EGYPTIAN INITIATIVE FOR PERSONAL RIGHTS

المبادرة المصرية للحقوق الشخصية

مسار
masaar
Technology & Law Community

اللائحة التنفيذية لقانون حماية البيانات الشخصية

اختبار تحويل القواعد العامة إلى التزامات قابلة للمساءلة

اللائحة التنفيذية لقانون حماية البيانات الشخصية:

اختبار تحويل القواعد العامة إلى التزامات قابلة للمساءلة

(تعليق قانوني من مؤسسة مسار والمبادرة المصرية للحقوق الشخصية)

فبراير 2026

"مسار" مجموعة من القانونيين والتقنيين المهتمين بالعمل على تعزيز الحقوق الرقمية والحريات المرتبطة بها في مصر، وتركز في عملها على الدمج بين التقنية والقانون وفهم تأثيرهما على الأفراد والمجتمع والحريات الأساسية. تستهدف "مسار" تركيز أنشطتها على الحريات الرقمية في النطاق المصري إلا أن ذلك لا يعزلها عن قضايا حقوق الإنسان في باقي مجتمعات المنطقة العربية والعالم.
للاتصال بمسار: masaarnet@gmail.com

المبادرة المصرية للحقوق الشخصية منظمة حقوقية مستقلة تعمل في مصر منذ عام 2002 على تعزيز وحماية الحقوق والحريات الأساسية في مصر، وذلك من خلال أنشطة البحث والدعوة والتقاضي في مجالات الحريات المدنية، والعدالة الاقتصادية والاجتماعية، والديمقراطية والحقوق السياسية، والعدالة الجنائية. للاتصال بالمبادرة: eipr@eipr.org

خلفية

في 15 يوليو 2020 صدر قانون حماية البيانات الشخصية رقم 151 لسنة 2020 بوصفه أول إطار تنظيمي مصري يضع قواعد التعامل مع البيانات الشخصية المعالجة إلكترونيًا كليًا أو جزئيًا. وبدأ العمل به بعد ثلاثة أشهر من اليوم التالي لتاريخ نشره، بما يعني دخوله حيز النفاذ خلال أكتوبر 2020. وقد ألزم المشرّع وزير الاتصالات وتكنولوجيا المعلومات بإصدار اللائحة التنفيذية خلال ستة أشهر من تاريخ العمل بالقانون.

وصِيغ قانون حماية البيانات الشخصية بمنهج يقوم على تفتيت عدد كبير من الالتزامات والقواعد إلى أحكام عامة تُترك تفاصيلها وإجراءاتها ومعاييرها الفنية للائحة التنفيذية. ونتيجة لذلك، لم يكن ممكنًا تفعيل كثير من أحكام القواعد التنظيمية فورًا، لأن بدء التطبيق العملي يتطلب -بالضرورة- معايير إجرائية وفنية محددة يمكن الاستناد إليها في القياس وإثبات الامتثال وترتيب المسؤولية القانونية عند المخالفة.

هذا التصميم التشريعي وضع تنظيم جانب مهم من القواعد، بصورة منفردة، في يد السلطة التنفيذية -مُمثلة في وزارة الاتصالات- بما يجعلها المتحكم الرئيسي في طريقة تطبيق القانون وتفسير كثير من قواعده. وبهذا فقد القانون قدرًا معتبرًا من الذاتية التنظيمية والقدرة على التطبيق المباشر دون ارتباط أو تعليق على قرارات وقواعد تنظيمية تصدرها السلطة التنفيذية لاحقًا عبر اللائحة التنفيذية.

وقد اتضح أثر هذا الاختيار التشريعي في طبيعة الموضوعات التي أُحيلت إلى اللائحة التنفيذية، إذ أُسند إليها وضع تفاصيل في ملفات محورية، على رأسها تنظيم منظومة الترخيص والتصريح والاعتماد لأنشطة جمع البيانات ومعالجتها، وتحديد فئات هذه التراخيص وإجراءات إصدارها وتجديدها ورسومها، إلى جانب وضع المعايير الفنية والقواعد الإجرائية لتأمين البيانات داخل مصر وخارجها، وتنظيم قيد ومسؤوليات مسؤولي حماية البيانات.

كما امتدت الإحالات إلى مسائل تمس الإنفاذ والإثبات، مثل تحديد شروط حجية الدليل الرقمي المستمد من البيانات الشخصية، فضلًا عن الضوابط والمعايير المتعلقة بنقل البيانات عبر الحدود والإجراءات الاحترازية اللازمة لإتاحتها لمتحكم أو معالج خارج البلاد.

وقد ترتّب على تأخير صدور اللائحة التنفيذية تعطل جانب كبير من البنية التطبيقية للقانون وتأخر انتقاله من الإطار التشريعي العام إلى قواعد تنفيذية قابلة للتطبيق والمساءلة. وظل مسار إعدادها غير واضح من حيث المراحل والجدول الزمني وآليات التشاور، حتى صدرت في 1 نوفمبر 2025 رسميًا بموجب قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 816 لسنة 2025 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية.

مقدمة

تأتي هذه الورقة بوصفها تعليقًا و تحليلًا قانونيًا للائحة التنفيذية لقانون حماية البيانات الشخصية، انطلاقًا من أن صدور اللائحة يُحدد عمليًا القواعد التفصيلية التي ستُدار بها دورة حياة البيانات الشخصية داخل الجهات العامة والخاصة، وكيفية ممارسة أصحاب البيانات لحقوقهم، وحدود التزامات المتحكمين والمعالجين، وأدوات الرقابة والإنفاذ المتاحة للدولة.

ومن ثمّ، فإن قراءة اللائحة قراءةً تحليلية تصبح ضرورية لفهم ما الذي أُضيف إلى الإطار التشريعي، وما الذي أُعيد تعريفه أو تضييقه أو توسيعه على مستوى التطبيق، وما الذي قد يترتب على ذلك من آثار مباشرة على الحق في الخصوصية وحماية البيانات.

اعتمدت الورقة منهجًا يقوم على فحص اللائحة بوصفها نصًا مُشغِّلًا للقانون، أي أنها تُترجم القواعد العامة إلى إجراءات ومعايير وأدوار مؤسسية قابلة للقياس والمساءلة. وفي هذا الإطار، تُقيِّم الورقة اللائحة من زاويتين:

- الأولى قانونية-إجرائية تتعلق بمدى وضوح القواعد وقابليتها للتطبيق وتحديدها لمسؤوليات الأطراف المعنية على نحو يمنع الالتباس ويحد من التعسف.
- والثانية حقوقية تتعلق بمدى ملاءمة القيود والإجراءات وتناسبها مع الغاية الحمائية للقانون، وبما إذا كانت اللائحة تُعزز ضمانات أصحاب البيانات أم تُضيف أعباءً أو مسارات إدارية تُضعف إمكانية ممارسة الحقوق بصورة فعّالة.

كما تضع الورقة في اعتبارها أثر المساحات التقديرية التي تمنحها اللائحة لجهات التنظيم، ومدى إحكام الضمانات الإجرائية المرتبطة بالترخيص والرقابة والتفتيش وتلقي الشكاوى.

وبناءً على ذلك، تنقسم الورقة إلى مسارين رئيسيين. أولهما هو اختبار مدى استيفاء اللائحة التنفيذية لمتطلبات التفويض المُحالة إليها من القانون، من خلال تتبع الموضوعات التي ترك القانون تفاصيلها للائحة، وبيان الكيفية التي عالجتها بها، ومدى كفاية هذه المعالجة لضمان تطبيق متسق وقابل للرقابة والمساءلة.

والمسار الثاني هو رصد أبرز الإشكاليات التي تكشفها اللائحة على مستوى التصميم التنظيمي أو الحماية الحقوقية أو قابلية الامتثال، مع تحليل أثرها العملي على أصحاب البيانات وعلى الجهات المخاطبة بأحكام القانون. وتنتهي الورقة بمجموعة من الملاحظات والتوصيات التي تستهدف دعم اتساق منظومة حماية البيانات مع الغاية الدستورية والحقوقية من حماية الخصوصية، وتعزيز قابلية إنفاذ القانون دون إخلال بضمانات الحقوق الأساسية.

وتكشف الإشكاليات المطروحة في الورقة أن اللائحة -رغم استيفائها جانبًا معتبرًا من الإحالات التشريعية- ما زالت تُنتج قدرًا من عدم اليقين القانوني؛ سواء على مستوى المدد وتداخل محطات النفاذ وتوفيق الأوضاع بين تاريخ صدور اللائحة وتاريخ نشرها وسريانها الفعلي، أو على سريان القانون، إذ تُعمّق مخاطر تفريغ الموافقة الصريحة (موافقة الشخص المعني) من مضمونها عبر الاعتداد عمليًا بموافقة ضمنية لمجرد تقديم البيانات للحصول على خدمة، دون وضع حد أدنى ملزم لمعايير الإخطار والفهم، ودون ضوابط تمنع التوسع في جمع بيانات غير ضرورية.

كما لم تحسم اللائحة بصورة واضحة كلفة ممارسة الحقوق ولا معايير تقديرها وتركتها لقرارات لاحقة، ولم تضع إطارًا إجرائيًا موحّدًا لطلبات الوصول والتصحيح والمحو وسحب الموافقة والاعتراض (جهة التلقي، شكل الطلب، أثر عدم الرد، المهل، وآلية القياس)، بما يهدد بتحويل الحقوق إلى مسارات متفاوتة بين الجهات ويُضعف قابلية القياس والمساءلة.

وتبرز إشكالات أوسع تمس شمولية حماية البيانات وحوكمة إنفاذ القانون، إذ تُكرّس الاستثناءات الواسعة (خصوصًا استثناء الأمن القومي بصياغته الفضفاضة وصلاحياته الإلزامية غير المنضبطة، واستثناء البنك المركزي والقطاع المصرفي) خطر انقسام مستويات الحماية وتفاوت حقوق الأفراد وآليات الإنفاذ بحسب الجهة الحائزة للبيانات، بما يمس جوهر مبدأ الشمولية.

ومن جهة أخرى، تُشدّد اللائحة قيود نقل البيانات عبر الحدود عبر جعل الترخيص/التصريح المسبق مدخلًا ملازمًا حتى مع توافر مستوى حماية كافٍ، مع بقاء تشغيل الاستثناءات بحاجة إلى ضوابط أكثر تحديدًا. بالإضافة إلى غياب إطار مُلزم للتقرير السنوي ونشر البيانات المجمعة، وضعف تنظيم الدور التوعوي والتدريبي، بما يضعف الثقة العامة ويزيد مخاطر الانتقائية أو التعسف في إنفاذ منظومة شديدة الحساسية.

أولًا: مدى استيفاء اللائحة التنفيذية لمتطلبات التفويض المُحالة من قانون حماية البيانات الشخصية

نصّ القانون على عدد كبير من القواعد والإجراءات وأحال إلى اللائحة التنفيذية تفصيلها. وبمقارنة بين نصوص القانون واللائحة، يتبيّن أن اللائحة التنفيذية في مجملها غطّت معظم الموضوعات التفصيلية المحال تنظيمها إليها. ومع ذلك، فإن هذا الاستيفاء يظل أقرب إلى الوفاء الشكلي بالإحالات التشريعية منها إلى بناء قواعد تشغيلية مُحكمة تُحسن اليقين القانوني. فيما يلي أبرز هذه الموضوعات مع بيان معالجة اللائحة لها:

1. الإطار العام لجمع ومعالجة البيانات والتزامات المتحكّم والمعالِج

أوجبت المادة (3) من القانون أن تُحدد اللائحة التنفيذية معايير وضوابط جمع البيانات الشخصية ومعالجتها وحفظها وتأمينها، وهو ما تناولته اللائحة في المادة (2) منها بوضع إطار عام يحكم عمليات التعامل مع البيانات منذ لحظة جمعها وحتى الاحتفاظ بها.

وفي هذا السياق ألزمت اللائحة الحصول على موافقة الشخص المعني قبل جمع بياناته، مع ضرورة إخطاره بالغرض بصورة واضحة، وعدّت أن تقديم الشخص بياناته للحصول على خدمة مشروعة يُعد موافقة ضمنية على المعالجة اللازمة لتقديم تلك الخدمة، مع عدم جواز استخدام البيانات لغرض آخر إلا بعد الحصول على موافقة جديدة. وألزمت اللائحة بتحديد مدة الاحتفاظ بالبيانات وفقًا للغرض الذي جُمعت من أجله، وبالحفاظ على سريتها، ومنع تداولها أو الإفصاح عنها إلا في الحدود التي يجيزها القانون.

وانتقل القانون في المادة (4) إلى تقرير التزامات محددة على المُتحكّم بوصفه مسؤول جمع البيانات، مع إحالة السياسات والإجراءات والمعايير الفنية المنظمة لهذه الالتزامات إلى اللائحة التنفيذية. وقد عالجت اللائحة هذه الإحالة في المادة (3) من اللائحة عبر تفصيل التزامات المتحكم، بما يشمل الحصول على ترخيص أو تصريح من المركز قبل معالجة البيانات، وعدم مخالفة الغرض المحدد للمعالجة، والتحقق من صحة البيانات الشخصية من مصدرها قبل استخدامها، ومحو البيانات بانقضاء الغرض المحدد وإخطار الشخص المعني بذلك، وعدم الاحتفاظ بالبيانات بصورة تسمح بتحديد صاحبها بعد انتهاء الغرض، إلى جانب تصحيح أي خطأ في البيانات فور علم المتحكم به.

كما أحالت المادة (5) من القانون إلى اللائحة التنفيذية تحديد السياسات والإجراءات والمعايير التفصيلية لالتزامات مُعالج البيانات، أي القائم بمعالجة البيانات للغير، فجاءت المادة (4) من اللائحة لتضع ضوابط تفصيلية تتقاطع في جوهرها مع التزامات المتحكم، مع مراعاة طبيعة دور المعالج بوصفه منفذًا لعمليات المعالجة لصالح متحكم أو نيابة عنه.

واشترطت اللائحة الترخيص أو التصريح من المركز قبل مباشرة النشاط، وأوجبت إعداد آلية معتمدة لتحديد حجم البيانات وغرض المعالجة، وتوثيق موافقة صاحب البيانات ومدى إخطاره بمدة المعالجة. كما ألزمت العاملين بالحفاظ على سرية البيانات وعدم إفشائها، وأقرّت تمكين مفتشي مركز حماية البيانات من الرقابة والتحقق من إجراءات التأمين.

وأضافت اللائحة التزامًا خاصًا بالمتحكم والمعالج الأجنبي الذي لا يوجد فرع له بمصر، يتمثل في تعيين ممثل محلي واعتماده من مركز حماية البيانات. وحظرت المادة (4) معالجة البيانات لغرض مغاير لغرض المتحكم إلا لأغراض إحصائية أو تعليمية وغير هادف للربح، وبشروط واضحة تتمثل في موافقة الشخص، وارتباط موضوع الدراسة بالبيانات، وترميز البيانات بما يمنع التعرف على أصحابها.

2. استخدام البيانات في تدريب الذكاء الاصطناعي والتقنيات الناشئة

تناولت اللائحة التنفيذية على نحو صريح استخدام البيانات في عمليات تدريب الذكاء الاصطناعي والتقنيات الناشئة والمبتكرة. إذ أقرت المادة (4 بند 7) من اللائحة التزام المعالج بأن يكون هذا الاستخدام "وفقًا للمبادئ المتعارف عليها محليًا وإقليميًا ودوليًا"، وبالقدر الذي يضمن توظيف تلك التقنيات بصورة لا يترتب عليها أي ضرر بالشخص المعني بالبيانات.

ويُفهم من هذا النص أن اللائحة تتعامل مع تدريب نماذج الذكاء الاصطناعي بوصفه صورة من صور المعالجة التي تستلزم مراعاة اعتبارات إضافية تتصل بطبيعة هذه التقنيات واتساع أثرها، وبما قد يترتب على نتائجها من تصنيف أو تنبؤ أو اتخاذ قرارات قائمة على البيانات.

وهذا يعني أن يلتزم المعالج -في حالة تدريب الذكاء الإصطناعي على بيانات محمية بموجب القانون- بإجراء المعالجة وفق أصول مهنية ومعايير حماية بيانات متداولة على نطاق واسع، بما يشمل -في حدوده العامة- الالتزام بالغرض المحدد وعدم تجاوز نطاقه، وتقليل البيانات إلى القدر اللازم للتدريب، واتخاذ تدابير فنية وتنظيمية كافية لتأمين البيانات ومنع إساءة استخدامها، وضمان قدر مناسب من الشفافية بشأن طبيعة الاستخدام وحدوده كلما كان ذلك مطلوبًا في إطار العلاقة مع صاحب البيانات.

إضافة إلى مراعاة الضوابط التي تمنع ترتّب آثار ضارة على الشخص المعني، سواء كانت أضرارًا مباشرة ناتجة عن إفشاء البيانات أو اختراقها، أو أضرارًا غير مباشرة قد تنشأ عن توظيف مخرجات التدريب في سياقات تمس الحقوق أو المصالح المشروعة للأفراد.

كما يُلزم النص المعالج بعدم الإضرار، بما يعني أن استخدام البيانات في التدريب ينبغي أن يُصمم ويُدار بطريقة وقائية تقلّل المخاطر على الشخص المعني بالبيانات، وأن يختار المعالج الإجراءات والأدوات التي تحول دون ترتّب نتائج تمس حقوق الأفراد أو تعرضهم للضرر، وذلك بوصفه جزءًا من التزاماته المهنية والقانونية عند استخدام تقنيات ناشئة في سياق معالجة البيانات الشخصية.

3. الإخطار عن خرق البيانات وانتهاكها

ألزمت المادة (7) من قانون حماية البيانات الشخصية المتحكّمَ والمعالجَ بإبلاغ مركز حماية البيانات عن أي خرق أو انتهاك خلال 72 ساعة من تاريخ العلم به، وبإخطار الشخص المعني خلال 3 أيام عمل، مع إحالة تفاصيل الإجراءات إلى اللائحة التنفيذية.

وقد جاءت المادة (5) من اللائحة لتضع إطارًا إجرائيًا أكثر تحديدًا، فأوجبت إنشاء سجل إلكتروني مؤمَّن يُقيَّد فيه كل خرق، على نحو يتيح توثيق الواقعة ومتابعتها، متضمنًا توقيت العلم وتوقيت الإبلاغ، وطبيعة الخرق وأسبابه، وحجم البيانات المتأثرة، وآثاره المحتملة، والتدابير التصحيحية المتخذة، وبيانات مسؤول حماية البيانات لدى الجهة، وأي بيانات إضافية يطلبها المركز.

كما كررت اللائحة حكمًا بالغ الحساسية يتمثل في الإبلاغ الفوري للمركز إذا كان الخرق يمس الأمن القومي، مع تقديم بيانات إضافية عن صلة الخرق بذلك.

أما إخطار الشخص المعني بالبيانات، فأعادت اللائحة التأكيد على وجوبه خلال 3 أيام عمل من تاريخ إبلاغ المركز، مع تحديد وسيلة الإخطار المتفق عليها مسبقًا (رسالة نصية، بريد إلكتروني، اتصال هاتفي...).

4. قيد واعتماد مسؤول حماية البيانات الشخصية وتحديد مهامه والتزاماته

أوجب القانون في المادة (8) إنشاء سجل لقيد مسؤولي حماية البيانات بالمركز، وفوّضت اللائحة التنفيذية في بيان شروط القيد وإجراءاته وآليات التسجيل، باعتبار أن وجود مسؤول حماية بيانات مؤهل ومعتمد يمثل أحد مرتكزات الامتثال داخل الجهات التي تجمع البيانات أو تعالجها.

وقد أفردت اللائحة المواد (7) و(8) و(9) لتنظيم ذلك، فحددت شروط قيد مسؤول حماية البيانات، بما يشمل توافر مؤهلات دراسية أو شهادات احترافية مع خبرة عملية ذات صلة، واجتياز الاختبارات المعتمدة من المركز، وحُسن السمعة وعدم الإدانة في جرائم مخلة بالشرف.

كما بيّنت اللائحة مستندات القيد المطلوبة، ومنها صورة الهوية، وصورة شخصية، وبيانات المؤهلات، وسنوات الخبرة، وصحيفة الحالة الجنائية، وما يفيد اجتياز الاختبار، وأي كود سابق إذا كان الشخص قد قُيِّد من قبل.

ثم أوضحت إجراءات دراسة طلب القيد والبت فيه خلال 30 يوم عمل من تاريخ تقديمه، مع إمكانية طلب استيفاء مستندات خلال مدة يحددها المركز، على أن يتم الرد خلال 15 يومًا من تاريخ الاستيفاء. ونصّت كذلك على التزام الممثل القانوني لكل كيان بتسجيل مسؤولي حماية البيانات لديه ليباشروا مهامهم وفق أحكام القانون.

كما أنشأت المادة (9) من اللائحة سجلًا إلكترونيًا بالمركز لقيد المسؤولين ومنح كل منهم رقمًا تعريفيًا (كود) يُبيّن حجم وطبيعة البيانات المصرح له التعامل معها بحسب نتيجة اختباره. ويُتاح طلب القيد إلكترونيًا سواء من خلال المتحكم أو المعالج لقيد موظف لديه، أو من الشخص الطبيعي نفسه الراغب في الاعتماد، بما يضع إطارًا واضحًا لتأهيل واعتماد مسؤولي حماية البيانات وتوثيق نطاق اختصاصهم.

وبالارتباط بهذا التنظيم الإجرائي لقيد المسؤولين واعتمادهم، نصّت المادة (9) من القانون على دور ومسؤوليات أساسية لمسؤول حماية البيانات، وأحالت إلى اللائحة تحديد أي التزامات وإجراءات ومهام أخرى تقع عليه؛ فجاءت المادة (12) من اللائحة لتضيف مجموعة من الالتزامات التفصيلية التي تُكمل الدور المنصوص عليه في القانون وتُفعّله عمليًا داخل الجهات المخاطبة بأحكامه.

وألزمت اللائحة مسؤول حماية البيانات بمراقبة تنفيذ سياسات التأمين الصادرة عن المركز لدى المتحكم أو المعالج، وإعداد تقرير سنوي يُقدّم للمركز عن حالة الخصوصية، كما قررت أنه إذا تم تغيير المسؤول يتعين على المسؤول البديل تقديم تقرير للمركز خلال 15 يومًا عن حالة حماية الخصوصية داخل الجهة.

وألزمت كذلك مسؤول حماية البيانات بمتابعة تلقي الشكاوى والطلبات المُقدَّمة من أصحاب البيانات والتأكد من تنفيذها، وبأن تُمارس مهامه على نحو لا يتعارض مع أي تكليفات أخرى قد تضر بحماية البيانات، كما أوجبت وضع نظام عمل منفصل إذا كان مسؤولًا واحدًا يعمل لعدة جهات، بما يضمن قيامه بمهامه دون إخلال أو تضارب.

وتأتي هذه الالتزامات مضافةً إلى المهام المنصوص عليها في القانون، مثل التقييم الدوري لنظم الحماية، وكونه نقطة اتصال مع المركز، وتمكين الأفراد من ممارسة حقوقهم، والإبلاغ عن الخروقات، وغيرها من الواجبات التي تجعل من مسؤول حماية البيانات حلقة وصل مركزية بين متطلبات الامتثال داخل الجهة وحقوق أصحاب البيانات، والرقابة التنظيمية من جانب المركز.

5. معايير حجية الدليل الرقمي المستمد من البيانات الشخصية

أقرت المادة (11) من قانون حماية البيانات الشخصية أن للدليل الرقمي المستمد من البيانات الشخصية ذات الحجية في الإثبات المقرّرة للأدلة المستمدة من البيانات والمعلومات الخطية، على أن ترتبط هذه الحجية باستيفاء معايير وشروط فنية تُحددها اللائحة التنفيذية.

وبموجب هذا، جاءت المادة (13) من اللائحة لتفصّل المعايير الحاكمة للدليل الرقمي من خلال اشتراط أن تتم عملية جمع أو استخراج الدليل باستخدام تقنيات تضمن عدم تغيير البيانات أو تحديثها أو محوها أو تحريفها، وأن يكون الدليل ذا صلة بالواقعة وفي نطاق الموضوع المطلوب إثباته أو نفيه وفقًا لقرار جهة التحقيق أو المحكمة المختصة.

ونظّمت المادة (13) من اللائحة إطار الجهة المختصة بجمع الدليل واستخراجه وحفظه، فقيدت ذلك بمأموري الضبط القضائي المخوَّل لهم التعامل مع هذه النوعية من الأدلة أو الخبراء المختصين من جهات التحقيق أو المحاكمة، مع اشتراط بيان مواصفات البرامج والأدوات والأجهزة المستخدمة في محاضر الضبط أو التقارير الفنية بما يضمن الحفاظ على الأصل دون عبث.

وأضافت اللائحة إلى ذلك متطلبًا إجرائيًا يتعلق بتوثيق الأدلة الرقمية قبل الفحص والتحليل بمحضر إجراءات من المختص، عبر طباعة نسخ من الملفات المخزن عليها الدليل أو تصويرها بأي وسيلة مرئية أو رقمية واعتمادها، مع تدوين تاريخ ووقت الطباعة أو التصوير، وهوية القائم بهما، وبيانات الأجهزة والمعدات والأدوات المستخدمة، والبيانات والمعلومات الخاصة بمحتوى الدليل المضبوط، بما يضع إطارًا فنيًا وإجرائيًا متكاملًا لاكتساب الدليل الرقمي المستمد من البيانات الشخصية حجية الإثبات المشار إليها في المادة (11) من القانون، إلا أن نص المادة لم يضع تعريفًا واضحًا لمن هي جهات الخبرة وكيفية اختيارها.

6. ضوابط التعامل مع البيانات الشخصية الحساسة وبيانات الأطفال

أقرت المادة (12) من قانون حماية البيانات الشخصية وضع نظام خاص للتعامل مع فئة البيانات الشخصية الحساسة، يقوم في أساسه على الحظر كقاعدة عامة، بحيث لا يجوز للمتحكم أو المعالج -شخصًا طبيعيًا كان أو اعتباريًا- جمع هذه البيانات أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بعد الحصول على ترخيص من مركز حماية البيانات.

وأوجبت المادة ذاتها -في غير الأحوال المصرح بها قانونًا- الحصول على موافقة كتابية وصريحة من الشخص المعني بالبيانات، وعدّت أي تعامل يتعلق ببيانات الأطفال يستلزم موافقة ولي الأمر، مع تأكيد خاص على ألا تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر مشروطة بتقديم بيانات تزيد على ما هو ضروري للمشاركة. وأحالت المادة (12) من القانون كذلك إلى اللائحة التنفيذية لوضع المعايير والضوابط التي تُنظّم هذه الفئة من البيانات وتحدد كيفية حمايتها.

وبالاستناد إلى هذا، جاءت المادة (14) من اللائحة التنفيذية لتفصيل الضوابط والمعايير الواجبة على المتحكم أو المعالج عند التعامل مع البيانات الشخصية الحساسة، فأقرّت في مقدمتها التزام الحصول على ترخيص أو تصريح من المركز وفقًا لطبيعة النشاط وفئات التراخيص والتصاريح المحددة في اللائحة، وربطت ذلك بالحصول على موافقة كتابية صريحة -ورقية أو إلكترونية- من الشخص المعني بالبيانات، أو من ولي الأمر في حالة بيانات الأطفال، وذلك في غير الأحوال المصرح بها قانونًا.

كما أقرت أن يكون جمع هذه البيانات ومعالجتها مقصورًا على ما هو أساسي ولازم للغرض المرتبط بطبيعة عمل المتحكم أو المعالج،

وبما يضمن ألا يترتب على استخدامها ضرر بالشخص المعني بالبيانات، وألزمت بالالتزام بمعايير التأمين التي يقررها المركز عند التعامل مع هذه الفئة من البيانات.

وخصّت اللائحة مشاركة الأطفال في الألعاب أو المسابقات أو الأنشطة المشابهة بضوابط إضافية، فأكدت عدم جواز الحصول من الطفل على أكثر مما هو ضروري للمشاركة، وعدم استخدام هذه البيانات في عمليات تصنيف أو تتبع أو مراقبة سلوكية للأطفال، كما أتاحت للمركز اعتماد معايير أخرى يقرها مجلس إدارته بهدف حماية البيانات الشخصية الحساسة.

إلى جانب ذلك، ألزمت المادة (14) من اللائحة المتحكم أو المعالج بالإمساك بسجلات إلكترونية مؤمنة وفقًا لمتطلبات المركز، بما يضمن توثيق التعامل مع البيانات الحساسة بصورة قابلة للمتابعة والرقابة. وتشمل هذه السجلات -على وجه الخصوص- تسجيل موافقات الشخص المعني بالبيانات الحساسة أو ولي أمر الطفل عند التعامل مع تلك البيانات بأي صورة من الصور المشار إليها، وكذلك تسجيل طلبات الحذف أو المحو أو التعديل أو وقف المعالجة التي يقدمها الشخص المعني أو ولي أمر الطفل، وما يفيد تفعيل هذه الطلبات.

ويُكمل هذا الإطار ما ورد في المادة (15) من اللائحة بشأن الضوابط الخاصة ببيانات الأطفال، حيث نظّمت آلية الحصول على موافقة ولي الأمر قبل جمع بيانات الأطفال الأقل من 15 سنة ومعالجتها لغرض تقديم خدمة أو لأي غرض آخر، مع اشتراط أن تتضمن الموافقة النطاق الزمني لها، دون إخلال بحق ولي الأمر في العدول عن موافقته أو تعديلها، وإسناد اعتماد الآليات والصور التي تصدر عنها هذه الموافقات إلى المركز.

كما تناولت المادة ذاتها الفئة العمرية من 15 سنة حتى 18 سنة، وأقرت التزام (الطفل أو ولي الأمر) تقديم موافقة ولي الأمر على جمع بيانات الطفل ومعالجتها، على أن يتولى المركز تحديد آليات ذلك بما يضمن استيفاء الاشتراطات القانونية المقررة في هذا الشأن.

7. ضوابط نقل البيانات الشخصية عبر الحدود وإتاحة البيانات لأطراف خارج مصر

حظرت المادة (14) من القانون نقل أو تخزين أو معالجة أو إتاحة البيانات الشخصية خارج مصر إلا بتوافر مستوى حماية لا يقل عن المقرر في القانون، وبشرط الحصول على ترخيص أو تصريح من مركز حماية البيانات، وفوّضت اللائحة التنفيذية في وضع السياسات والمعايير والضوابط اللازمة لذلك.

وقد تناولت المادة (16) من اللائحة هذا الملف بإسهاب، فوضعت في جوهرها تنظيمًا يقوم على حزمة من القيود المتراكبة التي تحكم نقل البيانات عبر الحدود، في مقدمتها اشتراط الحصول المسبق على ترخيص أو تصريح من المركز لنقل البيانات إلى دولة أجنبية، وربط منح هذا الترخيص بتقييم كفاية مستوى الحماية في الدولة المستقبِلة، مع إضافة شرط موافقة الشخص المعني بالبيانات على نقل بياناته خارج البلاد.

كما فرضت اللائحة التزامات تقنية وتنظيمية لضمان حماية البيانات خلال النقل أو التداول أو التخزين في الخارج، وقصرت النقل على الدول المحددة في الترخيص، وألزمت بتحديثه عند إضافة دول جديدة، بما يجعل نطاق النقل محددًا ومقيدًا بحدود الترخيص ذاته من حيث الدول والضمانات المفترضة لحماية البيانات.

ويعكس التنظيم الوارد في اللائحة التنفيذية أن نقل البيانات الشخصية عبر الحدود يُدار من خلال نهج يقوم على الترخيص أو

التصريح المسبق بوصفه المدخل الرئيسي للسماح بالنقل، بحيث يرتبط اتخاذ قرار النقل ابتداءً بصدور إذن من الجهة المختصة. وبذلك يصبح الترخيص المسبق هو الأداة المركزية التي يمر عبرها تنظيم التدفقات العابرة للحدود، مع ما يترتب على ذلك من تحديد نطاق النقل بالدول المعتمدة في الترخيص، وإلزام بتحديثه إذا أضيفت دول أخرى.

وفي سياق متصل بتنظيم النقل عبر الحدود، أتاحت المادة (16) من القانون للمتحكم أو المعالج أن يشارك البيانات الشخصية مع طرف آخر خارج مصر بترخيص من المركز متى توافرت شروط محددة، من بينها وحدة طبيعة عمل الطرفين أو وحدة الغرض، وتوافر المصلحة المشروعة، وتحقق مستوى حماية لا يقل عن المستوى المقرر في مصر، وأحالت للائحة التنفيذية وضع الاشتراطات والاحتياطات اللازمة لذلك.

وجاءت المادة (17) من اللائحة لتفصيل شروط إتاحة البيانات عبر الحدود، فاشترطت توافق نشاط وخدمة كلا الطرفين أو تكامله بما يحقق مصلحة مشروعة لهما أو لصاحب البيانات، وفرضت اتخاذ احتياطات تضمن مستوى حماية قانونية وتقنية للبيانات لدى الطرف الخارجي لا يقل عن المعمول به في مصر، إضافة إلى أي احتياطيات أو معايير أخرى يحددها المركز، بما يجعل «الإتاحة» لطرف خارجي إطارًا تنظيميًا موازيًا للنقل الدولي، قائمًا على الترخيص والاشتراطات والاحتياطات، وبحيث ترتبط مشروعيته بوجود مصلحة مشروعة وبضمان مستوى الحماية المكافئ داخل الدولة المستقبلة.

8. القواعد المنظمة للتسويق الإلكتروني المباشر

حددت المادتان (17) و(18) من قانون حماية البيانات الشخصية شروطًا وضوابط للتسويق الإلكتروني المباشر، من بينها الحصول على موافقة الشخص المعني، وبيان هوية المُرسل، وتوفير وسيلة واضحة للاعتراض أو إلغاء الاشتراك، ثم أحالت المادة (18) إلى اللائحة التنفيذية وضع القواعد والشروط والضوابط التفصيلية لهذا النوع من المعالجة.

وبناءً على هذا، أفردت اللائحة المادة (18) لتنظيم التسويق الإلكتروني المباشر، فميّزت بين التزامات سابقة على ممارسة النشاط تُلقيها على عاتق المُرسِل (لأي اتصال إلكتروني بغرض التسويق المباشر)، وبين ضوابط تحكم كيفية ممارسة التسويق الإلكتروني.

من حيث الشروط الواجبة على المُرسِل -سواء كان متحكمًا أو معالِجًا أو وسيطًا تسويقيًا- اشترطت اللائحة الحصول على ترخيص من المركز لمزاولة نشاط التسويق الإلكتروني، وأوجبت الحصول على موافقة صريحة مسبقة من الشخص المعني بالبيانات قبل توجيه الرسائل التسويقية إليه، وأقرت التزامًا بمحو البيانات الشخصية للمستهدف إذا عدل عن موافقته أو انتهى الغرض أو المدة المحددة للمعالجة.

وعلى مستوى الضوابط خلال ممارسة التسويق، قررت اللائحة عدم استخدام البيانات التي جُمعت لأغراض التسويق في أي غرض آخر أو مشاركتها مع أطراف أخرى دون موافقة جديدة، وألزمت بأن تتضمن الرسالة أو الاتصال معلومات واضحة منذ البداية عن هوية المُرسِل والغرض التسويقي، وبتمكين الشخص بسهولة من رفض الرسائل أو إلغاء الاشتراك عبر وسيلة يتيحها المركز، سواء برسالة أو بريد إلكتروني أو مكالمة هاتفية أو غير ذلك.

وامتد التنظيم إلى الوسطاء التسويقيين، حيث ألزمتهم اللائحة بالتحقق من أن الجهة الأصلية لديها موافقات الأشخاص قبل استخدام بياناتهم، وبالاحتفاظ بسجل يثبت مصدر البيانات، وما يفيد الموافقة، وإجراءات الاعتراض التي تلقوها.

كما أوجبت اللائحة احتفاظ المُرسِل بسجلات إلكترونية تكون متاحة للمركز عند الطلب، تتضمن كيفية وتاريخ الحصول على موافقة الشخص، وأي طلبات إلغاء أو تعديل للموافقة، وإجراءات الاستجابة لهذه الطلبات، مع توثيق آليات تأمين البيانات أثناء الحملة التسويقية. وخصّصت اللائحة وسيلة اتصال لدى المركز لتلقي شكاوى الجمهور المتعلقة برسائل التسويق المباشر.

9. التراخيص والتصاريح واعتمادات حماية البيانات ورسومها

نظّمت اللائحة التنفيذية منظومة التراخيص والتصاريح وشهادات الاعتماد بوصفها إحدى الأدوات التنظيمية الأساسية لتشغيل أحكام قانون حماية البيانات الشخصية، سواء من حيث تحديد الفئات والمستويات، أو وضع شروط وإجراءات الإصدار والتجديد والنماذج، أو ضبط الرسوم في حدود السقوف التي قررها القانون، بحيث لا تتجاوز مليوني جنيه للترخيص، ولا تتجاوز 500 ألف جنيه للتصريح أو الاعتماد.

وفي هذا الإطار، أقرت المادة (19) من اللائحة تصنيف تراخيص الأشخاص الاعتبارية بحسب حجم سجلات البيانات الشخصية لدى المتحكّم أو المعالِج، على نحو يبدأ بإعفاء الشريحة الأصغر من الرسوم ثم يتدرج تصاعديًا كلما زاد حجم البيانات، وصولًا إلى الحد الأقصى المقرر لمن تتجاوز سجلاته خمسة ملايين.

وإلى جانب معيار حجم البيانات، ميّزت اللائحة بين الترخيص الذي يغطي نشاط المتحكّم والمعالِج معًا وبين الترخيص الذي يقتصر على أحدهما، فخفضت الرسوم إلى 50% عند قصر النشاط على دور واحد، كما أقرت رسومًا مخفّضة وثابتة لفئات محددة مثل جمعيات المجتمع المدني والنقابات والأندية.

وعلى صعيد التصاريح، خصصت المادة (20) من اللائحة تنظيمًا للتصاريح المؤقتة التي تقل مدتها عن سنة، وربطت الرسوم بمدتين معًا: مدة التصريح وحجم البيانات محل المعالجة، في تدرج يبدأ بإعفاء الشرائح الصغيرة ويصل إلى الحد الأقصى القانوني للشرائح الأكبر، مع تكرار منطق التخفيض بنسبة 50% إذا كان التصريح يقتصر على نشاط المتحكّم فقط أو المعالِج فقط.

وبالتوازي مع تنظيم التراخيص والتصاريح، نظّمت اللائحة كذلك شهادات الاعتماد للمستشارين العاملين في مجال حماية البيانات، بوصفها آلية لاعتماد مقدمي الاستشارات سواء كانوا أشخاصًا طبيعيين (كالخبراء الأفراد) أو أشخاصًا اعتباريين (كالشركات الاستشارية). وحدّدت المادتان (32) و(33) شروط الحصول على شهادة الاعتماد لتقديم استشارات حماية البيانات، واشترطت للمستشار الفرد توافر مؤهلات علمية أو شهادات احترافية وخبرة عملية، كما اشترطت بالنسبة للأشخاص الاعتبارية تقديم ما يفيد نشاط الكيان وخبرته في المجال.

وجاءت المادة (34) لتُحدّد رسوم شهادة الاعتماد بمبلغ خمسة آلاف جنيه سنويًا، مع تقرير أن مدة الشهادة ثلاث سنوات قابلة للتجديد بذات الرسم، بما يضع إطارًا إجرائيًا ورسوميًا لاعتماد مقدمي الاستشارات ضمن منظومة الامتثال التي تُشغّلها اللائحة التنفيذية.

ثانيًا: أبرز الإشكاليات في اللائحة التنفيذية

رغم أن اللائحة التنفيذية غطت كثير من النقاط التي تم إحالتها إليها من قانون حماية البيانات الشخصية، ووفائها بالمتطلبات الشكلية للقانون، إلا أنها تثير عددًا من الإشكاليات الجوهرية عند فحصها والتي تتنوع بين إغفال إجرائي لبعض القواعد التنظيمية التي تحتاج تفصيل، أو تجاهل لبعض التفصيلات التي لم تتعرض لها اللائحة بالكامل.

1. تعميق المخاوف بشأن فعالية الموافقة الصريحة على جمع البيانات ومعالجتها

يُعدّ الحصول على موافقة حرة ومستنيرة من صاحب البيانات أحد المرتكزات الأساسية لحماية الخصوصية وحماية البيانات، بوصفه تعبيرًا عن حق الفرد في التحكم في بياناته وفي تقرير حدود استخدامها. وترتبط فعالية نظام الموافقة، في أي تشريع لحماية البيانات، بمدى اقترانه بضمانات تمكّن الأفراد من ممارسة حقوقهم على بياناتهم بصورة عملية، مثل الاطلاع والتصحيح والمحو والاعتراض، بما يحول دون تحوّل الموافقة إلى إجراء شكلي يُستعمل لتبرير المعالجة دون تمكين حقيقي.

وفي هذا الإطار، ينص قانون حماية البيانات الشخصية في المادة (2) على عدم جواز جمع أو معالجة البيانات إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانونًا، ويقرر حزمة من الحقوق لصاحب البيانات تتضمن حقه في العلم ببياناته والحصول عليها، وفي سحب الموافقة، وفي التصحيح أو المحو أو التعديل، وفي تقييد أو تخصيص المعالجة، وفي العلم بوقوع انتهاك أو خرق يتعلق ببياناته، وفي الاعتراض على المعالجة التي تكون مخالفة للحقوق والحريات الأساسية.

غير أن قراءة اللائحة التنفيذية تكشف عن نقاط متعددة تؤثر في الكيفية التي تُفعّل بها هذه الحقوق وفي مدى قدرة نظام الموافقة على تحقيق غايته الحمائية على أرض الواقع.

تظهر أول هذه النقاط في طريقة صياغة الموافقة وآليات تحققها، ففي اللائحة التنفيذية في المادة (2) قاعدة مفادها أن إدلاء الشخص الطبيعي ببياناته تنفيذًا لخدمة أو معاملة مشروعة يُعد بمثابة موافقة على جمعها ومعالجتها لهذا الغرض. ويعني ذلك أن اللائحة تُقر عمليًا بنمط من الموافقة الضمنية حين يقدم الفرد بياناته للحصول على خدمة، كالتسجيل في موقع أو شراء منتج أو إتمام معاملة رقمية.

والمشكلة ليست في الاعتراف بأن العلاقة الخدمية تستلزم حدًا أدنى من المعالجة لتحقيق الغرض، وإنما في أن اعتبار تقديم البيانات بذاته موافقة قد يفتح الباب لتوسّع غير منضبط في الاستناد إلى هذا المنطق دون التأكد من أن الشخص قد استوعب نطاق المعالجة وحدودها بصورة كافية، خاصة إذا لم تُترجم قاعدة الإخطار بالغرض بطريقة واضحة إلى معايير إجرائية محددة.

كما أن ذلك يفتح الباب أيضًا لجمع بيانات تتجاوز البيانات الضرورية اللازمة لتقديم الخدمة، خصوصًا أن البند الثامن من المادة (3) من اللائحة ترك تقدير حجم ونوع هذه البيانات للقانون المنظم للنشاط، ومن الناحية التشريعية والعملية نجد أن القوانين المنظمة لغالبية الأنشطة التجارية -على سبيل المثال- خالية من أي تنظيم لهذه المسألة.

وصحيح أن اللائحة ألزمت المتحكم بإخطار الشخص بالغرض بصورة واضحة، لكن النص لم يبين ماهية الطريقة أو حدها الأدنى، حيث أغفلت اللائحة بيان ما إذا كانت الطريقة المتبعة سوف تكون بإدراج الغرض ضمن سياسة خصوصية طويلة - والتي لا يقرأها أغلب المستخدمين - أم يلزم تقديم إشعار مختصر وبارز وقت جمع البيانات، أم تصميم واجهات موافقة تُظهر العناصر الجوهرية للمعالجة بلغة مبسطة.

لذا فإن غياب التحديد يمتد أثره إلى جوهر الموافقة المستنيرة بوصفها موافقة قائمة على معرفة حقيقية ومفهومة، لا مجرد إتمام معاملة أو الضغط على زر ضمن شروط عامة.

وفي هذا السياق، كان من الممكن أن تسهم اللائحة في تعزيز فعالية الموافقة عبر وضع حد أدنى من معايير صحتها، مثل أن تكون منفصلة قدر الإمكان عن الشروط العامة، وأن تُصاغ بلغة واضحة، وأن تكون قابلة للسحب بسهولة وبذات بساطة إعطائها، أو على الأقل أن تضع إطارًا يتيح إصدار نماذج إرشادية أو صيغ معيارية لضمان تحقق العلم والاستيعاب عند طلب الموافقة، بدل ترك الأمر لممارسات متفاوتة بين الجهات قد تُفرغ شرط الموافقة الصريحة من مضمونه.

2. تأثير العبء المادي والأطر الإجرائية على ممارسة حقوق صاحب البيانات.

أثار القانون منذ صدوره نقاشًا حول إجازته فرض مقابل مالي على بعض الخدمات المرتبطة بممارسة الحقوق، بما في ذلك الوصول إلى البيانات من قبل الشخص المعنى بها، وبسقف قد يصل -وفق ما أجازه القانون- إلى 20 ألف جنية مصري. وفي المقابل، يُناط بالمركز مهمة تحديد المقابل الفعلي لكل خدمة في حدود السقف الذي رسمه القانون.

ورغم أن اللائحة التنفيذية صدرت لاحقًا لتنظيم جوانب متعددة من الامتثال، فإنها لم تتناول بصورة مباشرة قواعد تكلفة ممارسة الحقوق أو حدودها أو معايير تقديرها، بما قد يعني إحالة هذا الملف إلى قرارات تنظيمية لاحقة تصدر عن المركز.

وهذا يظل مثارًا لإشكال حقوقي؛ لأن حق الشخص في معرفة بياناته التي تحتفظ بها الجهات عنه، وحقه في الحصول عليها أو تصحيحها أو محوها، ليست امتيازات، بل هي عناصر مكوِّنة لحق الخصوصية وحماية البيانات ذاته. ومن ثم، فإن فرض عوائق مالية مرتفعة على ممارستها يخلق تفاوتًا فعليًا في إمكانية النفاذ إلى الحقوق، ويجعل تمتع الأفراد بها مرتبطًا بالقدرة على الدفع، وهو ما يضر على نحو خاص بالفئات الأقل دخلًا ويقوض الغاية الحمائية للقانون.

وتتعمق المخاوف أكثر عند الانتقال إلى النقطة التالية، وهي غياب تفصيل الإجراءات الخاصة بممارسة الحقوق على نحو مُلزم وموحّد؛ فبمراجعة اللائحة، يمكن ملاحظة أن بعض النصوص تعالج أجزاءً متفرقة من هذا المسار بصورة غير مباشرة، مثل إلزام المتحكم بمحو البيانات بانقضاء الغرض وإخطار الشخص المعني بذلك، أو إلزام مسؤول حماية البيانات بمتابعة تلقي الشكاوى والطلبات والتأكد من تنفيذها، أو اشتراطات حفظ سجلات تتضمن ما يفيد تنفيذ طلبات الحذف أو المحو أو التعديل في بعض الحالات.

بينما أكد القانون على مسارين في المادتين (32) و(33)؛ أولهما الحق في تقديم الطلب من الشخص المعني بالبيانات إلى الحائز/ المتحكم/ المعالج بشأن ممارسة أي من حقوقه المنصوص عليها في القانون، وإلزام الأخير الرد عليه خلال ست أيام عمل، والثاني يتعلق باللجوء لمركز حماية البيانات عبر التقدم بشكوى بشأن انتهاك حقوقه المنصوص عليها في القانون، ويلتزم المركز بالرد عليها وإخطار طرفيها خلال 30 يوم عمل، والحق في اللجوء للمركز لا يعد قيدًا إجرائيًا على الحق في لجوء الشخص المعني بالبيانات للقضاء بشأن أي انتهاك لحقوقه.

غير أن هذه المعالجات الجزئية لا تُغني عن وجود إطار إجرائي موحّد يحدد بصورة صريحة الجهة المختصة داخل الكيان بتلقي طلبات أصحاب البيانات، سواء كان ذلك مسؤول حماية البيانات أو إدارة مختصة أو خدمة العملاء، ويحدد شكل الطلب المقبول وما إذا كان يتعين توفير نموذج إلكتروني أو ورقي، ويضع مهلة محددة للرد، ويبين ما إذا كان عدم الرد خلال المهلة يُعد رفضًا أم تقصيرًا يتيح تصعيد الأمر مباشرة إلى المركز، ويضع قاعدة عامة لمسؤولية الجهة عن عدم التنفيذ أو التأخير.

إن ترك هذه التفاصيل للممارسات الداخلية لكل جهة يفتح الباب لتفاوت كبير في الاستجابة، وقد يؤدي في الواقع العملي إلى تباطؤ أو تجاهل طلبات الأفراد، خاصة إذا لم يقترن ذلك بآلية واضحة تضمن قابلية القياس والمساءلة.

ومن أهم الاشكالات هي حق الاعتراض وحق سحب الموافقة، وهما حقان جوهريان لضمان أن سيطرة الفرد على بياناته ليست لحظة أولى تنتهي عند جمع البيانات، بل سيطرة مستمرة يمكن تفعيلها لاحقًا متى تعارضت المعالجة مع حقوقه وحرياته الأساسية، أو متى أراد العدول عن الموافقة التي سبق منحها.

ورغم أن القانون ينص على حق الشخص في الاعتراض على معالجة بياناته أو نتائجها متى تعارضت مع حقوقه وحرياته الأساسية، ويقرر كذلك حقه في سحب موافقته على الاحتفاظ ببياناته أو معالجتها. إلاّ أن اللائحة التنفيذية لم تفرد تنظيمًا إجرائيًا عامًا يبين كيفية ممارسة الاعتراض أو كيفية سحب الموافقة في عموم حالات المعالجة، ولا يحدد على نحو واضح ما الذي يتعين على المتحكم أو المعالج فعله عند تلقي الاعتراض، وما هي المدد الزمنية للبت فيه، وما هو معيار التوازن بين مصلحة الجهة في الاستمرار في المعالجة وبين مصلحة الشخص في وقفها، وما هي الوسائل التي يجب توفيرها كي تكون ممارسة الحق سهلة ومباشرة.

ونجد أن اللائحة تناولت هذا المنطق في سياق محدد هو التسويق الإلكتروني المباشر، حيث اشترطت توفير وسائل ميسرة لرفض الاتصالات أو العدول عن الموافقة السابقة، وهو تطور إيجابي لكنه يظل محصورًا في مجال التسويق.

وتبرز هنا الحاجة إلى تعميم الفكرة بوصفها قاعدة عامة. فكل خدمة أو معاملة تقوم على موافقة الشخص ينبغي أن تضمن له وسيلة واضحة ومبسطة لسحب هذه الموافقة أو إنهاء المعالجة المرتبطة بها، بذات السهولة التي أُتيح بها إعطاء الموافقة في البداية، بما يحول دون تحول سحب الموافقة إلى حق نظري يصعب ممارسته عمليًا.

ما نثيره اللائحة التنفيذية في هذا السياق لا يتعلق بمبدأ الموافقة نفسها، وإنما بكيفية تشغيله على مستوى الشفافية والمعايير الإجرائية وإتاحة الحقوق دون كلفة مُعيقة أو مسارات مُعقدة. ففعالية نظام الموافقة الصريحة لا تُقاس فقط بنصوص الإقرار، بل بقدرة الأفراد على فهم ما يوافقون عليه، وبقدرتهم على ممارسة حقوقهم بسهولة، وبوجود إجراءات موحدة يمكن القياس عليها والمساءلة بموجبها عند المخالفة.

3. الاستثناءات الواسعة على نطاق القانون والانتقاص من مبدأ الشمولية

يرمي قانون حماية البيانات الشخصية، في أصل فلسفته، إلى وضع إطار عام يضمن حماية خصوصية الأفراد في مواجهة الانتهاكات المحتملة المرتبطة بجمع البيانات ومعالجتها وتداولها. غير أن نطاق التطبيق الذي رسمته مواد إصدار القانون -ثم أكدت بعض جوانبه اللائحة التنفيذية- يتضمن استثناءات واسعة قد تؤدي، في قطاعات بعينها، إلى تقليص مجال الحماية أو جعلها متفاوتة بحسب الجهة القائمة بالمعالجة وطبيعة النشاط.

فقد استثنت المادة الثالثة من مواد الإصدار تطبيق القانون على ستة مجالات رئيسية، تشمل المعالجة للاستخدام الشخصي البحت، والمعالجة التي تتم بقصد الحصول على إحصاءات رسمية أو تنفيذًا لنص قانوني، والمعالجة لأغراض إعلامية مع اشتراطات تتعلق بالصحة والدقة وعدم الاستخدام لغير الأغراض الإعلامية، والبيانات المتعلقة بالضبط القضائي والتحقيقات والدعاوى، والبيانات لدى جهات الأمن القومي (وما تقدره لمقتضيات الأمن القومي)، إضافة إلى بيانات البنك المركزي المصري والجهات الخاضعة له (عدا شركات تحويل الأموال والصرافة) مع مراعاة قواعد البنك المركزي بشأن بيانات هاتين الفئتين.

ومنح القانون جهات الأمن القومي سلطة أن تطلب من المتحكم أو المعالج تعديل بيانات شخصية أو محوها أو عدم إظهارها خلال مدة زمنية محددة وفق اعتبارات الأمن القومي وعلى المتحكم تنفيذ ذلك فورًا.

وتبرز الإشكالية في الاستثناء المتعلق بجهات الأمن القومي، سواء من حيث اتساع نطاقه أو من حيث الصلاحيات الإضافية المرتبطة به. فالتعبير الوارد بشأن جهات الأمن القومي وما تقدره لمقتضيات الأمن القومي يفتح الباب لتأويل واسع حول حدود الجهات المشمولة ومعايير انطباق الاستثناء، كما يضيف -على مستوى الأثر- سلطة تقريرية لتلك الجهات تسمح لها بطلب تعديل بيانات شخصية أو محوها أو عدم إظهارها لدى جهات أخرى، مع إلزام المتحكم أو المعالج بتنفيذ ذلك فورًا.

وتكمن المشكلة هنا في أن معيار الأمن القومي يرد بصياغة عامة وفضفاضة دون تحديد موضوعي أو إجرائي لحدوده أو لمناط تطبيقه، وهو ما يُضعف إمكانية توقع استخدام الاستثناء ويجعل نطاقه قابلًا للاتساع بحسب التقدير الإداري.

وفي حين أن البند 5 من المادة الثالثة من مواد إصدار قانون حماية البيانات الشخصية، يعطي جهات الأمن القومي الصلاحية في «إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية» إلاّ تنه لم ينص على قيود موضوعية على نوع البيانات أو طبيعة الحالة التي تبرر الطلب، وما إذا كانت تتوافر آلية فعالة للرقابة على استخدام هذه الصلاحيات، سواء رقابة قضائية أو برلمانية أو رقابة مستقلة، بما يثير خطر أن يتحول الاستثناء -عمليًا- إلى نطاق خارج الحماية لا تحكمه قواعد اليقين القانوني ولا يتيح مساءلة واضحة عن أسباب التدخل وحدوده.

وصحيح أن حماية اعتبارات الأمن القومي قد تُستدعى في بعض السياقات بوصفها مصلحة مشروعة، إلا أن إدخالها كاستثناء واسع يتطلب -من منظور دستوري وحقوقي- أن تكون القيود محددة وواضحة وقابلة للضبط، وأن تقترن بضمانات تمنع تحولها إلى بوابة لإعفاءات شاملة أو أوامر ملزمة غير محكومة بمعايير.

ولا تقل الإشكالية أهمية في الاستثناء الخاص بالبنك المركزي المصري والجهات الخاضعة له، إذ يترتب عليه خروج القطاع المصرفي من نطاق القانون، مع الاكتفاء بقواعد البنك المركزي الخاصة بحماية بيانات العملاء.

ورغم أن وجود قواعد قطاعية قد يوفر بعض مستويات الحماية، فإن الاستثناء الشامل يطرح أثرًا مباشرًا يتعلق بحقوق أصحاب البيانات وآليات إنفاذها؛ إذ إن حقوقًا مثل سحب الموافقة أو الاعتراض أو تقديم الشكاوى إلى مركز حماية البيانات قد لا تنطبق في مواجهة جهة مستثناة من نطاق القانون، بما يجعل مركز الثقل في الحماية والرقابة محصورًا في الإطار القطاعي ذاته لا في المنظومة العامة التي أنشأها القانون.

ويؤدي ذلك إلى ازدواجية في مستويات الحماية وإلى تفاوت في الضمانات المتاحة للأفراد تبعًا للجهة التي تحتفظ ببياناتهم، وهو تفاوت شديد الحساسية إذا تعلق الأمر ببيانات مالية تُعد، بطبيعتها، من أكثر فئات البيانات الشخصية حساسية وتأثيرًا على الأمن الشخصي والاقتصادي للأفراد.

كما يثير هذا الاستثناء تساؤلًا حول مدى ضرورته بوصفه استثناءً كاملًا إذ كان من الممكن -من حيث المبدأ- معالجة أي تعارض محتمل في الاختصاص أو التنظيم عبر آليات تنسيق واضحة بين الجهة القطاعية (البنك المركزي) والجهة العامة المنشأة بموجب القانون (مركز حماية البيانات)، بدلًا من إخراج نطاق كامل من المعاملات والبيانات من تطبيق القانون وما يرتبه من حقوق وضمانات وآليات إنفاذ.

4. مخاوف بشأن قيود واستثناءات نقل البيانات عبر الحدود

تُعد مسألة نقل البيانات الشخصية خارج الحدود من أكثر ملفات حماية البيانات حساسية على المستوى الدولي، لأنها تقع عند تقاطعٍ مباشر بين حماية الخصوصية من جهة، ومتطلبات الاقتصاد الرقمي المعولم وتشغيل الخدمات العابرة للحدود من جهة أخرى.

وفي هذا السياق، يميل الاتجاه التشريعي الحديث إلى السماح بتدفق البيانات مع اشتراط توفير حماية مناسبة في الدولة المستقبِلة، بدلًا من المنع الصارم أو الإغلاق التنظيمي الذي قد ينعكس سلبًا على بيئة الخدمات الرقمية. غير أن القانون المصري اختار نهجًا يقوم على حظر نقل البيانات الشخصية خارج مصر إلا بعد الحصول على ترخيص أو تصريح من مركز حماية البيانات، وبعد التحقق من كفاية مستوى الحماية في الدولة الأجنبية.

وقد حاولت اللائحة التنفيذية تقديم إطار أكثر تفصيلًا لهذا النهج عبر وضع معايير للتقييم وتصور لاعتماد قائمة بالدول التي يتوافر فيها مستوى حماية كافٍ، إلا أن المخاوف العملية تظل قائمة، لأن هيكل التنظيم نفسه يُبقي على عبء جوهري يتمثل في طبيعة الترخيص المسبق كشرطٍ ملازم لعملية النقل. فحتى مع وجود مستوى حماية -في الدولة المستقبِلة- مساوي أو يزيد لمستوي الحماية في مصر، يظل من حيث المبدأ مطلوبًا التقدم للمركز بطلب ترخيص أو تصريح، كما يرتبط نطاق الترخيص بالدول المحددة فيه حصرًا ويستلزم تحديثه عند إضافة دولة جديدة.

وبالتوازي مع نظام الترخيص المسبق الذي كرسته اللائحة، يظل في القانون نفسه نطاقٌ مهم من الاستثناءات التي تسمح بنقل البيانات إلى دولة لا يتوافر فيها مستوى حماية كافٍ، وذلك وفق ما تقرره المادة (15) من القانون في حالات محددة، مثل موافقة الشخص المعني موافقة صريحة، أو الحالات المرتبطة بحماية حياة الشخص وتوفير علاجه، أو تنفيذ التزامات قانونية أو أحكام قضائية أو أوجه التعاون القضائي، أو اعتبارات المصلحة العامة، أو التحويلات النقدية وفق قوانين الدولة الأخرى، أو تنفيذًا لاتفاقيات دولية.

ومن حيث المبدأ، فإن وجود استثناءات من هذا النوع ليس غير مألوف في تشريعات حماية البيانات، إذ تُوجد عادةً آليات تسمح بالنقل في ظروف استثنائية ومحددة تجنبًا لتعطيل مصالح أساسية أو التزامات قانونية لا يمكن الوفاء بها بغير النقل. غير أن الإشكالية العملية هنا تتصل بكيفية تشغيل هذه الاستثناءات وحدود تفسيرها، خاصة إذا لم تقترن بضوابط إجرائية واضحة تحدد شروط تطبيق كل استثناء وحدوده ومعايير الضرورة والتناسب الخاصة به. فبعض العبارات، مثل الضرورة لحماية المصلحة العامة، تحمل بطبيعتها قدرًا من العمومية قد يُستند إليه لتبرير نقل البيانات دون قيود كافية إذا لم تُضبط بمعايير محددة يمكن القياس عليها، بما قد يفتح المجال أمام تفسيرات واسعة تختلف من جهة إلى أخرى، ويؤثر على اليقين القانوني وعلى توقعات أصحاب البيانات بشأن مصير بياناتهم عند النقل.

5. مركز حماية البيانات: سلطة واسعة وتبعية كاملة

أنشأ قانون حماية البيانات الشخصية مركز حماية البيانات الشخصية كهيئة عامة اقتصادية تتبع وزير الاتصالات وتكنولوجيا المعلومات، ومنح المركز حزمة واسعة من الاختصاصات التي تجعل منه محور منظومة الحماية وصاحب اليد العليا في تشغيلها. فالمركز يختص بإصدار التراخيص والتصاريح والموافقات اللازمة لممارسة أنشطة المعالجة، واعتماد مسؤولي حماية البيانات والمستشارين، وتلقي الشكاوى والبت فيها وإصدار القرارات بشأنها، والقيام بأعمال التفتيش والرقابة، ووضع السياسات والضوابط والتدابير المتعلقة بحماية البيانات، والتنسيق مع الجهات الحكومية وغير الحكومية، إلى جانب غير ذلك من الصلاحيات التنظيمية والتنفيذية.

ويعني ذلك أن تصميم المنظومة يقوم على تركيز أدوات التنظيم والرقابة والإنفاذ في جهة واحدة، وهو تركيز يرتبط مباشرة بمسألتين متلازمتين، الأولى هي مدى استقلالية هذه الجهة عن التأثير الحكومي المباشر، والثانية هي مدى شفافية عملها وقدرتها على إشراك أصحاب المصلحة في صياغة سياساتها ومعاييرها.

على مستوى الاستقلال المؤسسي، لا يتعامل القانون مع المركز بوصفه هيئة مستقلة تمامًا، بل يضعه داخل بنية تنفيذية تتبع الوزير المختص، ويعكس ذلك بشكل واضح نموذج الحوكمة الذي تبناه المشرع للمركز. فالقانون لا يقر استقلالًا كاملًا للمركز على نحو يُحصّنه من نفوذ السلطة التنفيذية أو تضارب المصالح في تنظيم قطاعات تتداخل معها الوزارة ذاتها، بل يجعل الوزير في موقع مركزي داخل منظومة اتخاذ القرار؛ إذ يرأس الوزير مجلس إدارة المركز، كما يضم تشكيل مجلس الإدارة ممثلين عن وزارات وجهات متعددة ذات طبيعة حكومية وأمنية.

ويثير هذا النموذج تساؤلات عملية حول قدرة المركز على تنظيم جهات قد تكون للدولة -أو للوزير بوصفه رئيسًا لمجلس الإدارة- مصلحة مباشرة أو غير مباشرة في نشاطها، خاصة في القطاعات التي تُعد من أكبر جامعي البيانات وأكثرها تأثيرًا، بما في ذلك جهات حكومية وشركات كبرى تعمل في مجال الاتصالات أو تقديم خدمات عامة رقمية.

كما أن غياب الاستقلال الكافي ينعكس على الثقة العامة في قرارات المركز وحيادها، ويجعلها أكثر تعرضًا لتأثيرات سياسية أو اقتصادية بحكم طبيعة التبعية وهيمنة ممثلي جهات حكومية على بنية المجلس، وهو إشكال يرجع إلى تصميم القانون ذاته أكثر مما يرجع إلى اللائحة التنفيذية، لكنه يظل مؤثرًا في تقييم فعالية المنظومة ككل.

وتبرز مسألة الشفافية والمشاركة بوصفها شرطًا موازيًا لسلامة الحوكمة وشرعية صنع القاعدة التنظيمية. فقد أثيرت منذ لحظة صدور القانون -ثم مسار إعداد اللائحة التنفيذية- ملاحظات تتعلق بضعف وضوح عملية الإعداد وحدود التشاور العام، وبأن مسارات المناقشة لم تكن على قدر كافٍ من العلنية التي تسمح بتقييم اتساع المشاركة وتوازنها.

وفي ضوء انتقال المركز إلى مرحلة التشغيل الفعلي، تصبح مسؤوليته المؤسسية مضاعفة في بناء قنوات تواصل منتظمة ومعلنة مع مختلف الأطراف المعنية، وإتاحة سياساته وقراراته وإرشاداته بشفافية، وإشراك المجتمع التقني والقانوني والمهني وأصحاب الخبرة، إلى جانب ممثلي المستخدمين والباحثين والجهات المعنية بالحقوق والحريات، في صياغة المدونات الإرشادية ومدونات السلوك والمعايير الفنية التي سيعتمد عليها الامتثال. لأن استمرار المركز في العمل كجهاز بيروقراطي مغلق -حتى مع اتساع صلاحياته- من شأنه أن يضعف من قبول قراراته اجتماعيًا ويهز الثقة في عدالة إنفاذه، ويجعل الالتزام بالقواعد أقرب إلى كونه امتثالًا مفروضًا لا منظومة حماية تستند إلى يقين قانوني وثقة عامة.

ويتصل بذلك أثر ثالث يتجاوز التصميم المؤسسي إلى كيفية انعكاس الصلاحيات الواسعة للمركز على الحقوق والحريات في الممارسة. فالمركز يتمتع بأدوات رقابية وإنفاذية، تشمل التفتيش والضبطية القضائية وإلزام الجهات بتدابير حماية محددة وفرض غرامات إدارية، وهي أدوات يمكن -من حيث المبدأ- أن تُستخدم لتعزيز الامتثال وحماية حقوق الأفراد وردع الانتهاكات. غير أن اتساع السلطة التنفيذية والرقابية في يد جهة واحدة، مع ضعف ضمانات الاستقلال وتعدد ممثلي جهات أمنية وحكومية داخل بنيتها الحاكمة، يثير مخاوف تتعلق بإمكان الانتقائية أو التعسف في توجيه الرقابة والإنفاذ.

لذا قد يتركز التفتيش على كيانات أصغر وأضعف تنظيمًا، في حين تُغضّ الطرف عن كيانات أكبر، أو تُستخدم إجراءات التفتيش وإثارة مخالفات بيانات شكلية كمدخل للضغط على جهات بعينها، بما في ذلك مؤسسات إعلامية أو منظمات غير هادفة للربح أو مشروعات صغيرة، بدلًا من توجيه الإنفاذ إلى مناطق الخطر الحقيقي وأكبر مجالات الأثر على حقوق أصحاب البيانات.

6. غياب التزامات المركز بالشفافية وأطر دوره التوعوي

وتتسع دائرة الإشكالات حين ننتقل إلى ما أغفلته اللائحة التنفيذية في تنظيم وظائف محورية للمركز تمس شفافية المنظومة وقياس أدائها وقدرة الجمهور والبرلمان والباحثين والإعلام على تقييمها. إذ يُعد وجود التقرير السنوي عن حالة حماية البيانات الشخصية في جمهورية مصر العربية من أهم أدوات المركز المؤسسية وأداة قياس ومراجعة عامة تكشف المؤشرات والاتجاهات وتسمح بفهم طبيعة الانتهاكات ومستويات الامتثال وتطور أداء المنظومة.

ومع ذلك، ورغم إسهاب اللائحة التنفيذية في تنظيم إجراءات التراخيص والتصاريح والتسجيل والتفتيش وغيرها من الجوانب الإجرائية، فإنها لم تُفرد إطارًا تنظيميًا يوضح كيف يُعد هذا التقرير، وما حدوده، وما الحد الأدنى من محتواه، وما موعد إصداره، وكيف يُنشر ويُتاح للجمهور.

ويترتب على هذا الإغفال ضرر مباشر يتمثل في تحويل التقرير من التزام مؤسسي دوري قابل للمساءلة إلى وعد عام غير منضبط، بما يضعف إمكانية تتبع اتجاهات الانتهاكات، وقياس فعالية إنفاذ القانون، وتحديد القطاعات الأعلى خطرًا، وكشف مواطن القصور في الحماية.

كان من الممكن أن تتضمن اللائحة تفصيلات عملية تجعل التقرير أداة شفافة قابلة للقياس، على نحو يقرر إلزامية نشره على موقع المركز خلال موعد سنوي محدد، ويضع هيكلًا ثابتًا يشتمل على حد أدنى من البيانات المجمعة التي لا تُعرّف الأفراد، مثل إحصاءات الشكاوى والبلاغات وأنواعها ونتائجها، وبيانات مجمعة عن خروقات البيانات وأسبابها والتدابير التصحيحية، وأنماط الامتثال لدى القطاعات المختلفة، وتقييمًا عامًا لمستوى تطبيق مبادئ الحماية الأساسية من واقع التفتيش والرقابة. إضافة إلى بيان ما إذا كان التقرير يتضمن توصيات تشريعية أو تنظيمية ذات طابع ملزم أو إرشادي، وكيف يتابع المركز تنفيذ توصياته عامًا بعد عام، مع وضع آلية مراجعة داخلية أو تشاورية تضمن جودة التقرير وعدم تحوله إلى سرد رسمي يطمس أوجه الخلل بدل كشفها.

وبالمثل، تكشف اللائحة عن إغفال واضح للدور التوعوي والتدريبي الذي يُفترض أن يمارسه المركز عبر تنظيم المؤتمرات وورش العمل والدورات التدريبية والتثقيفية وإصدار المطبوعات والمواد الإرشادية. وهذه الوظيفة شرط لازم لتمكين الحقوق عمليًا، لأن حماية البيانات لا تتحقق بالنصوص وحدها، وإنما بقدرة الأفراد على معرفة حقوقهم وممارستها، وبقدرة الجهات على فهم التزاماتها وتطبيقها تقنيًا وإجرائيًا بصورة صحيحة.

غير أن اللائحة لم تضع إطارًا يحدد متى وكيف يمارس المركز هذا الدور، وما الفئات المستهدفة، وما الحد الأدنى من الأنشطة، وما أدوات قياس الأثر، بما يترك التنفيذ عرضة لأن يكون انتقائيًا أو موسميًا أو موجّهًا لفئات بعينها، كأن ينحصر في مخاطبة الكيانات الأكبر، في حين يظل المستخدمون والمشروعات الصغيرة والجمعيات الأهلية والإعلام وغيرهم من الجهات هي الحلقة الأضعف في سلسلة الامتثال.

ويخلق هذا الإغفال ضررًا مزدوجًا، فهو من جهة يُفاقم اختلال ميزان القوة بين المتحكمين والمعالِجين من ناحية وأصحاب البيانات من ناحية أخرى، لأن الحق لا يُمارس دون معرفة، ولأن الجهات الأقوى ستكون الأقدر على الامتثال الشكلي في حين يظل الأفراد بلا أدوات للمساءلة، وهو من جهة أخرى يضعف جودة الامتثال التقني لأن كثيرًا من الخروقات تنشأ من قصور تدريبي وإجرائي لا من سوء نية.

كان يمكن للائحة أن تضع حدًا أدنى من التنظيم العملي لهذا الدور عبر إلزام المركز بوضع خطة سنوية معلنة للتوعية والتدريب تتضمن موضوعات رئيسية مثل حقوق الأفراد وآليات الشكوى والإخطار بالخرق والبيانات الحساسة والنقل عبر الحدود، وعبر تطوير مواد إرشادية ونماذج مبسطة قابلة للاستخدام، مثل سياسات خصوصية نموذجية وصيغ موافقة واضحة وإرشادات لسحب الموافقة وإجراءات التعامل مع طلبات الوصول والمحو، إلى جانب تصميم برامج تدريب معتمدة لمسؤولي حماية البيانات والعاملين على المعالجة وربط معايير الاعتماد وتجديده بساعات تدريب دورية، فضلًا عن ضمان إتاحة المطبوعات والتوجيهات بلغة مبسطة للجمهور، لا أن تظل محصورة في لغة فنية تُخاطب الشركات فقط.

ثالثًا: التوصيات لتعزيز الإطار القانوني والتنظيمي لحماية البيانات

بناءً على استعراض أبرز الإشكاليات التي تكشفها اللائحة التنفيذية، يمكن صياغة حزمة توصيات عملية موجّهة إلى كل من المشرّع المصري والجهات التنظيمية، خاصة مركز حماية البيانات، بهدف معالجة أوجه القصور وتعزيز قابلية الامتثال دون الانتقاص من جوهر الحماية الحقوقية.

وتنقسم هذه التوصيات إلى ثلاثة محاور رئيسية. الأولى، إجراءات تنظيمية عاجلة يمكن للمركز إصدارها في صورة قرارات مُلزمة أو أدلة إرشادية ونماذج معيارية، والثانية مقترحات تشريعية متوسطة المدى تتطلب تعديلًا للقانون، والثالثة، تحسينات تنظيمية وتقنية تعزّز التطبيق العملي والشفافية وبناء القدرات.

1. تعويض القصور في اللائحة التنفيذية بقرارات تنظيمية وأدلة مُلزمة يصدرها مركز حماية البيانات

يُوصى بأن يبادر مركز حماية البيانات بوضع إجراءات تفصيلية وموحّدة لممارسة حقوق أصحاب البيانات، بحيث لا تبقى الحقوق المنصوص عليها إطارًا عامًا يختلف تشغيله من جهة إلى أخرى. ويُفترض أن تصدر هذه الإجراءات في قرار تنظيمي أو دليل مُلزم يحدد مسار الطلبات الخاصة بالاطلاع والحصول على نسخة من البيانات، والتصحيح، والمحو، وتقييد المعالجة، والاعتراض، وسحب الموافقة. وينبغي أن يتضمن هذا الإطار تحديد جهة اتصال واضحة داخل كل كيان خاضع للقانون لتلقي الطلبات، سواء كان ذلك مسؤول حماية البيانات أو وحدة محددة لخدمة العملاء، مع إلزام الجهات بتوفير قناة إلكترونية عندما تكون المعالجة أو الخدمة رقمية، ووضع نموذج موحد للطلبات يمكن استخدامه ورقيًا أو إلكترونيًا.

كما ينبغي ضبط مهلة زمنية معقولة للرد على الطلبات، وإقرار أثر قانوني لعدم الرد خلال المهلة باعتباره مخالفة تستوجب تدخل المركز وإعمال صلاحياته الرقابية. وفي السياق ذاته، يُوصى بأن يُلزم المركز المتحكمين والمعالِجين بأن يكون سحب الموافقة بنفس سهولة إعطائها، وأن يُتاح عبر وسيلة بسيطة ومباشرة إذا كانت الموافقة قد مُنحت إلكترونيًا، مع تحديد فترة زمنية قصيرة لتنفيذ السحب ووقف المعالجة أو محو البيانات المرتبطة بها بحسب الأحوال، وإخطار صاحب البيانات بإتمام الإجراء بما يضمن إمكانية التحقق.

ويرتبط بفعالية الحقوق ضرورة تقليل العبء المالي الواقع على الأفراد عند ممارستها. لذلك يُوصى بأن يستخدم المركز صلاحياته في تحديد مقابل الخدمات المرتبطة بممارسة الحقوق باتجاه جعل القاعدة هي الإعفاء أو المقابل الرمزي شديد الانخفاض في الطلبات الروتينية، بحيث لا يتحول المقابل المالي إلى عائق فعلي أمام النفاذ إلى الحقوق، وبحيث يُسمح بفرض مقابل معقول فقط في حالات الطلبات المتكررة بصورة تعسفية أو مُفرطة وبما يقتصر على تغطية المصروفات الإدارية في حدودها الدنيا. ويُستحسن أن يصدر المركز معيارًا واضحًا لتعريف الطلبات التعسفية وكيفية التعامل معها، منعًا لتحول الاستثناء إلى قاعدة.

ولمعالجة العوار المركزي المرتبط باتساع بعض الاستثناءات، يُوصى بإصدار قرارات تفسيرية وأدلة إجرائية لتضييق مساحات الغموض قدر الإمكان داخل الإطار القائم، وبخاصة ما يتعلق بالاستثناء الإعلامي وبحدود الاستثناء المرتبط بالأمن القومي. فمن ناحية الاستثناء الإعلامي، يُستحسن أن يصدر المركز دليلًا يوضح نطاقه وحدوده بما يمنع فهمه كإعفاء كامل من متطلبات حماية البيانات، مع التأكيد على الالتزامات المهنية التي تمنع تعسف نشر البيانات أو معالجة بيانات حساسة دون مقتضى.

ومن ناحية الاستثناء المرتبط بالأمن القومي، تُوصى صياغة بروتوكول تعاون إجرائي مع الجهات المختصة يحدد شكل الطلبات التي

تتعلق بتعديل أو محو أو عدم إظهار البيانات، وأن تكون هذه الطلبات مكتوبة ومسببة ومؤرخة وتخضع لحد أدنى من التوثيق داخل الجهة المتلقية، مع إنشاء سجل داخلي مُؤمّن لتوثيق هذه الطلبات وتكييفها، وبما يحد من السيولة التطبيقية ويُيسّر المساءلة اللاحقة دون إفشاء معلومات قد تكون حساسة.

وفي سياق الشفافية وصحة الموافقة المستنيرة، يُوصى بأن يُصدر مركز حماية البيانات الشخصية معايير مُلزمة لصياغة طلبات الموافقة وآليات الإخطار عند جمع البيانات، مع تحديد حد أدنى إلزامي لمحتوى الإخطار، بما يمنع ترك هذه المسألة لممارسات متباينة بين الجهات. وتُشجّع هذه المعايير نموذج الإشعار متعدد الطبقات عبر إشعارٍ مختصرٍ وواضح وقت الجمع يبيّن -كحد أدنى- الغرض من المعالجة، ومدة الاحتفاظ، والحقوق الأساسية لصاحب البيانات، وآلية سحب الموافقة، مع إتاحة سياسة تفصيلية لمن يرغب في الاطلاع على معلومات أوسع.

كما ينبغي أن تتضمن المعايير حظرًا صريحًا لإدماج الموافقة داخل نصوص مطوّلة غير مفهومة أو صيغ عامة مُلتبسة، وكذلك حظر ربط الموافقة بشرط واحد غير قابل للتجزئة عند تعدد الأغراض، بما يصون معنى الموافقة الحرة والمحددة والمستنيرة في التطبيق.

ويمكن إسناد هذه المعايير إلى مرجعيات دولية راسخة؛ إذ تُعرّف اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) الموافقة بأنها موافقة حرة ومحددة ومستنيرة وغير ملتبسة، لا تُفترض ولا تُستنتج ضمنيًا، بل يجب أن يُعبِّر عنها صاحب البيانات صراحةً إمّا عبر بيان مباشر (مثل كتابة «أوافق» أو توقيع نموذج واضح)، أو عبر فعل إيجابي واضح يدل على الاختيار (مثل الضغط على زر «أوافق» أو وضع علامة في مربع غير مُحدد مسبقًا)

كما تضيف اللائحة العامة لحماية البيانات في الاتحاد الأوروبي قاعدة مهمة لحماية الناس من الموافقة غير المستنيرة، إذا جاء طلب الموافقة داخل مستند يتضمن أمورًا أخرى (مثل شروط الاستخدام أو العقد)، فيجب أن تُعرض الموافقة كقسم مستقل وواضح ومميّز عن بقية النص، بحيث يستطيع الشخص أن يراها ويفهمها ويوافق عليها تحديدًا، بدل أن تُخفى داخل فقرات طويلة أو صياغات عامة. كما تؤكد اللائحة أن الصمت، أو ترك مربع الموافقة كما هو، أو عدم القيام بأي فعل لا يُعد موافقة أصلًا، لأن الموافقة لا تُفترض بل يجب أن تُثبت بفعل إيجابي واضح .

ومن زاوية قابليّة الإنفاذ والرقابة، يُوصى باستكمال التنظيم الإجرائي لممارسة الحقوق بإلزام كل متحكم ومعالج بإمساك سجل داخلي مُؤمّن لطلبات أصحاب البيانات، يُثبت تاريخ الطلب ونوعه وملخص التعامل معه وقرار القبول أو الرفض وأسباب الرفض والمدة الزمنية للاستجابة، بحيث يكون هذا السجل قابلًا للتفتيش ويُسهم في منع الإنكار أو التلاعب في مسارات الطلبات، ويُحول الحقوق إلى التزامات قابلة للقياس والمساءلة.

وفي ملف خروقات البيانات، يُوصى بأن يطور المركز نموذجًا موحدًا للإبلاغ عن الخرق يحدد الحد الأدنى من البيانات التي يجب تضمينها، وأن يصدر دليلًا لتقييم خطورة الخرق وتحديد الحالات التي يقتضي فيها إخطار الشخص المعني وكيفية صياغة الإخطار، بما يضمن قدرًا معقولًا من الاتساق والجودة في البلاغات ويحسن قدرة المركز على التعامل معها. ويرتبط بذلك ضرورة وضع معيار إجرائي يحد من الغموض عند توصيف خرق بأنه يمس الأمن القومي، عبر تحديد الحد الأدنى من عناصر التسبيب والتوثيق المطلوب توافرها داخل الجهة القائمة بالإبلاغ.

كذلك ينبغي أن يعتمد المركز، في قراراته التنظيمية، منهجًا قائمًا على تقييم المخاطر في تشغيل المنظومة، بحيث تتدرج متطلبات التدخل والرقابة والمستندات المطلوبة بحسب حساسية البيانات وحجمها وطبيعة المعالجة ومستوى المخاطر المتوقع على الأفراد، بدلًا

من أن تؤدي القواعد الحالية إلى معاملة المعالجات البسيطة والمعالجات عالية المخاطر بمنطق متقارب. ويمكن أن يظهر هذا المنهج في تصنيف الطلبات، وفي أولويات التفتيش، وفي تحديد ما يستلزم اشتراطات إضافية، بما يدعم كفاءة الإنفاذ ويحقق التناسب.

2. الذكاء الاصطناعي وتدريب النماذج على البيانات الشخصية

يُوصى بأن يُصدر مركز حماية البيانات الشخصية دليلًا إرشاديًا/مدونة إرشادات مُتخصصة لتنظيم استخدام البيانات الشخصية في تطوير وتدريب نماذج الذكاء الاصطناعي والتقنيات الناشئة، بما يحوّل الالتزام العام الوارد في اللائحة التنفيذية (مثل مبدأ عدم الإضرار) إلى معايير تشغيلية محددة، قابلة للتحقق، والتدقيق، والمساءلة. على أن يتضمن الدليل -كحد أدنى- متطلبات واضحة بشأن:

1. ضبط نطاق البيانات المستخدمة وربطها على نحو صارم بالغرض المُعلن من التدريب، مع حظر أو تقييد أي توسّع غير مبرر في جمع البيانات أو استخدامها.
2. قواعد محددة لإعادة استخدام البيانات في تدريب نماذج جديدة أو تحديث نماذج قائمة، ومعايير تقييم مشروعية إعادة الاستخدام وحدوده.
3. معايير للإفصاح والإخطار عند استخدام البيانات الشخصية في بناء/تدريب النماذج، بما يشمل طبيعة الاستخدام، وأهدافه، ونطاقه، ومصادر البيانات، وفئات المتأثرين قدر الإمكان.
4. آليات عملية لتمكين حقوق مثل الاعتراض، وسحب الموافقة، والمحو، مع توضيح الحدود التقنية والقانونية لهذه الحقوق في حالات بعينها وكيفية التعامل معها.
5. تحديد الحالات التي يلزم فيها إجراء تقييم أثر (Data Protection Impact Assessment) قبل التدريب أو النشر، ومعايير تقدير مستوى المخاطر.
6. تحديد إجراءات تخفيف (Mitigating Measures) واجبة عند الاعتماد على المصلحة المشروعة أو أي أساس قانوني آخر، بما يشمل ضوابط تقليل المخاطر، واختبارات الضرورة والتناسب، والتدابير التقنية والتنظيمية.
7. منهجية لتقييم ما إذا كانت مخرجات التدريب (أو النموذج ذاته) قد أصبحت مُجهّلة/مُعمّاة على نحو يمنع استخراج بيانات شخصية أو إعادة التعرّف على الأفراد، وما يترتب على عدم تحقق ذلك.
8. توضيح الآثار المترتبة على تدريب نموذج ببيانات جُمعت أو عولجت بشكل غير مشروع، وما يلزم من إجراءات تصحيحية ومسارات امتثال ومسؤوليات.

كما ينبغي أن يتجاوز الدليل مفهوم الضرر الفردي المباشر إلى إدراج اعتبارات الضرر المجتمعي (مثل التمييز، والإقصاء، والوصم، وآثار التصنيف أو التنبؤ على جماعات بعينها)، بما يضمن موازنةً عملية بين حقوق صاحب البيانات ومصالحه من جهة، وبين المصالح والحقوق الجمعية للمجتمعات المتأثرة بمخرجات النماذج من جهة أخرى، خصوصًا في القطاعات عالية الحساسية مثل الخدمات العامة الرقمية، والائتمان، والتوظيف، والتعليم، والصحة، والأمن.

ويمكن الاستناد في بناء هذا الدليل إلى الاتجاهات الدولية التي تؤكد أن مبادئ حماية البيانات -مثل تقليل البيانات، وتحديد الغرض، والشفافية، والإدارة القائمة على المخاطر- تشكل أساسًا لذكاء اصطناعي مسؤول، ومن ذلك رأي مجلس حماية البيانات الأوروبي (EDPB) بشأن نماذج الذكاء الاصطناعي وعلاقتها بمبادئ حماية البيانات.

3. مقترحات تشريعية لتعديل قانون حماية البيانات الشخصية

على المستوى التشريعي، يُوصى بإعادة النظر في وضع مركز حماية البيانات بهدف تحقيق استقلالية حقيقية تعزز الثقة في قراراته وتحد من تضارب المصالح، وذلك عبر تعديل النصوص المنظمة لتبعيته وتشكيله على نحو يفصل المركز عن التبعية المباشرة للوزير المختص، ويضمن ولاية محددة لرئيسه لا تكون قابلة للعزل التعسفي، ويعيد توازن تشكيل مجلس الإدارة بحيث لا تهيمن عليه الجهات الخاضعة للتنظيم أو الجهات ذات المصلحة، مع تضمين خبرات قانونية وتقنية مستقلة وتمثيل أكثر توازنًا يضمن الحياد المؤسسي.

وتستدعي الإشكاليات المتعلقة بنطاق التطبيق إعادة النظر في الاستثناءات الموسّعة، وبخاصة الاستثناء المرتبط بالأمن القومي والاستثناء الخاص بالبنك المركزي والجهات الخاضعة له. ويُوصى بتعديل الصياغات التي تُبقي المعيار عامًا وفضفاضًا، وحصر الاستثناء في نطاق محدد وضروري ومُعرّف، مع إضافة ضمانات إجرائية ورقابية تمنع تحول الاستثناء إلى باب لإعفاءات شاملة أو أوامر غير قابلة للمراجعة.

وفيما يتعلق باستثناء البنك المركزي، يُفضل إنهاء الاستثناء الشامل وإخضاع القطاع المالي لإطار حماية البيانات العام مع إقرار آلية تنسيق مؤسسية بين المركز والجهة القطاعية لتفادي التعارض، لأن البيانات المالية شديدة الحساسية ولا يقل احتياجها للضمانات العامة عن غيرها من فئات البيانات.

ويمكن إسناد هذا التوجه إلى مرجعيات دولية؛ إذ تسمح اللائحة العامة لحماية البيانات في الاتحاد الأوروبي بفرض قيود/استثناءات على بعض الالتزامات والحقوق فقط عبر تدبير تشريعي، وبشرط أن تحترم جوهر الحقوق والحريات وأن تكون القيود ضرورية ومتناسبة في مجتمع ديمقراطي لتحقيق أغراض محددة (مثل الأمن القومي أو المصالح الاقتصادية/المالية الجوهرية). وتُلزم اللائحة بأن تتضمن التدابير التشريعية التي تقرر الاستثناءات ضوابط محددة تشمل غرض المعالجة أو فئاتها، فئات البيانات المعنية، نطاق القيد، الضمانات لمنع إساءة الاستخدام أو الوصول/النقل غير المشروع، تحديد الجهة المتحكمة أو فئاتها، مدد الاحتفاظ وضماناتها، تقييم المخاطر على حقوق الأفراد، وحق إبلاغ صاحب البيانات بوجود القيد ما لم يضر ذلك بغرضه.

وبالإضافة إلى المرجعيات التنظيمية المقارنة، يمكن تأسيس هذا التوجه على إطار حقوقي دولي أوسع؛ إذ يقرر العهد الدولي للحقوق المدنية والسياسية في المادة 17 الحق في الخصوصية ويحظر أي تدخل تعسفي أو غير قانوني. وقد دأبت آليات حقوق الإنسان بالأمم المتحدة على تفسير هذين الوصفين باعتبارهما يحيلان إلى مبادئ الشرعية والضرورة والتناسب، بما يعني أن أي تقييد يجب أن يكون منصوصًا عليه في القانون، وأن يحدد القانون بوضوح وتفصيل ظروف التدخل وحدوده وضماناته، وأن يخدم غرضًا مشروعًا، وأن يكون أقل الوسائل تدخّلًا ومتناسبًا مع الهدف، وألا يجرّد جوهر الحق في الخصوصية من معناه.

وفي باب العقوبات في القانون، تُوصى مراجعة التناسب بين العقوبات المقررة للأفعال الجسيمة وبين العقوبات المقررة لمخالفات إجرائية، بحيث تُبقى على العقوبات المُغلّظة على الانتهاكات المتعمدة التي تمس جوهر حماية الخصوصية، مثل الاتجار بالبيانات أو تسريبها عمدًا، في حين يُوصى أن يُتعامل مع المخالفات الإدارية والتنظيمية ذات الطبيعة القابلة للتصويب بأدوات تدريجية أقرب إلى الجزاءات الإدارية أو الغرامات التصاعدية بدلًا من توسيع نطاق التجريم الجنائي لأخطاء إجرائية. ويُسهم ذلك في تحقيق عدالة جنائية أوضح، ويعزز فعالية الإنفاذ عبر توجيه الردع إلى مناطق الخطر الحقيقي.

وبالتوازي، يُوصى بتعزيز حق الأفراد في التعويض وجبر الضرر بنص تشريعي أكثر صراحة يقرر حق المتضرر في تعويض عادل عن الضرر المادي أو المعنوي الناتج عن مخالفة قواعد حماية البيانات، بما يقوي مركز الأفراد أمام المحاكم ويخلق حافزًا حقيقيًا للامتثال، ويساعد على تطوير اجتهاد قضائي يُرسخ المعايير الحقوقية لحماية البيانات.

3. تحسينات تنظيمية وتقنية لتعزيز التطبيق وبناء القدرات والشفافية

يُوصى بتطوير منصة إلكترونية موحدة للتعاملات مع مركز حماية البيانات تتيح تقديم طلبات التراخيص والتصاريح وشهادات الاعتماد وتتبعها، وقيد مسؤولي حماية البيانات وإدارة سجلاتهم، وتلقي شكاوى الأفراد والرد عليها وتوثيقها، وتمكين الأفراد من تقديم طلبات ممارسة الحقوق بصورة إلكترونية موثقة عند الاقتضاء مع ضمان أمن المنصة وسهولة استخدامها. وتُعد هذه المنصة أداة لتقليل الاحتكاك البيروقراطي وتوحيد الإجراءات وتوثيقها، وينبغي أن تتضمن محتوى توعويًا مبسطًا للجمهور يشرح الحقوق وآليات الشكوى، ومحتوى إرشاديًا للشركات والجهات يوضح خطوات الامتثال ومتطلباته.

ويُوصى كذلك بتفعيل الدور التوعوي والتدريبي للمركز على نحو منتظم ومؤسسي، من خلال وضع خطة سنوية معلنة للتوعية والتدريب تستهدف مسؤولي حماية البيانات والعاملين على المعالجة من جهة، والجمهور العام من جهة أخرى، مع تطوير مواد إرشادية ونماذج مبسطة قابلة للاستخدام، مثل صيغ موافقة واضحة، وإرشادات لسحب الموافقة، وسياسات خصوصية نموذجية، وآليات التعامل مع طلبات الوصول والمحو. كما يُستحسن ربط الاعتماد وتجديده للمسؤولين والمستشارين بساعات تدريب دورية معتمدة لضمان بناء خبرة تراكمية لا تقتصر على الاختبار الأولي.

وفي سياق تعزيز الثقة والشفافية، يُوصى باعتماد سياسة نشر منهجية لقرارات المركز الجوهرية في صورة منقحة لا تكشف بيانات شخصية، مع نشر إحصاءات دورية عن طبيعة الشكاوى ونتائجها، وأنماط المخالفات، وإجراءات التفتيش، بما يمنح الجمهور والباحثين والمؤسسات التشريعية أدوات متابعة موضوعية ويحد من مخاطر الانتقائية في الإنفاذ. ويرتبط بذلك ضرورة وضع إطار واضح للتقرير السنوي عن حالة حماية البيانات، من حيث موعد إصداره، وحده الأدنى من محتواه، وآلية نشره وإتاحته، بحيث يصبح التقرير أداة مساءلة عامة ومؤشرًا حقيقيًا على أداء المنظومة.

وأخيرًا، يُوصى بتعزيز البنية التحتية التقنية لأمن البيانات، عبر توظيف الموارد المتاحة لتطوير أدوات رقابية وتقييمية تساعد المركز على أداء مهامه بكفاءة، بما في ذلك تطوير قدرات فحص أمن نظم المعلومات لدى الجهات عالية المخاطر، وتشجيع تبني التشفير القوي للبيانات المخزنة والمنقولة، ورفع جودة الامتثال التقني عبر إرشادات ومعايير فنية قابلة للتحقق. ويمكن أن يُستكمل ذلك بتطوير آليات رصد مبكر للخروقات والتسريبات بالتنسيق مع الجهات المعنية، بما يدعم الانتقال من إنفاذ لاحق إلى وقاية استباقية تقلل الضرر على أصحاب البيانات.

خاتمة

اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري هي امتدادٍ إجرائي لقانون حماية البيانات الشخصية، يتحدد من خلالها المعنى العملي للحق في الخصوصية داخل المجال الرقمي. ومن ثمّ فإن قيمة اللائحة تُقاس بقدرتها على تحويل الالتزامات العامة إلى قواعد تشغيلية قابلة للقياس والمساءلة، وبمدى ما تُتيحه من حماية فعلية تُقلّص فجوة القوة بين صاحب البيانات والجهات القادرة على جمعها وتحليلها وتداولها.

وتُظهر القراءة الأولى للائحة - مرحلة ما قبل النفاذ الفعلي - أن مشكلات الحماية لا تنشأ فقط من غياب المبادئ، بل كثيرًا ما تتولد من تصميم الإجراءات ذاتها، مثل طريقة تعريف الموافقة وآليات تحققها، ومن سهولة سحبها، ومن الكلفة الزمنية والمالية لممارسة الحقوق، ومن اتساع الاستثناءات أو سيولتها، ومن الاعتماد المفرط على الإذن المسبق بوصفه مدخلًا وحيدًا للضبط. في هذا المستوى تحديدًا تتحدد قابلية الحق للإنفاذ؛ لأن الحقوق التي تظل بلا مسارات واضحة ومواعيد ملزمة وسجلات قابلة للتفتيش تتحول إلى وعدٍ قانوني لا يملك صاحبه أدوات تشغيله.

وبالمثل، فإن التنظيم الذي يُثقل الامتثال بإجراءات ترخيص عامة دون منهج قائم على المخاطر يفتح الباب لامتثالٍ شكلي ينجز الأوراق ولا يضمن الحماية، ويُحمّل الفاعلين الأصغر كلفة لا تتناسب مع طبيعة معالجتهم، ويُربك في الوقت نفسه قدرة الجهة التنظيمية على إنفاذ متسق وعادل.

كما أن بنية الحوكمة التي تتمركز فيها أدوات التنظيم والرقابة والإنفاذ داخل جهة واحدة تجعل ضمانات الاستقلال والشفافية جزءًا لا ينفصل عن جوهر الحماية. فالمعيار الحقوقي لا يقتصر على وجود سلطة رقابية قوية فقط، بل يمتد إلى شروط ممارسة هذه السلطة مثل وضوح القواعد، ومعلومية المعايير، وإتاحة المعلومات العامة الضرورية لتقييم الأداء، وإمكانية مساءلة القرارات والطعن عليها بصورة فعّالة. وعندما تغيب الأطر المنظمة للتقارير الدورية والشفافية المؤسسية والتواصل المجتمعي، تتراجع قدرة المنظومة على بناء ثقة عامة مستقرة، وتضعف إمكانية تتبع اتجاهات الانتهاكات وقياس الامتثال، وتصبح الممارسة أقرب إلى إدارة بيروقراطية لملفٍ حساس بدلًا من كونها نظامًا للحماية قائمًا على اليقين القانوني.

وتتضاعف أهمية هذه الاعتبارات مع توسع استخدام البيانات في التقنيات الناشئة والذكاء الاصطناعي، حيث لم تعد المخاطر محصورة في التسريب أو الاختراق، بل تشمل أيضًا إعادة الاستخدام واسع النطاق، والتصنيف، واتخاذ القرارات المؤتمتة، وما قد يترتب عليها من أضرار مباشرة أو غير مباشرة. ولذلك فإن تطوير معايير تشغيلية أكثر تحديدًا في هذا المجال، وربطها بمنهج واضح لإدارة المخاطر وتقييم الأثر، يمثل شرطًا لازمًا لتجنب اتساع الفجوة بين سرعة التحول التقني وبطء الضمانات التنظيمية.

وبناءً على ذلك، فإن مسار تطوير المنظومة الحمائية للحق في الخصوصية يتطلب التعامل مع اللائحة باعتبارها إطارًا حيًا قابلًا للتقويم والتحسين. والتأكيد على أن تعزيز الحماية لا يتحقق بزيادة القيود المجردة، بل بتحسين جودة القواعد الإجرائية وتوحيدها وتبسيطها حيث يلزم، وبجعل ممارسة الحقوق ممكنة ومنخفضة الكلفة ومُتحقَّقة في الواقع.