق من توافر المستندات اللازمة لتنفيذ الإتاحة والاحتفاظ بها.
3 – 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.

23 مادة **4 من قانون حماية البيانات الشخصية**: "يصدر الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات اللائحة التنفيذية للقانون المرافق خلال ستة أشهر من تاريخ العمل بذلك القانون".

24 يتكون من 49 مادة.. تعرف على قانون حماية البيانات الشخصية

25 طلب إحاطة بسبب تأخر صدور اللائحة التنفيذية لقانون حماية البيانات الشخصية

26 المادة ٦ من قانون حماية البيانات الشخصية: يلتزم المخاطبون بأحكام هذا القانون بتوفيق أوضاعهم طبقًا لأحكام القانون المرافق ولائحته التنفيذية، وذلك خلال سنة من تاريخ صدور هذه اللائحة

27 المادة **3 من قانون حماية البيانات الشخصية**: "يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها ، توافر الشروط الآتية : ١- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني . ٢ - أن تكون صحيحة وسليمة ومؤمنة . 3 - أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها . 4-ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها. وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير.

بالإضافة إلى ذلك، أشارت المادة الخامسة[28] من الفصل الثالث إلى الالتزامات التي تقع على عاتق معالج البيانات الشخصية، وأشارت المادة إلى قواعد عامة يلتزم بها المعالج أثناء مرحلة المعالجة، لكنها أيضا أرجئت باقي القواعد والضوابط إلى اللائحة التنفيذية، وكان من الأولى أن تتضمن المادة كافة القواعد والضوابط المتعلقة بحماية البيانات أثناء مرحلة المعالجة بطريقة أكثر دقيقية.

28 مادة (٥): التزامات المعالج:

مع مراعاة أحكام المادة (١٢) من هذا القانون ، يلتزم معالج البيانات الشخصية بما يأتى :

١ - إجراء المعالجة وتنفيذها طبقا للقواعد المنظمة لذلك بهذا القانون ولائحته

التنفيذية ووفقا للحالات المشروعة والقانونية وبناء على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أى ذى صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد له.

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

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

٤ - 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 فى الأحوال المصرح بها قانونا.

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

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

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

٩ - إعداد سجل خاص بعمليات المعالجة لديه ، على أن يتضمن فئات المعالجة التى يجريها نيابة عن أى متحكم وبيانات الاتصال به ومسؤول حماية البيانات لديه، والمدد الزمنية للمعالجة وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها ووصفا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة.

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

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

١٢ - يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له فى جمهورية مصر العربية وذلك النحو الذى تبينه اللائحة التنفيذية.

فقد تحدثت المادة المذكورة عن ضرورة أن تتم المعالجة بطريقة مشروعة ولا تخالف النظام أو الآداب العامة، وكذلك عدم تجاوز المدة اللازمة للمعالجة وإخطار صاحب البيانات أو كل ذي صفة بالمدة اللازمة للمعالجة، بالإضافة إلى محو البيانات بانقضاء مدة المعالجة، وغيرها من الضوابط العامة.

لكن المادة افتقرت إلى الضوابط والقواعد الأكثر دقة على سبيل المثال؛

أ) لم تتحدث المادة عن ضرورة توافر مبدأ الشفافية وتحديد الهدف (بمعنى أن يقوم المعالج بشرح واف وكاف لصاحب البيانات عن أسباب المعالجة والغرض منها، بمصطلحات صحيحة مباشرة وواضحة ولا تتضمن أي مصطلحات غامضة أو معقدة).

ب) (السلامة والسرية)؛ تحدثت المادة عن حماية وتأمين عملية المعالجة بمضمونها الواسع، لكن كان من الأولى، أن تتحدث المادة بدقة أكثر عن الأمن المناسب للبيانات الشخصية، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقد أو التلف أو التلف العرضي، وذلك باستخدام التدابير الفنية أو التنظيمية المناسبة.

ج) ضرورة أن تكون البيانات التي سيتم تطبيق مرحلة المعالجة عليها ملائمة ومتلائمة ومحدودة لما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها، والهدف من ذلك هو (تقليل البيانات).

ونص القانون في المادة الأولى من الفصل الأول على إنشاء هيئة عامة تسمى «مركز حماية البيانات الشخصية»، تتبع الوزير المختص، وتكون لها الشخصية الاعتبارية، ويكون مقرها الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، وتهدف إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، ولها فى سبيل تحقيق أهدافها أن تباشر جميع الاختصاصات المنصوص عليها بهذا القانون، وألزمت المادة الثامنة[29] من الفصل الرابع (مسؤول حماية البيانات) المركز بإنشاء سجل لقيد مسئولى حماية البيانات الشخصية، لكنها أيضا ارجئت كافة شروط القيد وإجراءاته وآليات التسجيل للائحة التنفيذية.

كما ارجئت كافة الالتزامات والإجراءات والمهام الأخرى التي يجب على مسئول حماية البيانات الشخصية القيام بها أيضا إلى اللائحة التنفيذية وفقا للمادة التاسعة[30] من الفصل ذاته.

كما ارجئت المادة الإجراءات الخاصة بالإبلاغ والأخطار في حالة الخرق أو الانتهاك للائحة التنفيذية، وكان من الأولى أن تتضمن المادة كافة آليات الإبلاغ والإخطار وإلزام المتحكم والمعالج باللجوء اليها في حالة اكتشاف أي خرق أو انتهاك للبيانات.

29 المادة **8 من قانون حماية البيانات الشخصية** : "ينشأ بالمركز سجل لقيد مسئولى حماية البيانات الشخصية ، وتحدد اللائحة التنفيذية لهذا القانون شروط القيد وإجراءاته وآليات التسجيل.....، ويكون الشخص الطبيعي المتحكم أو المعالج هو المسئول عن تطبيق أحكام هذا القانون».

30 المادة **9 من قانون حماية البيانات الشخصية**: "يكون مسئول حماية البيانات الشخصية مسئولا عن تنفيذ أحكام القانون ولائحته التنفيذية وقرارات المركز ، ومراقبة الإجراءات المعمول بها داخل كيانه الإشراف عليها ، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقا لأحكام هذا القانون..... وتحدد اللائحة التنفيذية لهذا القانون الالتزامات والإجراءات والمهام الأخرى التي يجب على مسئول حماية البيانات الشخصية القيام بها

وحظرت المادة ١٤[31] من القانون عملية نقل البيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية إلا بشرطين، توافر مستوى من الحماية لا يقل عن المستوى المنصوص عليه في القانون، وبترخيص أو تصريح من المركز.

ويعتبر الشرطان اللذان نصت عليهما المادة مجرد مبادئ عاملة لعملية نقل أو تجهيز البيانات للمعالجة عبر الحدود، وأحيل الأمر للائحة التنفيذية، وكان من الأولى أن تستفيض المادة في الحديث عن مستوى الحماية المنتظر، وكذلك السياسات والمعايير والضوابط والقواعد اللازمة.

فعلى سبيل المثال؛ كان على المشرع أن يذكر ضرورة تكوين لجنة داخل مركز حماية البيانات مسؤولة للبت في طلبات نقل البيانات عبر الحدود، ومهامها تتمثل في تقييم مدى كفاية مستوى الحماية لدى الدولة الأجنبية التي سيتم نقل البيانات إليها، وتعمل اللجنة في تقيمها على مراعاة عناصر محددة تضمن مستوى الحماية المطلوب على سبيل المثال لا الحصر؛

أ) أن يتوافر في الدولة الأجنبية سيادة القانون، واحترام حقوق الإنسان والحريات الأساسية، والتشريعات ذات الصلة، العامة منها والقطاعية، بما في ذلك فيما يتعلق بالأمن العام والدفاع والأمن القومي والقانون الجنائي، ووصول السلطات العامة إلى البيانات الشخصية، فضلا عن تنفيذ مثل هذه التشريعات، وقواعد حماية البيانات، والقواعد المهنية والتدابير الأمنية، بما في ذلك قواعد نقل البيانات الشخصية إلى بلد ثالث آخر أو منظمة دولية أخرى يتم الامتثال لها في ذلك البلد أو المنظمة الدولية، وقانون الدعوى، وكذلك حقوق موضوعية قابلة للإنفاذ وتعويض فعال إداري وقانوني لأصحاب البيانات التي يتم نقل بياناتهم الشخصية.

ب) الالتزامات الدولية في الدولة الأجنبية، أو التزامات أخرى ناشئة عن اتفاقيات أو عقود ملزمة قانونا وكذلك عن مشاركتها في أنظمة متعددة الأطراف أو إقليمية، ولا سيما فيما يتعلق بحماية البيانات الشخصية.

31 البيانات الشخصية عبر الحدود

مادة (14): يحظر إجراء عمليات نقل للبيانات الشخصية التى تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوى من الحماية لا يقل عن المستوى المنصوص عليه فى 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 .

الأمر نفسه تكرر في المادة ال١٦[32] واليت تحدثت عن حالات إتاحة البيانات الشخصية خارج جمهورية مصر العربية لكنها غير مكتملة على النحو الذي تم ذكره خلال السطور السابقة، وظلت تحمل المادة شروط عامة، فضفاضة، غير محددة، حيث أن جميع الضوابط والمعايير تم ربطها باللائحة التنفيذية، وهو ما يعني أن المادة خلت من مضمونها الحقيقي وهو وضع شروط محددة يجب توافرها عند نقل البيانات عبر الحدود.

ويتضح مما تم ذكره خلال السطور السابقة، إن الكثير من الضوابط والمعايير والآليات قد أحيلت للائحة التنفيذية، وكان من الأولى أن يصدر القانون كاملا يحمل جميع الضوابط والآليات المطلوب تنفيذها، حيث أن قانون حماية البيانات الشخصية، هو قانون ذات طابع إجرائي، الهدف منه حماية بيانات المواطنين وحياتهم الخاصة وتنظيم العلاقة بين المستخدم والأطراف الأخرى مثل الحائز والمتحكم وكذلك المعالج، ما يعني ضرورة أن تكون القواعد الإجرائية والضوابط وكذلك الآليات شاملة لتطبيقها دون الاستناد إلى اللائحة التنفيذية.

32 مادة **(١٦) من قانون حماية البيانات الشخصية**: للمتحكم أو المعالج ، بحسب الأحوال ، إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية بترخيص من المركز متى توافرت الشروط الآتية:

١ - اتفاق طبيعة عمل كل من المتحكمين أو المعالجين ، أو وحدة الغرض الذى يحصلان بموجبه على البيانات الشخصية.

٢ - توافر المصلحة المشروعة لدى كل من المتحكمين أو المعالجين للبيانات الشخصية أو لدى الشخص المعنى بالبيانات.

٣ - ألا يقل مستوى الحماية القانونية والتقنية للبيانات الشخصية لدى المتحكم أو المعالج الموجودة بالخارج عن المستوى المتوافر فى جمهورية مصر العربية.

وتحدد اللائحة التنفيذية لهذا القانون الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لذلك.

رابعا: مخاطر مشكلات البنية التشريعية لحماية البيانات الشخصية

تكمن مخاطر العوار التشريعي في بنية حماية البيانات الشخصية، في احتمالية وقوع بعض الانتهاكات المتعلقة ببيانات الأشخاص وخرق حياتهم الخاصة، وتتمثل صور الانتهاك على سبيل المثال؛ في الاستغلال التجاري للبيانات الشخصية للمواطنين، فضلا عن الاستغلال السياسي في إطار الاستقطاب والحملات السياسية.

ظهر خطر الاستغلال السياسي للبيانات بوضوح في واقعة تسريب بيانات المواطنين في الولايات المتحدة الأمريكية والمعروفة إعلاميا بواقعة (كامبريدج أناليتيكا)[33]، حيث تم تسريب بيانات شخصية حساسة لما يقرب من ٢٠٠ مليون مواطن أمريكي تم استغلالهم أثناء العملية الانتخابية عام ٢٠١٦.

وظفت شركة البيانات "كامبريدج أناليتيكا" أستاذا بجامعة كامبريدج لتطوير تطبيق يمكنه الحصول على المعلومات الشخصية للناخبين الأمريكيين من مستخدمي فيسبوك، إذ ادعى البروفسور ألكسندر كوجان بأنه يجمع البيانات لأسباب أكاديمية أي لأغراض البحث العلمي.

ومن ثم قامت شركة البيانات "كامبريدج أناليتيكا" التي عملت مع حملة ترامب في انتخابات الرئاسة الأمريكية عام ٢٠١٦ باستخدام معلومات شخصية عن أكثر من ٥٠ مليون من مستخدمي فيس بوك، وذلك بهدف بناء نظام للتنبؤ والتأثير على خيارات الناخبين الأمريكيين في صناديق الاقتراع.

نال التسريب من حوالي ١,١ تيرا بايت من البيانات[34]، التي تتضمن تواريخ الميلاد، وعناوين السكن، وأرقام الهواتف، والآراء السياسية الخاصة بحوالي ٦٢ في المئة من السكان في الولايات المتحدة.

ويتضح من الوقعة المذكورة، أن توجه العالم نحو تشريع قوانين مثل اللائحة العامة لحماية البيانات الشخصية الخاص بتكتل الاتحاد الأوروبي، يقطع الطريق على تكرار مثل هذه الوقائع التي تسمح بانتهاك وخرق الحياة الخاصة للمواطنين.

وبما أن قانون حماية البيانات الشخصية في مصر جاء ليواكب المعيار العالمي الخاص بحماية البيانات الشخصية، فكان الأولى أن يصدر القانون كاملا خاليا من الغموض والعوار التشريعي حتى يتواكب مع المعيار الأساسي العالمي لحماية البيانات الشخصية وهو «GDPR».

كما تجدر الأشارة إلى ضرورة تعديل النصوص القانونية في قانون تنظيم الاتصالات وقانون جرائم تقنية المعلومات على النحو الذي تم ذكره سابقا، لسد الثغرات القانونية ولتعزيز حماية الحياة الخاصة من الخرق أو الانتهاك.

33 فيسبوك متورطة في فضيحة تسريب بيانات 50 مليون مستخدم لصالح حملة ترامب

34 تسريب معلومات عن ملايين الأمريكيين في "أكبر انتهاك" للبيانات الانتخابية في الولايات المتحدة.

خامسا: خاتمة وتوصيات

رغم وجود مواد بالدستور تنص بشكل واضح وصريح على حماية حرمة الحياة الخاصة، ورغم إصدار قانون لحماية البيانات الشخصية، لكن مازالت البيانات والحياة الخاصة مهددة بالخرق والانتهاك، نظرا للأسباب التي تم ذكرها ومناقشتها في هذه الورقة، ما يعني أنه إذا كان هناك رغبة حقيقة في حماية الحياة الخاصة والبيانات الشخصية للمواطنين فلابد من معالجة الأزمات التشريعية الموجودة في تلك القوانين، وخلق بيئة تشريعية غنية بالقواعد التنظيمية والضوابط، ولذلك يوصي المركز الإقليمي للحقوق والحريات بالآتي:

١- ينبغي على السلطة التشريعية إجراء تعديل تشريعي في قانون تنظيم الاتصالات، يتمثل في إقرار عقوبة على شركات الاتصالات في حال مخالفة نصوص القوانين والدستور تتمثل في تسريب أو انتهاك بيانات أو مكالمات للمستخدمين.

٢- ينبغي على السلطة التشريعية تعديل كافة مواد القانون المتعلقة بـ(حيازة-معالجة-تحكم) في البيانات، وعدم أرجاء القواعد التنظيمية والضوابط إلى اللائحة التنفيذية.

٣- ينبغي على السلطة التنفيذية، إقرار اللائحة التنفيذية لقانون حماية البيانات الشخصية، إعمالا بنصوص القانون والتي كان من المفترض أن تصدر خلال ٦ أشهر من صدور القانون.