دكتور/ أحمد عبد العزيز محمد أبو الحسن
باحث بمركز أبحاث القانون والتكنولوجيا الناشئة

دراسة نقدية للائحة التنفيذية لقانون حماية البيانات الشخصية المصري: مشروعية التنظيم وكفاءته الوظيفية

المراسلة: د.أحمد عبد العزيز محمد أبو الحسن
باحث بمركز أبحاث القانون والتكنولوجيا الناشئة

معرف الوثيقة الرقمي (DOI): jolets.v6i1.253/10.54873

البريد الإلكتروني: Ahmed.aboualhassan@bue.edu.eg

نسق توثيق البحث أحمد عبد العزيز محمد أبو الحسن
دراسة نقدية للائحة التنفيذية لقانون حماية البيانات الشخصية المصري: مشروعية التنظيم وكفاءته الوظيفية

الملخص:

تناولت هذه الدراسة بالتحليل والنقد اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الصادرة بقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ٨١٦ لسنة ٢٠٢٥. وهذا على عدة محاور؛ بداية بدراسة أثر الفجوة الزمنية بين القانون وإصدار اللائحة وأثر القانون على اللائحة، مروراً بتحليل الاتساق والكفاية بين القانون واللائحة والاتساق الداخلي للائحة، وانتهاء بتقييم أثرها على الاقتصاد والتقنية

اعتمدت الدراسة المنهج التحليلي النقدي لتقييم مشروعية واتساق اللائحة ومدى التزامها بحدود التفويض التشريعي. وقد كشف التحليل عن وجود عوار منهجي وعدم اتساق بين اللائحة والقانون نتيجة اعتماد اللائحة على هيكلية تقتصر على الإحالات المباشرة الموجودة في القانون دون اعتبار الارتباطات الموضوعية داخل اللائحة، وتوسعها في صلاحيات المركز بما يتجاوز حدود الاختصاص التشريعي والإحالات، كما اعتمدت في بعض اجزاءها على المنهج المقارن لتقييم التوافقية التشريعية مع النظم القانونية والفنية والاقتصادية الحاكمة لحركة اقتصاد البيانات، وكشفت الدراسة عن تمايز الاتجاه المصري لحماية البيانات الشخصية عن عينات المقارنة

كما ناقشت الدراسة الأثر الاقتصادي والتقني للائحة، مبرزةً التحديات التي تفرضها منظومة التراخيص والرسوم والعقوبات وواحدية البينة التقنية والفنية المبنية عليها اللائحة، ومدى تصادم هذه البنية مع أسس التقنيات الحديثة والأعمال

خلصت الدراسة إلى أن استمرار اللائحة بصيغتها الحالية قد يؤدي إلى حالة من التعارض التشريعي، ويطرح إشكاليات متعددة تتعلق بمشروعية العديد من مواد اللائحة من عدمها، مما يؤدي إلى صعوبة الامتثال وزيادة النزاعات الناشئة عن الاختلافات بين القانون واللائحة

وانتهت الدراسة بتقديم حزمة من التوصيات التشريعية لتقويم مسار اللائحة، أبرزها ضرورة تبني مبدأ «الخصوصية بالتصميم»، وتخفيف أعباء الامتثال للشركات الناشئة والمهنيين، وتفعيل كافة أسباب المشروعية القانونية لضمان توازن دقيق بين حماية الحقوق الأساسية ومتطلبات الاستثمار في الاقتصاد الرقمي، وإلغاء كافة التوسعات اللائحية المخالفة لنص القانون ومن أهمها غرامات مخالفة شروط التراخيص وصلاحيات المركز المتوسعة

الكلمات المفتاحية: حماية البيانات الشخصية، اللائحة التنفيذية، المشروعية، الاقتصاد الرقمي، التراخيص، مسئول حماية البيانات، الحوسبة السحابية، الذكاء الاصطناعي.

Abstract:

This study provides a critical and analytical examination of the Executive Regulations of the Egyptian Personal Data Protection Law (Law No. 151 of 2020), promulgated by the Minister of Communications and Information Technology Decree No. 816 of 2025. The analysis spans several axes: initially exploring the implications of the temporal gap between the enactment of the Law and the issuance of its Regulations, along with the Law's impact on the latter; proceeding to evaluate the consistency and adequacy between the Law and the Regulations, as well as the internal consistency of the Regulations themselves; and concluding with an assessment of their economic and technological impacts.

Methodologically, the study adopts a critical analytical approach to evaluate the legality and coherence of the Regulations, specifically scrutinizing their adherence to the boundaries of legislative delegation. The analysis reveals a methodological defect and a fundamental inconsistency between the Regulations and the Law. This stems from the Regulations' reliance on a structural framework confined to the direct cross-references explicitly stated in the Law, while disregarding substantive interconnections. Furthermore, the Regulations unlawfully expand the powers of the Center beyond the permissible scope of legislative jurisdiction and delegated authority. In certain sections, the study also employs a comparative methodology to assess legislative harmonization with the legal, technical, and economic frameworks governing the global data economy, ultimately highlighting the distinct divergence of the Egyptian approach from the comparative models.

Furthermore, the research discusses the economic and technological implications of the Regulations, highlighting the challenges imposed by the overarching regime of licenses, fees, and penalties. It critiques the monolithic technical and operational architecture underlying the Regulations, demonstrating its friction with the fundamental dynamics of modern technologies and agile business models.

The study concludes that the persistence of the Regulations in their current iteration threatens to entrench a state of legislative dissonance. It raises significant concerns regarding the legality of numerous regulatory provisions, thereby complicating compliance efforts and inevitably increasing disputes arising from the contradictions between the primary Law and its Executive Regulations.

Finally, the study proposes a comprehensive set of legislative recommendations to rectify the trajectory of the Regulations. Prominent among these are the necessity of adopting the "Privacy by Design" principle, mitigating compliance burdens for startups and professionals, and activating all lawful bases for processing to ensure a delicate balance between safeguarding fundamental rights and fostering investment in the digital economy. Furthermore, it advocates for the nullification of all regulatory overreaches that contradict the statutory text, most notably the administrative fines for license breaches and the unlawfully expanded powers of the Center.

Keywords: Personal Data Protection, Executive Regulations, Legality, Digital Economy, Licensing, Data Protection Officer (DPO), Cloud Computing, Artificial Intelligence (AI).

مقدمة الدراسة

أ: عن اللائحة:

بعد ترقب دام لأكثر من خمس سنوات، صدرت اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة 2020، بموجب قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 816 لسنة 2025. ويأتي هذا الإصدار متجاوزاً الموعد التنظيمي الذي حدده المشرع في المادة الرابعة من القانون، والتي ألزمت بإصدار اللائحة خلال ستة أشهر من تاريخ العمل به؛ وهو ما يضفي أهمية خاصة لهذه الدراسة النقدية، لا سيما في ظل التطورات التقنية والتشريعية المتسارعة التي تخللت الفترة ما بين صدور القانون ولائحته

وتكتسب هذه اللائحة أهمية استثنائية، كونها الأداة اللازمة لتفعيل نصوص القانون الذي ظل معلقاً في حيز التنفيذ لسنوات. ونتاج لهذا ظلت حالة عدم اليقين والاستقرار التشريعي ملازمة للعديد من القطاعات في مصر بشكل مباشر وجميع القطاعات بشكل غير مباشر وهذا يرجع لامتداد الأثر التشريعي والعملي لهذا القانون لما وراء حماية البيانات الشخصية، بل ليرسم ملامح البنية التحتية القانونية لأي تحول رقمي حديث في الدولة، مؤسساً بذلك للتوازن الدقيق بين حقوق الأفراد في حماية بياناتهم، وبين اعتبارات المصلحة العامة، ومقتضيات الأمن القومي، ومتطلبات الاستثمار الوطني والأجنبي

كما أن القواعد الناظمة لحماية البيانات الشخصية اليوم لا تنفصل عن حركة الاقتصاد الرقمي الحديث؛ بل أضحت من أهم المؤثرات القانونية على مناخ الاستثمار الرقمي، وعلى قدرة الدول النامية - كمصر - في توظيف إمكاناتها الجغرافية والبشرية لتكون مركزاً إقليمياً لحركة البيانات والصناعات الخدمية، وعلى رأسها صناعات التعهيد ومراكز البيانات. ولا يقف هذا الأثر عند الحدود الوطنية، بل يمتد ليحدد قدرة الدولة ومستثمريها على النفاذ للأسواق العالمية وجذب رؤوس الأموال الأجنبية؛ فقوانين البيانات الشخصية تعتبر اليوم "المرجعية التشريعية" لحركة انسياب البيانات عبر الحدود، والتي تعد ركيزة لأي نشاط بشري حديث، سواء كان استثمارياً، أو بحثياً، أو حتى تواصلاً اجتماعياً

ب: سياق الدراسة:

لا تمثل هذه الدراسة جهداً بحثياً منعزلاً، بل تأتي استكمالاً للمسار البحثي الذي اختطه «مركز أبحاث القانون والتكنولوجيا الناشئة (CLETS)" بكلية القانون بالجامعة البريطانية بمصر منذ صدور القانون رقم ١٥١ لسنة ٢٠٢٠. وتستند هذه الورقة إلى التراكم المعرفي الذي حققه المركز عبر سلسلة من الإصدارات والجهود الأكاديمية المحلية والناقدة للقانون

وقد تجلى هذا المسار بوضوح بدءاً من إصدار المركز لدراسته النقدية الأولى للقانون فور صدوره - والتي عُدت حينها باكورة الإنتاج العلمي المتخصص في قوانين حماية البيانات الشخصية بمصر - مروراً بإفراد مساحات واسعة للأبحاث المتخصصة في مجلة "القانون والتكنولوجيا الناشئة" وهي المجلة التابعة للمركز ولكلية القانون بالجامعة البريطانية بمصر والتي تختص بنشر الأبحاث القانونية والأكاديمية المحكمة عن تقاطعات القانون والتكنولوجيا الناشئة، وإصدار «القاموس العصري لمصطلحات قانون حماية البيانات الشخصية» كتجربة فريدة للتحليل متقاطع التخصصات لإرساء أسس ونظم التعريفات والإصلاح المستجد التكنوقانوني بشكل مؤسسي وأكاديمي عبر تعاون مع كلية دار العلوم بالقاهرة ومجمع اللغة العربية، وصولاً إلى المؤتمر الدولي الثالث للكلية الذي خصص محاور أساسية لقضايا البيانات الشخصية.

وقد تُوجت هذه الجهود بتنظيم الكلية لورشة عمل متخصصة بالتعاون مع هيئة قضايا الدولة، تحت عنوان: "**قانون حماية البيانات الشخصية ولائحته التنفيذية: الإطار القانوني وآليات التطبيق**"، والتي عقدت في 12 فبراير 2026، بإشراف عميد الكلية **أ.د. إبراهيم سلامة**، وقيادة وكيل الكلية للدراسات العليا والبحوث **أ.د. سامي واصل**.

وعليه، تأتي هذه الدراسة كتتمة لازمة وحجر أساس جديد لاستكمال هذا المسار الأكاديمي، وإيذاناً

بـانطلاق أحد أهم وأكبر الأحداث العلميـة للكليـة؛ وهو مؤتمرهـا الدولـي القـادم بـعنوان: (**الذكاء الاصطناعـي وحـقوق الإنسـان**)، والذي ستشكل دراسـات حمايـة البيانـات الشخصيـة فـي عصر الذكاء الاصطناعـي أحد أهم محـاوره الأسـاسية.

ج: منهجية الدراسة ومحاورها:

تسعى هذه الدراسة إلى تحليل اللائحة التنفيذية وتقييمها نقدياً من خلال المحاور التالية:

- **إشكاليات الفجوة الزمنيـة والفـراغ التنظيمـي:** تحليـل تداعيـات تأخـر صـدور اللائحـة لأكثـر مـن خمـس سـنوات علـى مـدى اتسـاق المنظومـة التشـريعية مـع التغيـرات الجذريـة الحادثـة فـي مجـال حمايـة البيانـات (تقنيـاً وتشـريعياً). وكذلـك دراسـة أثـر الإحـالات المتعـددة والمبنـي علـى طبقتيـن أولهمـا الاحـالات التشـريعية للائحـة ثـم احـالات اللائحـة لقـرارات إداريـة مسـتقبلية علـى 'الكفايـة التنفيذيـة' الحاليـة للائحـة، وتداعيـات ذلـك علـى مبـادئ الشـفافية والأمـن والاسـتقرار القانونـي.
- **اسـتنباط وتحليـل الفلسـفة العامـة:** قـراءة التوجهـات التشـريعية التـي تبنتهـا اللائحـة فـي تنظيـم الحقـوق والالتزامـات، ومـدى مواءمتهـا لفلسـفة القانـون الأصليـة.
- **التقييـم الفنـي والموضوعـي:** قيـاس مـدى اتسـاق اللائحـة مـع القواعـد المسـتقرة والمبـادئ الأكثـر شـيوعاًفـي مجـال حمايـة البيانـات (مثـل مبـدأ تقليـل البيانـات، والخصوصيـة بالتصميـم).
- **اختبـار التوافقيـة (Compatibility):** بحـث مـدى التـزام اللائحـة بالحـدود التـي رسـمها القانـون، وهـل التزمـت بالإحـالات الحصريـة أم توسـعت فـي خلـق مراكـز قانونيـة جديـدة؟ فضـلاً عـن فحـص الاتسـاق الداخلـي بيـن نصوصهـا الإجرائيـة والموضوعيـة.
- **الأثـر الحقوقـي:** قيـاس أثـر اللائحـة علـى حقـوق الأفـراد، ومـدى تحقيقهـا للمقاصـد الدسـتورية والقانونيـة للمشـرع فيمـا يتعلـق بحرمـة الحيـاة الخاصـة وحمايـة البيانـات.
- **تقييـم التـوازن التشـريعي:** قيـاس مـدى مراعـاة اللائحـة لمعاييـر التـوازن بيـن الأسـس الحقوقيـة مـن جهـة، والحتميـات العمليـة والمصالـح الاسـتثمارية والضـرورات العامـة مـن جهـة أخـرى.
- **اختبـار القابليـة للتحقيـق والأثـر الاقتصـادي:** قيـاس «الجـدوى التطبيقيـة» لنصـوص اللائحـة، وهـل تـؤدي المغـالاة فـي الاشـتراطات الفنيـة إلـى خلـق حالـة مـن «الامتثـال المسـتحيل»؟ ومناقشـة أثـر ذلـك علـى صناعـة التعهيـد، ومـدى نجـاح اللائحـة فـي توفيـر «اليقيـن التشـريعي» الـلازم لجـذب الاسـتثمارات الأجنبيـة وتوطيـن التكنولوجيـا.

د: خطة الدراسة:

المبحث التمهيدي: السياق الحاكم للائحة التنفيذية

المطلب الأول: الفجوة الزمنية وتداعياتها على فاعلية التنظيم القانوني.

المطلب الثاني: الانعكاسات التشريعية للقانون على التنظيم اللائحي.

المبحث الأول: التوافق التشريعي للائحة وتحقيق الجاهزية والكفاية

المطلب الأول: الانضباط التشريعي وحدود الاتساق مع القانون.

المطلب الثاني: الكفاية التنظيمية وجاهزية آليات الإنفاذ.

المبحث الثاني: تقييم التوازن اللائحي والأثر الاقتصادي والتقني

المطلب الأول: التقييم الداخلي للنصوص وأثره على بيئة الامتثال والمساءلة.

المطلب الثاني: الكلفة والتكاملية التقنية والاقتصادية للائحة.

وتختتم الدراسة بخاتمة عن الأثر التشريعي وتقديم مقترحات لتحسين النص ورفع كفاءته بناء على المخرجات والنتائج التي ستخرج بها الدراسة

المبحث التمهيدي

السياق الحاكم للائحة التنفيذية

قبل البدء في التحليل المفصل للائحة التنفيذية لقانون حماية البيانات الشخصية المصري، لا يمكن بأي حال من الأحوال تجاهل أكبر عاملين أثرا وسيؤثران عليها، وهما: التأخر الشديد في إصدارها، والانتقادات المكثفة الموجهة لقانونها الحاكم، والتي سيمتد الكثير منها ليؤثر على اللائحة ويحدد مسارها المستقبلي

ولهذا في هذا المبحث التمهيدي، سوف نقوم بإلقاء الضوء على هذين العاملين كوسيلة لتحقيق نوع من القاعدة النقدية والمحايدة لتقييم اللائحة، وهذا في مطلبين كالآتي:

المطلب الأول: الفجوة الزمنية وتداعياتها على فاعلية التنظيم القانوني.

المطلب الثاني: الانعكاسات التشريعية للقانون على التنظيم اللائحي.

المطلب الأول

الفجوة الزمنية وتداعياتها على فاعلية التنظيم القانوني

صدرت اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري بالوقائع المصرية في الأول من نوفمبر ٢٠٢٥، لاحقةً لصدور القانون الأم في ١٥ يوليو ٢٠٢٠؛ لتمثل هذه الفجوة الزمنية — التي تجاوزت الخمس سنوات وتخطت بوضوح المهلة التنظيمية المحددة بستة أشهر في مواد الإصدار — متغيراً جوهرياً يستوجب الدراسة والتحليل. ففي قطاع رقمي يتسم بالديناميكية والتطور اللحظي، يطرح هذا الفاصل الزمني تساؤلات ملحة حول احتمالية تشكل حالة من «الجمود التشريعي» (Legislative Stagnation). ولا تقتصر دلالات هذه الفجوة على البعد الزمني المجرد، بل تتقاطع مع طفرات تقنية غير مسبوقة (أبرزها بزوغ عصر الذكاء الاصطناعي)، وتحولات تشريعية عالمية متسارعة سعت لاحتواء وتنظيم هذا الانفجار التقني المتلاحق

وفي هذا المطلب، سنُخضع هذه الفجوة الزمنية لتقييم تحليلي موضوعي؛ لقياس أثرها الفعلي على بنية القانون ولائحته التنفيذية، واختبار مدى مرونة النص التشريعي وقدرته على استيعاب وملاحقة تلك التغيرات الجذرية، وذلك من خلال محورين دراسيين، كالآتي

أولاً: قياس انعكاسات الطفرات التقنية المستحدثة على مدى فاعلية ومرونة النصوص القانونية واللائحية.

ثانياً: تحليل التطورات التشريعية المقارنة واختبار قدرة النموذج الوطني على استيعابها ومواكبتها

أولا: التغيرات التقنية وأثرها على فاعلية القانون واللائحة:

جاء القانون المصري لحماية البيانات الشخصية 151 لسنة 2020 بإشكالياته المتعلقة بعدم ملاحقته ومواكبته للتطبيقات التقنية المؤثرة على حماية البيانات الشخصية في فترته -وهي ما سنتناوله فيما يتعلق بانعكاس القانون على اللائحة لاحقا-، ولكننا هنا سنقتصر على اثر التطور التقني في الفترة الزمنية التي تزيد عن خمس سنوات بين القانون واللائحة، وأثرها على القانون واللائحة، وهل كان من الأجدى اجراء تغييرات على القانون ذاته ثم اصدار لائحة تنفيذية للقانون المحدث، أم ماذا؟

فالنسبة للتغيرات التقنية فهي عديدة ومؤثرة، بل يمكن القول بأنها مغيرة بشكل جذري للمشهد التقني واستخدامات وقدرات التقنية، مما جعل حتى رواد الاتجاه الموحد Omnibus Model[1] القائم على التنظيم

1 paul M Schwartz, ‹Global Data Privacy: The EU Way› (2019) 94 NYU L Rev 771, 775–80, p: 771, https://www.nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-eu-way/ ,accessed

المسبق Ex-ante Regulation[٢] عالميا المتمثل الاتحاد الأوروبي يطلقون مراجعتهم الشمولية لجميع ما يتعلق بالأسس القانونية لحماية البيانات الشخصية لمواكبة التغيرات التقنية فيما أطلق عليه المفوض الأوروبي digital omnibus[٣]، والذي من ضمن أهدافه تكييف بعض القواعد الأساسية لحماية البيانات الشخصية لتتناسب مع الطفرة التقنية، ولتحسين المؤامة بين القاعدة القانونية والتطور التقني

وقد تمثلت الطفرة التقنية في:

أ: بدء عصر «الذكاء الاصطناعي التوليدي»:

وهو ما كان له انعكاساته البالغة الأثر على التنظيم القانوني لحماية البيانات الشخصية، سواء من حيث بعض المبادئ الأساسية للمعالجة المشروعة للبيانات كمبدأ «تقليل البيانات وتناسبها مع الغرض»، وتكييف مبدأ «مشروعية الغرض» وهل يجوز جمع ومعالجة البيانات الشخصية لأغراض تدريب وتطوير النماذج[٤]، وأيضا مشروعية المخرج الصادر من النموذج كالقرار المؤثر على الشخص المعني بالبيانات أو حتى استعمالها التنميط أو التصنيف الاجتماعي وكذا التوجيه والتلاعب السلوكي مثلا[٥]، وكذا أثرها على ممارسة الحقوق المشروعة للأشخاص المعنية بالبيانات كمثلا «الحق في تقييد المعالجة» وكذا «الحق في المحو»

ب: تطور تقنيات انترنت الأشياء internet of things :

والتي أثرت على أليات جمع البيانات والعلاقة بين المتحكم والشخص المعني، فأفرزت عن جمع مستمر فيزيائي للبيانات الشخصية عن طريق العديد من الأجهزة الذكية المتصلة المزودة بمستشعرات تعمل على مدار الساعة لتلتقط كما هائلا من البيانات تعالج لتقديم الخدمات التي يفترض أن تقدمها تلك الأجهزة، ولكنها أيضا تستعمل في أغراض أكثر خفية مثل التلاعب السلوكي بما يعرف بإنترنت السلوك Internet of behaviors، وهو نتاج الجمع المكثف للبيانات الشخصية من أكثر من مصدر ومعالجتهم عن طريق قواعد علم النفس السلوكي لاستنباط أنماط سلوكية خفية تستخدم للتلاعب بالأفراد[٦]، كما أن هذا التطور أظهر نوعا لم يتكن يحظى بحماية كبيرة من قبل ألا وهو البيانات المستنتجة Inferred Data وهي البيانات التي يتم استنتاجها عن طريق معالجة خاصة للبيانات الشخصية المجمعة[٧].

وأيضا أثرت هذه التقنيات في شكل أنماط العلاقات بين أطراف عملية معالجة البيانات الشخصية فمن ناحية يمكن أن يكون الشخص المعني بالبيانات هو ذاته متحكم في نفس الوقت لبيانات أشخاص آخرين يمكن أن يطلق عليه العابرين في مجال التقاط المستشعر للبيانات الشخصية، كما أن شكل العلاقة نفسه تغير

17 February 2026.

2 Alexandre de Streel and others, ‹The European Proposal for a Digital Markets Act: A First Assessment› (CERRE 2021), p:11, https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/ accessed 17 February 2026.

3 European Commission, Digital Omnibus Regulation Proposal (Shaping Europe’s Digital Future, 19 November 2025) https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal accessed 18 February 2026.

4 Philipp Hacker, Andreas Engel and Marco Mauer, ‹Regulating ChatGPT and Other Large Generative AI Models› (2023) Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, p: 13-15.

5 Michael Veale and Frederik Zuiderveen Borgesius, ‹Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach› (2021) 22 Computer Law & Security Review, https://www.semanticscholar.org/reader/8b165eba2d0b9308682fdc4d775c00d1d3907a59 , accessed: 18\2\2026

6 European Data Protection Supervisor, ‘Internet of behaviours’ (TechSonar) https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/internet-behaviours_en accessed 18 February 2026.

7 Sandra Wachter and Brent Mittelstadt, ‹A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI› (2019) 2019 Columbia Business Law Review 494, p: 24, https://doi.org/10.7916/cblr.v2019i2.3424 accessed 18 February 2026.

من علاقة خطية نتيجة مزود خدمة اومتحكم ومستهلك أو شخص معني بالبيانات إلى مزود خدمة يقوم جهازه بجمع فيزيائي لا رقمي لكمية ضخمة مستمرة من البيانات لكلا من الشخص المعني من المستهلك اوصاحب الجهاز و العابرين بمجال هذا الجهاز مما يجعل العلاقة ذاتها علاقة شبكية أكثر تعقيدا من مجرد سيناريوهات الجمع الذي تتم في البيئة الرقمية

ج: تطور نظم الحوسبة السحابية:

على الرغم من أن نظم الحوسبة السحابية تثير اشكالياتها الخاصة فيما يتعلق بنقل البيانات ومعالجتها عبر الحدود، إلا أن تطورها الحادث في السنين الأخيرة المعروف ب (الحوسبة الحدية edge computing) حيث يتم جمع ومعالجة البيانات في جهاز الشخص المعني بالبيانات ولا يتم نقل إلا النتائج الإحصائية لخوادم المتحكم بما يعرف بالتعلم الفيدرالي والذي يسمح بتدريب نماذج الذكاء الاصطناعي بدون نقل البيانات لخوادم مركزية[8]، أفرز عن تغير شامل في شكل عملية المعالجة ذاتها كونه يصطدم بالافتراض الأساسي لدورة المعالجة للبيانات الشخصية والتي تبدا عادة ب جمع البيانات وتخزينها في خوادم المتحكم

د: تطور وتعاظم الاعتماد على تقنيات البلوك تشين blockchain:

حيث يتم الآن اعتماد تلك التقنية كبنية تقنية أساسية للنموذج الثالث للويب اللامركزي web 3.0، وهو على الرغم من الوعود المستمرة فيما يتعلق بتحسين الخصوصية وحماية البيانات الشخصية، إلا أنها ستحتاج لتغيير المفاهيم الأساسية في قوانين حماية البيانات الشخصية من حيث المراكز القانونية كمفهوم «المتحكم controller" لمشاركة جميع العقد nods في اتخاذ القرار داخل سلسلة الكتل، كما أن سلاسل الكتل أيضا تقوم على أليات تمنع ممارسة بعض الحقوق كمثلا الحق في المحو والتصحيح أيضا حيث أن البيانات المسجلة داخل أو على الشبكة لا يمكن محوها بالطرق التقليدية دون ان يؤدي هذا لانهيار الشبكة بأكملها لأن أليات الربط هاش تعتمد على جزء من بيانات العقدة السابقة والتالية[9].

ولهذا يمكن القول بأن هذه التغيرات التقنية سواء التي بدأت أو تعاظم دورها وأثرها بعد صدور القانون المصري لحماية البيانات الشخصية، تطرح إشكاليات تضرب في أسس النموذج التقليدي لحماية البيانات الشخصية الذي ولد منها هذا القانون، وبالتالي أيضا لائحته التنفيذية.

ثانيا: المتغيرات التشريعية المقارنة منذ فترة نشر القانون حتى نشر اللائحة التنفيذية:

مع تزايد رقمنة القطاعات المختلفة تحولت اللائحة العامة لحماية البيانات الشخصية إلى تشريع أساسي يحال اليه في أكثر من قانون أحدث منه، مما أسفر عنه تخصيصا للقواعد العامة لحماية البيانات الشخصية في كل قطاع، فمثلا يمكن أن نشير إلى بعض السيناريوهات المميزة لتطور قواعد حماية البيانات الشخصية في بعض القطاعات المميزة، والتي يمكن أن نضرب عليها بعض الأمثلة من خلال المنظومة التشريعية الأوروبية -كونها الاكثر تطورا وتخصيصا-، كالاتي

أ: تطور حماية البيانات الشخصية في ما يتعلق بتنظيم البنية التحتية الرقمية:

بداية من حالات تشغيل انترنت الأشياء والأنظمة والأجهزة الذكية، نجد أن قانون ‹قانون البيانات الأوروبي› (Data Act) منح الحق الصريح لمستخدمي تلك الأجهزة والأنظمة في الوصول للبيانات المولدة عن طريقها سواء كانت بيانات شخصية أو غير شخصية، وأيضا الحق في نقل البيانات بين مزودي

8 Eduardo Ustaran and others, ‹Data Protection and Privacy in the Age of Federated Learning› (2022) 14 Law, Innovation and Technology 1, 2-3 https://doi.org/10.1109/SENNET64220.2025.11135972 accessed 18 February 2026.

الخدمات المختلفين Data Portability بدون رسوم تعسفية من مزودي الخدمات[١٠]، مع اعتماده واحالته للائحة العامة لضمان حماية البيانات الشخصية في تلك النظم، وهي كلها إشكاليات وسيناريوهات للمعالجة لم يتناولها القانون المصري لحماية البيانات الشخصية المصري ولائحته التنفيذية

ب: تطور حماية البيانات الشخصية في ما يتعلق بتنظيم الأسواق والخدمات الرقمية:

أما على صعيد تنظيم الأسواق والخدمات الرقمية؛ فقد أرسى تشريعا «الأسواق الرقمية» (DMA) و»الخدمات الرقمية» (DSA) حزمة من الالتزامات والقيود المستحدثة الناظمة لكيفية معالجة البيانات الشخصية، سواء لأغراض تقديم الخدمات أو لضبط ممارسات المنصات المهيمنة (حراس البوابة Gate-keepers)[١١].

ففي هذا السياق، حظر قانون الأسواق الرقمية (DMA) دمج البيانات الشخصية المُجمَّعة من الخدمات والمنصات المتعددة التي يملكها ويديرها كيان مهيمن واحد، ما لم يتم الحصول على موافقة صريحة ومستقلة من الشخص المعني بالبيانات على واقعة الدمج ذاتها[١٢]. وبالتوازي، حظر قانون الخدمات الرقمية (DSA) ممارسات الاستهداف الإعلاني المباشر المستندة إلى «البيانات الحساسة»، فضلاً عن الحظر المطلق لتتبع سلوكيات القُصّر لأغراض إعلانية[١٣]، وأيضا فقد نص هذا القانون على حظر الخوارزميات التلاعبية والانماط المظلمة في تصميم واجهات التفاعل وغيرها من وسائل التلاعب بسلوكيات المستخدمين[١٤]، وهو ما يعني الانتقال من الحماية القائمة على الالتزامات للحماية القائمة على التصميم وهندسته

ويعكس هذا التوجه إدراكاً عميقاً من المشرع الأوروبي للدور المحوري للبيانات الشخصية كمحرك رئيس للاقتصاد الرقمي؛ إذ تطور توظيفها من مجرد آلية لتحسين جودة الخدمات، لتتحول إلى العصب الأساسي المشغل لبنى التحليل، والإحصاء، والاستهداف الخوارزمي، والتطوير. بل إن احتكار هذه البيانات واستغلالها بات يمتلك القدرة على التلاعب بآليات السوق الحرة في القطاع الرقمي، وتوجيه سلوكيات المستهلكين وتفضيلاتهم، على نحو يهدد أسس المنافسة العادلة ويخلق حواجز هيكلية أمام الكيانات الناشئة

ج: تطور حماية البيانات الشخصية في ما يتعلق بتنظيم الذكاء الاصطناعي:

يعد القانون الأوروبي للذكاء الاصطناعي أحد أهم القوانين الحديثة التي اعتمدت على اللائحة العامة لحماية البيانات الشخصية في أحكامها الأساسية، ولكنه أيضا أضاف العديد من القواعد المنظمة لمعالجة البيانات الشخصية في أطر تدريب ومخرجات واستعمالات نماذج الذكاء الاصطناعي، ومنها استحداث منظومة جديدة لتدرج المخاطر والحظر ابتداء من حظر ممارسات تُشكل انتهاكاً جسيماً للخصوصية؛ كأنظمة «التعرف الآني على الهوية البيومترية» (كالتعرف الآلي على الوجوه) في الأماكن العامة، وأنظمة التعرف على المشاعر في بيئات العمل والتعليم، وكذا تقنيات التصنيف الاجتماعي (Social Scoring)[١٥].

10 Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L 2023/2854, arts 1(5), 3, 4, 23.

11 Christophe Carugati, ‹The interplay between the Digital Markets Act and the General Data Protection Regulation› (2023) Bruegel Working Paper 06/2023, 4–7 https://www.bruegel.org/working-paper/inter-play-between-digital-markets-act-and-general-data-protection-regulation accessed 18 February 2026.

12 Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1, art 5(2)(b).

13 Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1, art 5(2).

14 Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) [2022] OJ L 277/1, art 25.

15 Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 1689/1, art 5(1)(c), (f), (h).

كما نص على ضرورة الالتزام بحوكمة البيانات عامة ومنها الشخصية بشكل يضمن جودتها، وتمثيلها الإحصائي السليم، وخلوها من التحيزات الخوارزمية قبل البدء في المعالجة[١٦]، وأيضا طور العديد من الحقوق للأشخاص المعنية بالبيانات منها تطويره للحق في عدم الخضوع للقرارات المؤتمتة بالكامل لينص أيضا على الحق في تفسير القرارات[١٧].

كما خصص هذا القانون العديد من أحكامه لمجابهة العديد من المخاطر النظامية التي قد تحدث جراء الذكاء الاصطناعي ومعالجة البيانات الشخصية باستخدام قدرات المعالجة المتطورة الكامنة في تلك النماذج والأنظمة، فقط حظر استعمال الذكاء الاصطناعي للتلاعب في قرارات الشخص المعني بالبيانات أو بإدراكه للوقائع والحقائق، وخاصة ما يعرف بالتقنيات لاشعورية (Subliminal Techniques) والتي تستهدف التلاعب بإدراك الشخص المعني بالبيانات الشخصية للوقائع أو توجيه قراراته خفيةً والتأثير على البني الديموقراطية والحقوق الأساسية منها الحق في الوصول للمعلومة وصحتها والتعبير عن الرأي فيما يعرف بتأثيرات الخوارزميات على الرأي من حيث خلق حالات التعصب والتطرف والحصر في تيار رأي معين، من خلال فرضه قيودا صارمة على «أنظمة التوصية الخوارزمية» (Recommender Systems) التي تعتمد على التنميط الدقيق للبيانات الشخصية بغرض تصنيف المستخدم وحصره داخل ما يُعرف بـ «غرف الصدى» (Echo Chambers) و»فقاعات الفلترة» (Filter Bubbles)[١٨].

د: تطور حماية البيانات الشخصية فيما يتعلق بتنظيم القطاع الصحي:

وفي القطاع الصحي، استحدث التشريع الخاص بالفضاء الأوروبي للبيانات الصحية استثناءات قطاعية تجيز «الاستغلال اللاحق» للسجلات الطبية في الأغراض البحثية دون الحاجة لاشتراط الموافقة الصريحة المسبقة لكل حالة، حيث شرع ونظم الية تقنية محايدة تجعل تبادل البيانات الصحية لأغراض الغرض الرئيسي تقديم الخدمات الصحية والغرض الثانوي البحث العلمي والإكلينيكي والتطوير ومجابهة الاوبئة يتم بسلاسة وسهولة عن طريق بنية تقدمية تضمن تجهيل البيانات وتجريم أي محاولات لإعادة تحديد هوية المرضى الذين يتم معالجة بياناتهم المجهلة لأغراض الغرض الثانوي[١٩].

ه: تطور حماية البيانات الشخصية فيما يتعلق بتنظيم القطاع المالي والمصرفي:

نهاية بالقطاع المالي حيث جاء توجيه خدمات الدفع الثاني (PSD2) وقانون المرونة التشغيلية الرقمية DORA ليلزم المؤسسات المالية بتبادل البيانات إلكترونياً كوسيلة لتفعيل «الحق في نقل البيانات»، وأيضا أضاف قواعد صارمة لضمان موثوقية النظم واستمرارية توافر البيانات[٢٠].

فلهذا لا يمكن النظر للفترة الزمنية بين سن القانون وإصدار اللائحة باستخفاف، فهي قد شهدت تغيرات هائلة على المستويين التقني والتشريعي تجعل التساؤل حول مدي فاعلية وجدوى اصدار لائحة لقانون قد جاء اثناء تشريعه بإشكالياته الاصيلة وعدم استيعابه لكم التعقيدات الكامنة في السيناريوهات المختلفة

16 Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 1689/1, art 10(3), (5).

17 Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, art 22; Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 1689/1, art 86.

18 Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 1689/1, art 5(1)(a); Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L 277/1, art 34(1)(b), (c).

19 Regulation of the European Parliament and of the Council on the European Health Data Space (EHDS Regulation) [2024], arts 33, 34, 35(4).

٢٠ Kilian Trautmann, ‹Cloud Computing Evolution and Regulation in the Financial Services Industry› (٢ (٢٠٢٣ ISACA Journal https://www.isaca.org/resources/isaca-journal/issues/٢٠٢٣/volume٢-/cloud-computing-evolution-and-regulation-in-the-financial-services-industry accessed ١٨ February ٢٠٢٦.

لمعالجة البيانات الشخصية في عصره ناهيكم عما جاء بعده من تطور تقني وتشريعي، مما ينقلنا للنقطة التالية، وهي بحث الإشكاليات الكامنة في القانون ذاته وأثرها على اللائحة التنفيذية

المطلب الثاني

الانعكاسات التشريعية للقانون على التنظيم اللائحي

وفي هذا المطلب، سنُخضع اللائحة لتقييم تحليلي وموضوعي لاختبار مدى التزامها بالإحالات التشريعية الواردة في القانون الأم، وبيان انعكاس ذلك على جاهزية النص القانوني للدخول في مرحلة الإنفاذ الفعلي والامتثال. كما سنبحث أثر هذه الانعكاسات على استقرار السوق والمراكز القانونية للأطراف المعنية، وذلك من خلال خمسة محاور دراسية محايدة، كالآتي

أولاً: قياس مدى كفاية النص القانوني واستيعابه للاستخدامات الدقيقة والمستحدثة للبيانات الشخصية وقت صدوره

ثانياً: تحليل الطبيعة الأحادية للنص ومدى مرونته وقابليته للتعاطي مع الحالات الخاصة لمعالجة البيانات الشخصية

ثالثاً: تقييم محددات النطاق التشريعي (من حيث التوسع والتضييق) ومدى اتساقها مع المعايير الدولية والوقائع التطبيقية

رابعاً: فحص البنية الإجرائية واختبار ملاءمتها للمتطلبات التشغيلية والعملية.

خامساً: دراسة هيكل الرقابة وآليات الامتثال لبيان مدى فاعليتها وتوازنها التنظيمي.

أولا: عدم كفاية النص القانوني للاستخدامات الدقيقة للبيانات الشخصية وقت صدوره:

لم ينص القانون المصري في نصه على أي من الاستخدامات المتقدمة للبيانات الشخصية والتي جاءت في قوانين سنت في نفس فترته الزمنية مثل مثلا اللائحة العامة لحماية البيانات الشخصية المصرية، مثل مثلا:

أ: استعمال البيانات الشخصية في التنميط:

يعتبر استعمال البيانات الشخصية في التصنيف والتنميط هو الرابط بين العديد من الاستعمالات المتقدمة للبيانات الشخصية مثل التتبع التسويقي والتقييم الائتماني والتأميني وكذا الاتخاذ المؤتمت للقرار وأيضا تدريب وتطوير ومخرجات الذكاء الاصطناعي، وفي حين خلا القانون المصري بالكلية من أي نص أو تعريف للتنميط أو إشارة له، نصت العديد من القوانين المعاصرة زمنيا له على تعريف وتنظيم للتنميط حفاظا على حقوق الأشخاص المعنية بالبيانات[٢١]، كون أن التنميط من أكثر وسائل المعالجة التي قد ينجم عنها مساسا للحقوق والحريات الأساسية للأفراد[٢٢].

٢١ نظم المشرع الأوروبي «التنميط» (Profiling) وعرّفه صراحة في المادة ٤(٤) من اللائحة العامة لحماية البيانات (GDPR)، كما أفرد المادة (٢٢) لضمان حق الشخص المعني في عدم الخضوع لقرارات مؤتمتة مبنية على هذا التنميط. وعلى الصعيد العربي المعاصر للقانون المصري، نجد أن قانون حماية البيانات الشخصية البحريني رقم (٣٠) لسنة ٢٠١٨، وإن لم يورد مصطلح «التنميط» لفظاً في مادة التعريفات، إلا أنه اعتنق مضمونه ونظمه صراحة في المادة (١٩) تحت مسمى «الحق في عدم الخضوع للقرارات الآلية»؛ حيث كفل لصاحب البيانات الحق في طلب عدم إخضاعه لقرار يُبنى حصرياً على المعالجة الآلية متى كان هذا القرار يهدف إلى «تقييم جوانب شخصية تتعلق به؛ كأدائه في العمل، أو حالته الائتمانية، أو سلوكه، أو مدى جدارته بالثقة»، وهو ما يجسد جوهر الحماية القانونية من التنميط الخوارزمي.

٢٢ يكمن خطر التنميط في خلقه ملفات وقوالب نمطية قد ينجم عنها تمييز او تقييد لخيارات الافراد او حرمان من الخدمات أو حتى وضع الافراد في قوالب محددة تخضعهم لتمييز عرقي واثني أو تحد من حرياتهم السياسية وتخضعهم لمراقبة ديكتاتورية مثلا، for

ب: استعمال البيانات الشخصية لأغراض أتمتة القرار:

ينجم عن عملية التنميط عادة ما يعرف بالاتخاذ المؤتمت للقرار حيث يتم ادخال البيانات الشخصية في عمليات معالجة متقدمة باستعمال خوارزميات معقدة وأنظمة ذكاء اصطناعي تعالجها لأغراض استنباط قرار نهائي فيما يخص معاملة معينة، أو يمس حقاً أصيلاً للشخص المعني، أو يوجه تصرفاً ضده. وهو ما ينعكس أثره مباشرة على المراكز القانونية للأفراد ومصالحهم الجوهرية، وهو ما قد يحدد ويؤثر على مصالح الشخص المعني بالبيانات، بل قد يصيبه بأضرار غير محددة تبعا لطبيعة هذا القرار وسياقه

ومع الحاجة لتقليل الكلفة في اتخاذ القرار أو حتى بدافع تسريعه قد يتم اتخاذه بشكل كامل بدون وجود بشري في دورة الاتمتة هذه human in the loop، مما يجعل الشخص المعني بالبيانات عرضة للاستبداد الخوارزمي (Algorithmic Dictatorship)، وأيضا قد يتم حرمان الشخص من الحق في التظلم أو معرفة المنطق الخوارزمي وراء اتخاذ القرار، وهو أعلى درجات انتهاك حقوق الشخص المعني بالبيانات

ولم يتطرق القانون المصري ولا حتى لائحته التنفيذية -والتي قصرت تنظيمها لاستعمال البيانات الشخصية لأغراض الذكاء الاصطناعي على تدريب النماذج لا مخرجاتها وموجهة فقط للمعالج [٢٣]- لمثل هذه الحالات، في حين جاءت مثلا اللائحة العامة لحماية البيانات الشخصية بتنظيم متكامل لها ضمن مثلا الحق في الاعتراض والحق في طلب المراجعة البشرية للقرار

ج: معالجة البيانات الشخصية لأغراض التوجيه والاستهداف الإعلاني وتحليل السلوكيات

فيما قصر القانون المصري ولائحته التنفيذية تنظيمهم لمعالجة البيانات الشخصية لأغراض الإعلانات المباشرة، فإن العديد من القوانين المعاصرة لصدور هذا القانون انتبهت للاستعمالات الأكثر خطورة وضررا للبيانات الشخصية في هذا الإطار كمثلا استعمالها للاستهداف الإعلاني وتحليل الأنماط والسلوكيات، واستنباط تفضيلاته الخفية، وهندسة خياراته الاستهلاكية أو حتى قناعاته الشخصية

وعلى عكس هذا فقد نظمت اللائحة العامة استعمال البيانات الشخصية لمثل هذه الأغراض عن طريق منح الشخص المعني بالبيانات الحق في الاعتراض على استعمال بياناته الشخصية لأغراض التنميط والتوجيه التسويقي[٢٤].

ثانيا: واحدية النص وعدم المامه بالحالات الخاصة لمعالجة البيانات الشخصية:

جاءت أحد عيوب القانون المصري والتي انتقلت للائحة التنفيذية في عدم تنظيمه لبعض من الحلات الخاصة لمعالجة البيانات الشخصية، كمثلا معالجة البيانات الشخصية في إطار علاقات العمل، معالجة البيانات الشخصية في القطاع الصحي ولأغراض الطب الوقائي والبحث الاكلينيكي، وأيضا لأغراض البحث العلمي والتاريخي والأدبي، وكذا معالجتها لأغراض الصحفية والإعلامية والتي اكتفى باستثنائها الكامل من أحكام القانون

هذا التعامل الموحد لجميع حالات معالجة البيانات الشخصية والذي ركز على المعالجة في السياق التجاري أثر على المرونة اللازمة للمحافظة على التوازن بين حقوق الشخص المعني بالبيانات والحاجات

Data Protection Working Party, ‹Guidelines on Automated individual decision– ٢٩ more in this: Article making and Profiling for the purposes of Regulation ٢٠١٦/٦٧٩› (WP٢٥١rev.٠١, ٢٠١٨) ٥–٦.

٢٣ قرار وزير الاتصالات وتكنولوجيا المعلومات رقم ٨١٦ لسنة ٢٠٢٥ بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠، م ٤ / ٧: التزام المعالج بالتعامل مع البيانات الشخصية، حال معالجتها واستخدامها لعمليات تدريب الذكاء الاصطناعي والتقنيات الناشئة والمبتكرة، وفقاً للمبادئ المتعارف عليها محلياً وإقليمياً ودولياً، بما يضمن استخدام تلك التقنيات بالصورة التي لا يترتب عليها ثمة ضرر بالشخص المعني بالبيانات.

24 General Data Protection Regulation (GDPR) [2016] OJ L 119/1, art 21(2), (3).

المختلفة لكل سياق من سياقات المعالجة

وقد أثر هذا على اللائحة التنفيذية والتي حاولت أن تنص على تنظيم خاص لمعالجة البيانات الشخصية لأغراض البحث العملي أو الأغراض الإحصائية اعتماد على البند السادس من المادة الخامسة من القانون والتي نصت في التزامات المعالج على أنه لا يجوز للمعالج أن يعالج البيانات الشخصية لغرض (يتعارض وليس يخالف) أغراض المتحكم أو نشاطه إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة، فنصت في البند السادس من المادة الرابعة الخاصة ب (السياسات والإجراءات والضوابط والشروط والتعليمات والمعايير القياسية لالتزامات معالج البيانات الشخصية) على أنه (حظر معالجة أي من البيانات الشخصية في غرض خلاف غرض المتحكم أو نشاطه إلا إذا كان بقصد إحصائي أو تعليمي وغير هادف للربح، وبالشروط الآتية: (أ) الالتزام بالحصول على موافقة الشخص المعني بالبيانات. (ب) أن يكون موضوع الدراسة ذا صلة بالبيانات الشخصية التي يتم معالجتها. (ج) حال تداول البيانات الشخصية بأي صورة من الصور يجب أن يتم ترميزها بحيث لا يمكن من خلالها الاستدلال على الشخص المعني بالبيانات.)

وبتحليل هذه الاشتراطات نجد أنها عادة ما ينص عليها كاستثناءات لتسهيل معالجة البيانات الشخصية لصالح البحث العلمي ولكن مع تناقض غريب غير محمود حيث أن عادة ما يتم النص على ضرورة ترميز البيانات بديلا عن الحاجة لموافقة الشخص المعني بالبيانات عن المعالجة لأغراض الغرض الثانوي (أي البحث العملي)[٢٥]، كما أن ربط هذه الحالة تحت بند المعالجة أو التزامات المعالج يقصر الحالة على المعالج دون المتحكم، وهو أيضا ما يرتبط بتعريف للمعالج جاء فقط في القانون المصري الذي أضاف لتعريف المعالج (ولصالحه)[٢٦]، وهو إن فهم هنا في هذا السياق أن المقصود به (الغرض الثانوي) فإن الأصح أن يطبق على هذا نص اللائحة العامة والتي نصت على أنه فور أن يقوم المعالج بمعالجة البيانات الشخصية لغرضه الخاص فهو يتحول لمتحكم بحكم الوظيفة[٢٧]، وهو الأصح والأكثر منطقية حيث أن القاعدة هنا هي أن المتحكم يحدد الغرض وطريقة المعالجة والمعالج حال تواجده يعالج البيانات طبقا لتعليمات وغرض المتحكم فقط بدون ان يكون له مصلحة محققة فيما يتعلق بتلك المعالجة[٢٨].

ثالثا: إشكالية التوسع والتضييق غير المتناسب مع المعايير الدولية والوقائع التطبيقية:

تتبدي واحدة من أكبر إشكاليات قانون حماية البيانات الشخصية المصري في توسعه في بعض الحالات وتضييقه في الأخر، هذا التوسع والتضييق قد يطرح تصادما على العديد من المستويات أولهما تصادما داخليا داخل النص التشريعي ذاته وثانيهما تصادما مع الوقائع العملية والتطبيقية، وثالثهما تعارضا مع الاتجاهات العالمية في معظم قوانين حماية البيانات الشخصية

وعلى الرغم من وجود العديد من تلك الحالات ، فإن المثال الذي يمكن أن يبين جميع تلك الأثار بشكل كامل هو ما نص عليه القانون من استثناء (البيانات الشخصية لدي البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة) وهي حسب قانون البنك المركزي المصري (البنك المركزي والجهاز المصرفي وشركات الصرافة وشركات تحويل الأموال وشركات الاستعلام والتصنيف الائتماني وشركات ضمان الائتمان ومشغلي نظم الدفع ومقدمي خدمات الدفع)، وفي نفس الوقت توسع في تعريف البيانات الحساسة فضم البيانات المالية لها

25 Regulation (EU) 2016/679 (GDPR), art 89(1), art 5(1)(b)

٢٦ تنص المادة (١) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ في تعريفها لـ «المعالج» على أنه: «كل شخص طبيعي أو اعتباري مختص بطبيعة عمله بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم...». ويُراجع كذلك البند (٦) من المادة (٤) من قرار وزير الاتصالات وتكنولوجيا المعلومات رقم ٨١٦ لسنة ٢٠٢٥ بإصدار اللائحة التنفيذية للقانون، والذي قصر الاستثناء الإحصائي والتعليمي على المعالج بالشروط المذكورة.

27 Regulation (EU) 2016/679 (GDPR), art 28(10), European Data Protection Board (EDPB), ‹Guidelines 07/2020 on the concepts of controller and processor in the GDPR› (Version 2.0, 2021) 34-35.

28 Regulation (EU) 2016/679 (GDPR), art 4(7), art 4(8), art 28(3)(a), European Data Protection Board (EDPB), ‹Guidelines 07/2020 on the concepts of controller and processor in the GDPR› (Version 2.0, 2021) 24–25. لـقواعد

وهذا خلافا لمعظم قوانين حماية البيانات الشخصية والتي لم تستثني القطاع المصرفي من أحكامها، وأيضا لم تضم البيانات المالية للبيانات الحساسة كونها من أكثر البيانات التي تعالج بشكل دوري ويومي

كما أن هذا يعني أن أكبر الجهات التي تعالج البيانات المالية مستثناة من أحكام القانون، وفي نفس الوقت فإن أي نشاط تجاري يقدم خدمات المدفوعات الإليكترونية هو متحكم في البيانات الحساسة مما يعين وجوب أن يخضع لشروط القانون الخاصة بالبيانات الحساسة ومن أهمها ضرورة التحصل على الموافقة الصريحة للشخص المعني بالبيانات على معالجة بياناته المالية

ومن ناحية تكييف العلاقات والالتزامات بين المراكز القانونية المنخرطة في نفس دورة المعالجة للبيانات الشخصية والبيانات الشخصية الحساسة، فإن هذا يعني عدم تمكن المتحكم او المعالج الخاضع للقانون حال تعاقده مع متحكم أو معالج غير خاضع للقانون من ايفاء كامل التزاماته القانونية المتعلقة بمعالجة تلك البيانات الحساسة، وخاصة ما يتعلق بالطرف المستثنى

وهو ما زادت اللائحة التنفيذية من أثره نتيجة بنيتها القائمة على واحدية مسار الالتزامات، وافتراضها الوجود الحتمي لجميع المراكز القانونية المنصوص عليها قانونا وخضوعهم جميعا لأحكام القانون في جميع حالات المعالجة، وخاصة في ظل الزامها للمعالج أن يسجل في سجل المعالجة الخاص به بعض البيانات عن المتحكم والتي لا يمكن ايفاءها إلا لمتحكم خاضع للقانون[٢٩].

رابعا: إشكاليات البنية الإجرائية:

في حين جاءت معظم قوانين حماية البيانات الشخصية قائمة على نظم الاخطار المسبق والامتثال المستمر، نص القانون المصري على نظام من التراخيص والتصاريح المسبقة القائمة تاركا للائحة التنفيذية تحديد شروطها، وعلى الرغم من أن وجود تصاريح او تراخيص مسبقة للأنشطة الخطرة هو أمر معتاد، إلا أن الاعتماد على هذا النظام في نشاط يقوم به أي شخص يتعامل مع الأشخاص بشكل اليكتروني له مخاطره الخاصة المتمثلة في ابسطها العبء الإداري الضخم على الجهة الإدارية، وأيضا عب الامتثال الضخم على جميع المخاطبين بأحكام القانون، كما أنه في حالات خاصة قد تشل السوق وحركة الاستثمار والمعاملات

والحقيقة أن الأثر الأكبر للقانون في نظام التراخيص هذا هو ما نص عليه في المادة السابعة والعشرون من أليات التقدم والمدد وكيفية القبول والرفض حيث أنه نص على مدة ضخمة للبت في طلبات التراخيص والتصاريح وهي تسعون يوم من تاريخ استيفاء جميع المستندات، وأيضا نصه على أن عدم الرد على طلب الترخيص أو التصريح يعتبر رفضا، أما عن باقي أثار نظام التراخيص والتصاريح الذي أتى في اللائحة فقد كان بالإمكان تفاديه إذا ما أتت بتنظيم أكثر كفاءة واتساقا مع أحكام القانون المرنة في هذا الشأن، ولكن هذا سيتم تناوله بالتفصيل المناسب في مكانها الخاص اللاحق في تلك الدراسة

خامسا: إشكاليات بنية الرقابة والامتثال:

يمكننا القول بأن القانون المصري جاء في بعض مواده الناظمة لبنية الامتثال والرقابة مخالفا لما اتفق عليه من مبادئ عالمية من ناحية والتوازنات المطلوبة تشريعيا من ناحية اخري فيما يتعلق ببنية الرقابة والامتثال كالاتي

٢٩ اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري، م ٤ ثانيا ٣- الاعتماد في سياسات العمل على إعداد سجل إلكتروني مؤمن ، يتضمن الآتي : -قيد ووصف عمليات المعالجة التي يجريها ، و فئات البيانات الشخصية التي يستخدمها ونطاق استخدامها ، على أن يتضمن السجل بيانات المعالج ، وصورة عقد المعالجة المبرم مع المتحكم ، وبيانات مسؤول حماية البيانات الخاص بالمتحكم ، وبيانات الممثل القانوني للمتحكم ، ومعايير المعالجة ، وفي حالة نقل البيانات عبر الحدود توضيح البلاد التي يتم نقل البيانات لها ، والنظم الخاصة بتأمينها ومسار البيانات ، ووصف عام للمعايير التقنية المستخدمة لحماية البيانات

أ: فيما يتعلق ببنية الرقابة:

فقد عيّن وأسمى الجهة المعنية بالرقابة بأنها «مركز حماية البيانات الشخصية»، وكيّفها في المادة (١٩) من القانون على أنها «هيئة عامة اقتصادية تتبع الوزير المختص (وزير الاتصالات وتكنولوجيا المعلومات)». وهو ما يجعل المركز «جهة تابعة هيكلياً للسلطة التنفيذية وتحت مظلة حقيبة وزارية تقنية، مما يسلبه الاستقلالية المؤسسية والحياد الرقابي التام، ويضعه في شبهة تعارض المصالح (Con-flict of Interest)، لاسيما وأن الحكومة والوزارة ذاتها تُعد من أكبر المتحكمين في بيانات المواطنين»

فيما نجد أن الاتجاه الأمثل هو ما جاء باللائحة العامة لحماية البيانات الأوروبية (GDPR)، والتي نصت وكيّفت «مفوضيات حماية البيانات الشخصية» (Supervisory Authorities) على أنها «سلطات عامة مستقلة، تتصرف باستقلالية تامة (Complete Independence) في أداء مهامها وممارسة سلطاتها، ويبقى أعضاؤها خاليين من أي تأثير خارجي مباشر أو غير مباشر»، وذلك وفقاً لنصوص المادتين (٥١) و (٥٢) من اللائحة[٣٠].

وفي اتجاه مقارن آخر، جاء مثلاً في القانون التونسي لحماية المعطيات الشخصية تكريس لهذه الاستقلالية ولكن بشكل أقل -ولكنه اكثر ملائة من الاتجاه المصري-؛ حيث أسند المهمة إلى «الهيئة الوطنية لحماية المعطيات الشخصية»، وكيّفها في المادة (٧٥) على أنها «هيئة عمومية تتمتع بالشخصية المعنوية والاستقلال المالي»، لضمان عدم خضوعها لهيمنة الوزارات التنفيذية[٣١]. أما القانون البحريني، فقد أضاف الهيئة للحقيبة العدلية لا الحقيبة التقنية؛ حيث أسند في المادة (١) والمادة (٤٧) تبعية «هيئة حماية البيانات الشخصية» إلى «الوزير المعني بشئون العدل»، مما يُضفي على قراراتها طابعاً قانونياً وحقوقياً محايداً، وينأى بها عن تضارب المصالح التقني[٣٢].

والحقيقة أن هذا الاتجاه ما هو إلا معبّر عن سياسة مصرية متفردة -والتي تثير بدورها بعض الإشكاليات- في إيلاء كل ما يتعلق بالجانب التشريعي (من اقتراح للقوانين وسنّ للوائح) والرقابي على التقنية وقطاعها لوزارة الاتصالات وتكنولوجيا المعلومات؛ وهو ما نجم عنه توسعٌ كبيرٌ في مهام تلك الوزارة، والتي أصبحت في مصر تجمع بين ثلاث مهام درجت الممارسات العالمية على الفصل بينها، بشكل ألقى بظلاله وأثر بوضوح على بنية القوانين المصرية والجهود التنظيمية في هذا القطاع

ب. من ناحية الامتثال (أزمة تكييف دور مسئول حماية البيانات - DPO):

نجد أن القانون المصري قد جاء باتجاهه الخاص الذي اتبع أيضاً نمط التوسع والتضييق غير المتناسبين فيما يتعلق بتنظيمه لمهنة ووظيفة «مسؤول حماية البيانات الشخصية»، وهو ما يمكن اختصاره في الآتي

1: التوسع في المهام والمسائلة:

فهو من ناحية قد توسع بشكل غير مبرر في المهام والالتزامات المطلوبة من «مسؤول حماية البيانات الشخصية»، حيث جاء القانون مكلفاً إياه في المادة (٩) بالآتي: (إجراء التقييم والفحص الدوري للنظم، والعمل كنقطة اتصال مباشرة مع المركز وتنفيذ قراراته، وتمكين المركز من إجراء التفتيش على الكيان). وبمقارنة ذلك بالاتجاه العالمي (كالمادة ٣٩ من اللائحة العامة)[٣٣]،

فنجد أن صياغة القانون المصري لتلك المهام شابها بعض الغموض الذي ألقى بظلاله على اللائحة وخاصة فيما يتعلق بتقديم التقارير، حيث نص على الآتي: «١ – إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايته.»، وهو ما يُفهم أنه يخص عمله الداخلي داخل الكيان الذي يعمل به، حيث إن الدارج عالمياً أن دورة عمل

30 GDPR, Chapter VI (Independent Supervisory Authorities), Articles 51 & 52.

٣١ القانون الأساسي التونسي عدد ٦٣ لسنة ٢٠٠٤ المتعلق بحماية المعطيات الشخصية، الباب السادس، المادة ٧٥.

٣٢ قانون رقم (٣٠) لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية بمملكة البحرين، الباب الأول (التعاريف- المادة ١)، والباب السادس (المادة ٤٧).

33 GDPR, Regulation (EU) 2016/679, Article 39(1)(a) and (b) (Tasks of the data protection officer.

المسؤول تكون كالآتي: (الفحص، الإبلاغ الداخلي لجهة الإدارة العليا، تقديم الاستشارات والحلول لكيفية الامتثال الأمثل، الانتظار للتحرك والتعديل، إذا لم ينجم عن هذا تعديل وتصحيح لموطن خلل الامتثال يجب عليه لكي لا يتحمل المساءلة التضامنية مع المُساءَل أن يبلغ الجهة الرقابية لتتخذ إجراءاتها حسب ما يتراءى لها طبقاً لصلاحياتها)[٣٤]، وبهذا يكون دور مسؤول حماية البيانات الشخصية هو مراقب ومساعد داخلي للامتثال، مما ينجم عنه الثقة بين الأطراف الداخلية الفاعلة، والنظر للمسؤول من قبل المتحكم والمعالج على أنه مساعد وأداة مهمة لا كمراقب وعين داخلية

كما أنه في اتجاه منفرد تشريعياً، قام بمعاقبته جنائياً على (الإخلال بمهام وظيفته)، حيث نصت المادة (٣٧) من القانون على معاقبة مسئول حماية البيانات بغرامة ضخمة (لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه) حال تقاعسه عن أداء الالتزامات الواردة في المادة (٩). هذا التجريم المباشر للموظف يخالف القواعد العالمية المستقرة التي تُلقي بمسئولية عدم الامتثال وتوقيع الجزاءات على (المتحكم أو المعالج) بصفتهما الكيان الأصيل المستفيد من المعالجة، ولا تسأل المسئول شخصياً عن قصور الإدارة[٣٥].

2: الفراغ التشريعي فيما يتعلق بالضمانات الوظيفية:

وفي نفس الوقت خلا من أي ضمانات له؛ فلم تُورد نصوص القانون أي حماية وظيفية تكفل استقلاليته، أو تمنع توجيهه، أو تحظر إقالته وعزله نتاج ممارسته لمهام عمله والتبليغ عن المخالفات، على عكس الضمانات التي اتفق في أكثر من نظام قانوني على منحها له، كمثلا اللائحة العامة الأوروبية[٣٦] والقانون البحريني لحماية البيانات الشخصية وقراراته المكملة[٣٧]، والنظام السعودي لحماية البيانات الشخصية وقراراته المكملة[٣٨]، وهي ما يمكن تعدادها في الآتي: ((أولاً: كفالة الاستقلالية التامة للمسئول في أداء مهامه الرقابية والاستشارية بمعزل عن أي تأثيرات أو ضغوط إدارية، ثانياً: الحظر القاطع لتوجيه أي تعليمات أو أوامر له من قِبل جهة العمل فيما يتعلق بآلية ممارسة تلك المهام، ثالثاً: إقرار الحصانة الوظيفية ضد العزل أو العقاب بحيث يُمنع إنهاء عقده أو توقيع أي جزاءات عليه كإجراء انتقامي لأدائه مهامه أو إبلاغه عن المخالفات، رابعاً: ضمان التبعية الإدارية والارتباط المباشر بأعلى سلطة في الكيان لضمان وصول تقاريره لمركز صنع القرار دون حجب، خامساً: التمكين المؤسسي عبر توفير كافة الموارد اللازمة مع منحه صلاحية الوصول المطلق للبيانات وعمليات المعالجة، وسادساً: درء تعارض المصالح عبر حظر تكليفه بأي مهام تنفيذية أخرى تتصادم مع حياديته الرقابية)

هذا الفراغ التشريعي يترك المسئول أعزل أمام إدارته التي تدفع راتبه وتملك حق إقالته، ومهدداً في ذات الوقت بالغرامة الجنائية من قِبل الدولة؛ مما يضعه في «مأزق وظيفي مستحيل» و»تضارب مصالح قاتل» يُفرغ هذه الوظيفة من أي قيمة رقابية حقيقية

ج: غياب اليات التظلم من قرارات مركز حماية البيانات الشخصية:

يبرز الأثر التالي للقانون على اللائحة التنفيذية في خلو القانون التام من بنية تظلمات في قرارات مركز حماية البيانات الشخصية، وهو عوار شديد الخطورة والأثر، وخاصة في ظل التوسع الكامل في سلطات المركز، والذي نلمسه في تعداد سلطات المركز وصلاحياته في القانون؛ حيث نلمس الآتي بتحليل مواد

34 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (‹DPOs›), WP 243 rev.01, Section 3.2 (Position of the DPO).

35 Article 29 Data Protection Working Party (WP29), Guidelines on Data Protection Officers (‹DPOs›), WP 243 rev.01, Section 3.2: «DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a corporate responsibility of the controller or the processor, not of the DPO.»

36 (GDPR), Article 38(3).

٣٧ قرار وزير العدل والشئون الإسلامية والأوقاف بمملكة البحرين رقم (٤٣) لسنة ٢٠٢١ بشأن شروط وإجراءات تعيين مراقب حماية البيانات الشخصية (المنفذ للقانون رقم ٣٠ لسنة ٢٠١٨)، المادة (٥)

٣٨ اللائحة التنفيذية لنظام حماية البيانات الشخصية بالمملكة العربية السعودية (الصادرة بقرار رئيس مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي رقم ٧٩٨ وتاريخ ١٤٤٥/٠٢/٢٣هـ)، المادة (٣٢) فقرة (٣)،

القانون المتعلقة بصلاحيات وسلطات المركز

- منحت المادة (التاسعة عشرة من القانون) المركز سلطات واسعة بداية من الدور التوعوي حتى الدور الرقابي والتفتيش، مروراً بدوره في وضع وإرساء سياسات مثلى وقرارات تتعلق بمعايير حماية البيانات الشخصية وتأمينها، وسلطة إيقاف الرخص وسحبها وإلغائها.
- وأيضاً أعطى لرئيسه التنفيذي سلطة توجيه الإنذارات، ولمجلس الإدارة سلطة إصدار جزاءات إدارية طبقاً للمادة (الثلاثين) من القانون، وهي كلها سلطات ذات آثار جسيمة على أي نشاط أو شخص يعالج البيانات الشخصية، دون وجود لجنة تظلمات مستقلة توازن هذه القوة.
- كما برز دوره كحارس لبوابة المشروعية من خلال منظومة التراخيص والتصاريح؛ إذ حظرت المادتان (١٤) و(٢٦) من القانون على أي متحكم أو معالج إجراء عمليات معالجة للبيانات الحساسة أو نقلها عبر الحدود أو ممارسة التسويق الإلكتروني إلا بعد الحصول على ترخيص أو تصريح مسبق من المركز.
- وأيضاً توسع القانون في صلاحيات المركز في التعديل والاستحداث؛ عبر إحالة تفويضات تشريعية مفتوحة للمركز ومجلس إدارته —كما في المادتين (١٥) و(٢٦)— لاستحداث الاشتراطات، وتعديل المعايير الفنية والمالية، وإصدار التراخيص والقيد في السجلات، وهو ما مَثّل تفويضاً استغلته اللائحة لتمرير التزامات غير مسبوقة.
- وأيضاً تكييف بنية التراخيص والتصاريح القائمة على الرفض لا الموافقة؛ وهو ما نصت عليه صراحة المادة (٢٨) من القانون باعتبار مضي مدة تسعين يوماً على تقديم طلب الترخيص دون رد من المركز بمثابة رفض للطلب، مما يؤسس المنظومة على القرار الإداري السلبي بالرفض، ويضع الكيانات تحت وطأة التعسف في ظل انعدام جهة تظلم محايدة.

هذا الفراغ التشريعي يخالف ما جاء في عدد كبير من القوانين، ففي القانون البحريني لحماية البيانات الشخصية، حُدد نظام متكامل للتظلمات في المادة الخامسة والخمسون من القانون. وبالمثل، فصلت المادتين الخامسة والثلاثون والسادسة والثلاثون من النظام السعودي لحماية البيانات الشخصية اليات التظلم أيضا، مع ضمان حق الالتجاء للقضاء في كلا منهما، وهو ما يؤسس لديموقراطية القرار ويمنع المركز من التعسف في استعمال السلطة

وتأسيسا على هذا التحليل السريع لا يمكننا غض الطرف عن تأثير القانون السلبي على اللائحة، حيث أن بعضا من أحكام القانون انعكست بأثر سلبي متفاوت الشدة على اللائحة، مما جعل النص اللائحي يرث العديد من عوار النص التشريعي الأصلي، وخاصة في ظل الاحالات المتعددة التي نص عليها القانون للائحة لإكمال العديد من تفاصيله الدقيقة، وهو ما سنتطرق اليه لاحقا في خضم هذه الدراسة

المبحث الأول

التوافق التشريعي للائحة وتحقيق الجاهزية والكفاية

بعد أن استعرضنا في المبحث التمهيدي السياق الزمني والتشريعي الحاكم الذي وُلدت فيه اللائحة التنفيذية، ننتقل في هذا المبحث إلى الاشتباك المباشر مع النص اللائحي ذاته، وذلك لتقييمه من زاويتين متلازمتين لا غنى عنهما لنجاح أي أداة تشريعية: «التوافقية والالتزام بأحكام القانون الأصلي» و»وتحقيقها لهدفها الرئيس وهو تحقيق الحد الأكبر من الجاهزية التشغيلية للقانون

وهو ما سنحاول تحليله في هذا المبحث وهذا على مطلبين، كالآتي:

المطلب الأول: الانضباط التشريعي وحدود الاتساق مع القانون.

المطلب الثاني: الكفاية التنظيمية والجاهزية للإنفاذ.

المطلب الأول

الانضباط التشريعي وحدود الاتساق مع القانون

يُعد «الانضباط التشريعي» (Legislative Discipline) والاتساق الهيكلي بين التشريع الأصلي (القانون) والتشريع الفرعي (اللائحة التنفيذية) المعيار الحاكم لسلامة البنيان القانوني واستقرار المراكز القانونية. وفي هذا السياق، يبرز تساؤل منهجي حول مدى التزام اللائحة بحدود التفويض التشريعي، ومراعاتها للترابط العضوي بين نصوص القانون وغاياته؛ تجنباً لخلق بيئة تنظيمية تتسم بالتناقض أو الازدواجية

وفي هذا المطلب سنقيم هذا، وذلك من خلال سبعة محاور ، كالآتي:

أولاً: تحليل مدى الاتساق التشريعي في معايير «مشروعية الغرض والمعالجة» بين مرونة القانون وحصرية اللائحة

ثانياً: تقييم التكييف القانوني لاشتراطات «النقل العابر للحدود للبيانات» واختبار توافقها مع القواعد الحاكمة في التشريع الأصلي

ثالثاً: فحص التوازن التنظيمي لآليات «التسويق الإلكتروني المباشر» ومقاربة التباين المعياري بين النصين

رابعاً: دراسة التحولات في التنظيم القانوني لمهنة «مسؤول حماية البيانات الشخصية» (DPO) وانعكاساتها العملية

خامساً: تحديد النطاق القانوني والدستوري للتوسع في صلاحيات «المركز»، واختبار مشروعية تقرير سلطة توقيع الغرامات الإدارية

سادساً: قياس أثر التوسع اللائحي في «متطلبات التراخيص» على البنية العامة للامتثال والمساءلة.

سابعاً: استعراض محددات «المراكز القانونية» واختبار دقة توزيع الالتزامات بين أطراف عملية المعالجة.

أولا: إشكالية عدم الاتساق بين حصرية مشروعية الغرض والمعالجة في اللائحة وتنوعها في القانون:

جاءت أول إشكاليات اللائحة في اعتمادها الكامل على الموافقة كالسبب الوحيد والحصري لمشروعية المعالجة، وهذا نتاج اعتمادها على الإحالة التي جاءت في المادة الثانية من القانون والتي نصت على: (لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانوناً.)

فقد تغاضت اللائحة عن (الأحوال المصرح بها قانوناً) والتي بها إحالة داخلية للمادة رقم ٦ من القانون وهي مادة (شروط المعالجة) والتي نصت على أسباب غير الموافقة لمشروعية المعالجة بل وساوت بينها وبين المعالجة، حيث نصت على أربعة أسباب لمشروعية المعالجة وهي: (الموافقة، الضرورة العقدية أو الالتزام القانوني أو للمطالبة بحقوق قانونية أو للدفاع القانوني، تنفيذ أوامر قضائية أو من جهات تحقيق أو ما ينص عليه القانون، الالتزامات المشروعة للمتحكم غير المخلة بالحقوق الأصيلة والأساسية للشخص المعني بالبيانات)، وأيضا المادة الثانية عشر والخاصة بمعالجة البيانات الشخصية الحساسة والتي نصت أيضا على (وفيما عدا الأحوال المصرح بها قانونًا، يلزم الحصول على موافقة كتابية وصريحة من الشخص المعني. وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر.) أي أن الاستثناء أيضا امتد للموافقة الحصرية الكتابية على معالجة البيانات الشخصية الحساسة)

ونتيجة عدم مراعاة اللائحة لهذه الإحالة والتي نصت على أن مشروعية المعالجة تُبنى على أربعة أسباب متساوية في القوة، جاءت بنيتها الموضوعية والإجرائية كاملة مبنية على موافقة الشخص المعني بالبيانات، فالأثر المبني على هذا لا يقف فقط على عدم نص اللائحة على أي سبب آخر لمشروعية المعالجة في المادة الثانية من اللائحة والتي نصت فقط على الموافقة كسبب لمشروعية جمع ومعالجة البيانات الشخصية في تجاهل تام للمادة السادسة من القانون، والذي يمكن أن نقول إن المادة السادسة من القانون تسري بقوة الإلزام التشريعي الأعلى، وتسمو في تطبيقها على النص اللائحي القاصر إعمالاً للمبدأ الدستوري المستقر بشأن «تدرج القواعد القانونية»؛ فالتشريع الفرعي (اللائحة التنفيذية) لا يملك بأي حال إلغاء، أو تقييد، أو تعطيل المفاعيل القانونية لأسباب المشروعية البديلة التي أقرها التشريع الأصلي

وبحصر هذا الأثر على عملية الامتثال من حيث الالتزامات الموضوعية للمتحكم والمعالج، وإجراءات التراخيص المتعددة، نجد أن اللائحة اكتفت حصريا بذكر والنص على (الموافقة) كالسبب الوحيد المكافئ لمشروعية المعالجة بدلا من أن تنص على (سند مشروعية المعالجة)، وهو ما يمكن ضرب امثلة عليه في أكثر من موضع كالآتي

أ: بالنسبة للالتزامات الموضوعية والتي قد ينجم عنها اصطدام بين المتحكم والمعالج الممتثل وجهة انفاذ القانون التي قد تطالب اثناء التفتيش بالالتزام الحرفي، نجد الاتي

- نصت المادة (٢) (سياسات وإجراءات المعايير العامة) على أن يتضمن السجل الإلكتروني المؤمن للمتحكم: «موافقة الشخص المعني بالبيانات، وتاريخ صدور هذه الموافقة، والصورة التي صدرت عليها»، وهو ما يعني جمود بند سبب مشروعية معالجة البيانات في الموافقة المسبقة فقد لا غير.
- ركزت اللائحة في المادة (٣) بند (٥ و ٨) على إلزام المتحكم بإعداد آلية تتيح للشخص المعني «العدول عن الموافقة المسبقة»، وطلبات «محو بياناته والعدول عن موافقته السابقة»، وهو ما يجب أن يعدل للاتي في حالة الموافقة يجب أن يوفر المتحكم آلية للشخص المعني بالبيانات للعدول عن موافقته حيث أنه لا يجوز أن يكون العدول مطلقا حال وجود أسباب ذات طبيعة الزامية على الطرفين او لصالح المتحكم مثل تنفيذ الالتزامات القانونية او الأوامر القضائية مثلا.
- ولحقها نص المادة (٤) الخاصة بالتزامات المعالج، بإلزامه بإعداد آلية «تسمح بتسجيل

موافقة الشخص المعني بالبيانات على ذلك»، وهو على الرغم من أنه من التزامات المتحكم، ولكنه أيضا يجب أن يصاغ بصورة أكثر عمومية تدل على «تسجيل سبب مشروعية معالجة البيانات الشخصية».

- في المادة (٤) بند (٦) من اللائحة، والتي تنظم الاستثناء الممنوح للمعالج بإجراء معالجة لأغراض إحصائية أو تعليمية، اشترطت اللائحة بشكل قاطع: «الالتزام بالحصول على موافقة الشخص المعني بالبيانات»، وهو من ناحية الموافقة يلقي بظلاله على عدم اعتبار تنوع حالات المعالجة للأغراض الإحصائية والتي يجب أن تفصل بين الإحصاء لأغراض التقييم والتحسين الذاتي للنظم دون الاستخدام لتطوير البرامج والنظم بل يقتصر على حالات التقييم وتفادي القصور في نظم المعالجة، وهو غرض مشروع لا يجب أن يستند ل «موافقة الشخص المعني بالبيانات»، أم في حالات المعالجة لأغراض تطوير برامج ونظم بما فيها ما يتعلق بتدريب وتطوير نماذج وتطبيقات الذكاء الاصطناعي فهو ما يمكن أن يستند لموافقة الشخص المعني بالبيانات.
- في المادة الرابعة عشر البند الثاني نصت المادة على (٢- الحصول على موافقة كتابية صريحة (ورقيا أو إلكترونيا) من الشخص المعنى بالبيانات أو ولي الأمر في حالة بيانات الأطفال في غير الأحوال المصرح بها قانونا)، وهو ما قد يشل بعض الحالات التي تتطلب تدخل مباشر للحفاظ على المصالح الحيوية للشخص المعني بالبيانات (كحالات التدخل الطبي في الطوارئ مثلا).

وهناك أيضا حالات تعارض أخرى فيما يتعلق بنقل البيانات الشخصية عبر الحدود واتاحتها والتسويق الاليكتروني سوف نوردها في مكانها المخصص لاحقا

ب: أما عن الأثر الإجرائي فيما يتعلق بشروط وعملية استخراج التراخيص:

فقد امتد أثر هيكلة اللائحة الأحادية على الموافقة كالحالة الواحدة لمشروعية المعالجة على تلك الإجراءات، حيث اشترطت المواد (٢١ و٢٢) لترخيص المتحكم والمعالج تقديم: «بيان الآلية المستخدمة للحصول على موافقة الشخص». وتأكد ذلك في المواد (٣٥ و٣٧)، ليبلغ ذروته في المادة (٤١) ضمن القائمة الإلزامية لنماذج التراخيص التي تطلب: «بيان بآلية الحصول على موافقة الشخص المعني»، وهو ما يعني تصادم كبير بين واجهة وأليات تقديم التراخيص والتصاريح إذا التزم مركز حماية البيانات الشخصية المصري بجمود النص أثناء تصميمه للواجهة التفاعلية والبوابات الإليكترونية المنصوص عليها في اللائحة كالألية الحصرية المنصوص عليها في اللائحة لتقديم طلبات التراخيص والتصاريح، وخاصة اذا تم دمج هذا مع اليات وصلاحيات المركز فيما يتعلق بالتراخيص والتصاريح، ولهذا نأمل أن تخرج الترجمة الاليكترونية الإجرائية لتلك الاليات بصورة اكثر اتساقا مع القانون من الصورة النصية للائحة

ج: أثر عدم الاتساق:

وبعد هذا التتبع يمكننا ان نرى أن تغافل اللائحة عن اعتبار وايلاء أسباب المشروعية الأخرى الواردة في المادة السادسة من القانون، نجم عنه عدم اتساق وعوار تغلغل في كل مواد اللائحة ابتداء من المواد التنظيمية من المادة الثانية وحتى نهاية مواد الإجراءات في اخر مادة في اللائحة المادة الواحدة والأربعون، مما قد ينجم مع الاخذ في الاعتبار النص القانوني وحتميته وعلوه عن النص اللائحي تصادم بين واقعي بين المخاطبين بأحكام القانون وجهات الانفاذ كمركز حماية البيانات الشخصية سواء أثناء مراحل الامتثال والمراقبة او مراحل تقديم الرخص والتصاريح، مما قد يترجم لدعاوي تفسير وإلغاء أو بطلان للائحة، وهو ما قد يحمل المخاطب أعباء مالية وإدارية وتشغيلية بل حتى جزاءات مالية (غرامات الرخص الصادرة من المركز)، نتيجة لعوار اللائحة وعدم اتساقها مع النص القانوني وهو ما لا يمكن القول بأن للمخاطب له يدا فيه

ثانيا: التعارض بين تكييف مشروعية النقل العابر للحدود في اللائحة والنقل العابر للحدود في القانون:

امتد أثر الهيكلية البنيوية للائحة لاختلاف جذري ومركب بين قواعد نقل البيانات الشخصية عبر الحدود في القانون بمادتيه الرابعة عشرة والخامسة عشرة، والإتاحة في المادة السادسة عشرة، واللائحة في المادة السادسة عشرة فيما يتعلق بالنقل عبر الحدود، والسابعة عشرة فيما يتعلق بإتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية، وهو ما يتمثل في الآتي:

١. المنهجية التشريعية للقانون (قاعدة الكفاية، واستثناء الموافقة):

تبنى قانون حماية البيانات (رقم ١٥١ لسنة ٢٠٢٠) في المادتين (١٤ و١٥) منهجية تتوافق تماماً مع المعايير الدولية (مثل اللائحة الأوروبية GDPR)، فقد وضع قاعدة عامة في المادة الرابعة عشرة ثم استثناءاتها في المادة الخامسة عشرة، كالآتي:

فقد أرسى في المادة (١٤) القاعدة العامة المتمثلة في «مستوى الحماية الكافي" (Adequacy Decision)؛ حيث يُحظر نقل البيانات لدول لا توفر مستوى حماية يقل عن المستوى المقرر في مصر، ويجوز النقل إذا توفر هذا المستوى بموجب ترخيص من المركز.

ثم جاءت المادة (١٥) لتضع «الاستثناءات" (Derogations) في حال غياب مستوى الحماية الكافي في الدولة المستقبلة؛ ومن بين هذه الاستثناءات: (الحفاظ على حياة الشخص المعني بالبيانات وتوفير الرعاية الصحية له أو إدارتها، الحصول على الموافقة الصريحة، أو الضرورة العقدية، أو الدفاع عن حقوق قانونية، التعاون القضائي بين الدول، والاتفاقيات الثنائية بين الدول، والتحويلات النقدية).

أي أن القانون جاء بشرط أساسي لمشروعية نقل البيانات الشخصية عبر الحدود وهو شرط الكفاية، ثم بعد ذلك نص على استثناءات إدراكاً منه للأهمية اللازمة لمرونة شروط نقل البيانات الشخصية عبر الحدود، ووجود حالات لا تتعلق بالحقوق الشخصية للأفراد، بل تتعلق بإنفاذ القانون والتعاون الدولي والعلاقات الدولية بما لهذه الأسباب من أهمية لازمة تفوق الاعتبارات الفردية. كما أنه يتوافق منطقياً مع فلسفة النقل العابر للحدود، حيث إن شرط الكفاية هو ما يسهم في تكوين قاعدة قانونية متوافقة عابرة للحدود، أما الموافقة كشرط أساسي للنقل فهو غير منطقي نتيجة لجهل معظم الأفراد بالمخاطر وآثار عملية النقل، مما يجعلها شرطاً استثنائياً للنقل لا شرطاً أساسياً. وأيضاً لا منطقية من دمجهما معاً، حيث إن الكفاية تعني تحقق كافة شروط الحماية التي وافق عليها الشخص المعني بالبيانات أثناء معالجة بياناته الشخصية في الأصل، هذا إن كانت المعالجة تقوم على الموافقة، أما في حالة عدم قيامها على الموافقة فهو يخلق تعارضاً بين عملية لاحقة والعملية الأساسية يزيد من عدم التوافقية القانونية.

٢. الدمج بين الكفاية والموافقة وطرح باقي الاستثناءات في اللائحة:

وهو عكس ما جاءت به اللائحة والتي لم تسهم في تحقيق غرض المشرع، بل عصفت به تماماً من خلال نصها على آلية معقدة ومخالفة تماماً لمقاصد المشرع، حيث دمجت اللائحة التنفيذية في المادة (١٦) بين الحالة العامة للكفاية واستثناء الموافقة؛ فقد نصت في البند (٢) على أنه: «يلتزم المتحكم أو المعالج... حال نقل البيانات الشخصية... بالحصول على موافقة الشخص المعني بالبيانات". وبتحليل هذا النص نجد أنه خالف بشكل مطلق النص الأصلي للقانون، حيث إنه دمج «شرط الحماية الكافية» مع «شرط الموافقة» كشرطين متلازمين وجوبيين لعملية النقل في كافة الأحوال، وهو ما يُكيّف مخالفة اللائحة للقانون في محورين، كالآتي:

- تكييفها للموافقة كشرط إضافي مع شرط الكفاية، في حين أنها طبقاً للقانون استثناء لها.
- تجاهلها التام لباقي الحالات الاستثنائية لمشروعية نقل البيانات الشخصية عبر الحدود التي جاءت في المادة الخامسة عشرة.

٣. الأثر على الامتثال والإجراءات:

وهو ما يعني امتداد الاصطدام بين الممتثل والمرخص والمركز حال طلب ما يدل على موافقة الشخص المعني بالبيانات أثناء الترخيص أو التفتيش.

ثالثا: التعارض بين مرونة التسويق الاليكتروني المباشر في القانون والتشدد في اللائحة:

يعتبر التسويق الالكتروني المباشر أحد أسس التجارة الاليكترونية الحديثة، وعلى الرغم من ضرورة حماية حقوق الأشخاص المعنية بالبيانات من تبعات التسويق الإليكتروني، ولكن هذا لا يعني شلل النظم المتعارف عليها في المعاملات التجارية

أ: أليات عدم الاعتراض في القانون:

ولهذا جاء القانون في المادتين (١٧ و١٨) ليضع إطاراً تشريعياً متوازناً يجمع بين حماية خصوصية الأفراد ودعم حاجات السوق. فبينما اشترط القانون الموافقة كأصل عام، فإنه فتح متسعاً تشغيلياً مرناً في المادة (١٨ / بند ٢) حين ألزم المُرسل بالاحتفاظ بسجلات إلكترونية تُثبت: «موافقة الشخص المعني بالبيانات وتعديلاتها، أو عدم اعتراضه على استمراره»، وهو ما يعرف ب (عدم الاعتراض - Opt-out / Soft Opt-in)، وهو ما يتفق مع المعايير التجارية والدولية التي تمنح القدرة على التواصل مع عملائها الحاليين لتسويق منتجات أو خدمات مشابهة للخدمات التي يهتم بها العميل استناداً إلى تلك العلاقة، شريطة توفير آلية واضحة ويسيرة تمكن العميل من «الاعتراض» أو إلغاء الاشتراك متى أراد، دون الحاجة لافتعال إجراءات معقدة لاستصدار «موافقة صريحة مسبقة» على كل رسالة تسويقية

ب: الاقتصار على الموافقة الصريحة لأغراض التسويق الاليكتروني المباشر في اللائحة التنفيذية

إلا أن اللائحة التنفيذية، قد اقتصرت في مادتها (١٨) على شرط الموافقة الصريحة كشرط لمشروعية التسويق الإلكتروني المباشر، حيث نصت على: «أن يكون قد حصل على موافقة صريحة من الشخص المعني بالبيانات على تلقي الاتصال التسويقي». وامتد هذا التضييق إلى هندسة حقوق الشخص المعني، حيث أسست اللائحة آليات المحو ووقف الإرسال حصرياً على حالة: «عدول الشخص المعنى بالبيانات عن موافقته»

رابعا: تغيير التنظيم القانوني لمهنة مسؤول حماية البيانات الشخصية:

تعتبر مهنة مسؤول حماية البيانات الشخصية عصب الامتثال في أي قانون ونظام يتبع النظام الأوروبي لحماية البيانات الشخصية، وعليه فقد نجم عن هذا اطار متطور وناضج حول للعالم يحكم جميع أجزاء هذه الوظيفة -مع اختلافات بسيطة في تفاصيل تنفيذ هذا الاطار بين النظم الوطنية- ابتداء من التدريب انتهاء بالعلاقة بين المسئول والمتحكم أو المعالج وكيفية انتهاؤها وضوابطها

وقد تناولنا سابقا الحوار المتعلق بهذا التنظيم والراجع للقانون، ولكن يلحظ أن اللائحة من ناحية قد حاولت اصلاح بعض سهو القانون من ناحية وخالفت القانون في العديد من الأحكام والتفسير من ناحية أخرى، مما نجم عنه عدم توافقية بين اللائحة والقانون فيمات يتعلق بتنظيم مهنة «مسئول حماية البيانات الشخصية» كالآتي

أ: ما حاولت اللائحة إصلاحه:

نتيجة صمت القانون عن توفير ضمانات لمسئول حماية البيانات الشخصية، حاولت اللائحة أن تسد هذا الصمت التشريعي بوضعها اليات لهذه الضمانات في اشتراطات التراخيص، حيث نصت المادة (٢١) من اللائحة والخاصة ب (شروط ترخيص / تصريح المتحكم و المعالج من الأشخاص الاعتبارية للبيانات الشخصية و البيانات الشخصية الحساسة) على الآتي: (٥- تقديم سند العلاقة التعاقدية مع مسئول حماية البيانات الشخصية والمتضمنة صراحة قبوله تحمل مسئوليات مسئول حماية البيانات الشخصية ، وما يفيد التزام المتحكم أو المعالج بمنح مسئول حماية البيانات الشخصية الاستقلالية في تنفيذ مهامه بالقدر الذي يسمح له القيام بها .)، ويلاحظ بتحليل هذا النص الآتي

١. الاستعاضة بالضمانة التعاقدية عن الضمانات التشريعية:

إن محاولة اللائحة فرض «الاستقلالية» كشرط للحصول على الترخيص عبر (سند العلاقة التعاقدية) يُمثل التفافاً إجرائياً به ذكاء ولكنه يجابه مساءلة الحوار التشريعي والخروج عن أصول تدرج القاعدة القانونية، فمن ناحية فهو جعل الاستقلالية رهنا بتفسير العقد ومنازعاته من ناحية، ومن ناحية أخرى تجاوز النص القانون الأصلي الخالي من تلك الضمانات (وهو ليس اختصاص اللائحة بإصلاح الحوار التشريعي)

٢. تقييد الاستقلالية بعبارات مطاطة تُفرغها من مضمونها (Diluted Independence):

على الرغم من محاولة اللائحة لسد الفراغ التشريعي وتأسيس اتفاق مع القواعد المستقرة فيما يتعلق بضمانات المسئول، فقد شابت محاولتها تلك عوار في الصياغة وقصور في الضمانات، حيث نصت على الآتي: "بالقدر الذي يسمح له القيام بها". هذا التقييد اللفظي يتعارض المعيار العالمي لـ (الاستقلالية التامة - Complete Independence)، كونه يمنح الإدارة التنفيذية للكيان الذي يعمل به المسئول سلطة تقديرية واسعة ومبهمة لتحديد حجم ونطاق هذه الاستقلالية؛ مما يفتح باباً للتدخل الإداري المقنع وتقليص صلاحيات المسؤول بحجة أن ما مُنح له "يكفي" من وجهة نظر الإدارة.

٣. الاصطدام بمبدأ تدرج القواعد القانونية (Hierarchy of Norms) وغياب التفويض التشريعي:

بمقارنة هذا المسلك مع المعايير الإقليمية، نجد أن النظام السعودي تضمن «تفويضاً تشريعياً» واسعاً للائحة بتنظيم أحكام المسئول[٣٩]، في حين أسس القانون البحريني لمبدأ الاستقلالية صراحة في متنه وأحال تفصيله لقرار تنفيذي[٤٠]. أما القانون المصري، فقد جاء خالياً من المبدأ ومن التفويض معاً. وعليه، فإن اللائحة (كأداة تشريعية أدنى) لا تملك دستورياً خلق مركز قانوني جديد يقيد سلطة صاحب العمل المكتسبة بموجب «قانون العمل» في توقيع الجزاءات أو العزل، مما يجعل هذه المحاولة اللائحية مشوبة بعيب تجاوز حدود السلطة (Ultra Vires)، وخاصة مع صمت قانون حماية البيانات الشخصية فيما يتعلق هذا وهو كان هنا سيعامل معاملة القانون الخاص الذي يقيد العام

٤. الأثر العملي وزعزعة استقرار المراكز القانونية:

من الملاحظ هنا بداية ظهور اثار استعمال اللائحة للتراخيص كأداة اكراه إدارية لتحقيق أغراض تتجاوز النص القانوني وحدوده، فقد استعملت اللائحة الرخصة وخاصة في ظل صلاحيات المركز الكبيرة في ما يتعلق بمنح الرخص -وهي ما فصلناه سابقا وارجعناه للتنظيم القانوني ذاته- كأداة لفرض التزامات وأحكام على طالبي التراخيص، بشكل يتجاوز المبادئ الدستورية الأساسية، ويطرح مسالة عدم المشروعية محل اعتبار كبير، وهو ما يمكن ترجمته على الصعيد العملي في تسلسل من النزاعات القضائية وتزعزع المراكز القانونية، كالآتي

أولاً: النزاع الإداري (طعون حجب التراخيص): في حال امتناع الكيان عن إدراج «بند الاستقلالية» لغياب سنده في القانون الأصلي، وقوبل برفض المركز لمنحه الترخيص؛ يُطرح الطعن أمام مجلس الدولة بعدم المشروعية على هذا البند في اللائحة كسيناريو قابل للتحقق بقوة

---

٣٩ نظام حماية البيانات الشخصية بالمملكة العربية السعودية (الصادر بالمرسوم الملكي رقم م/١٩ وتاريخ ١٤٤٣/٢/٩هـ وتعديلاته)، المادة (٣٠)

٤٠ قانون رقم (٣٠) لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية بمملكة البحرين، المادة (٤١/ج)

ثانياً: النزاع العمالي (الدفع ببطلان العقد للإكراه الإداري): في حال رضوخ الكيان وإبرام العقد متضمناً شرط الاستقالالية كمسوغ إجباري للترخيص، ثم قيامه لاحقاً بعزل المسئول، وقيام المسئول برفع قضية مدنية أو عمالية على الكيان؛ فإن الكيان قد يستعمل آلية الإكراه الإداري غير المشروعة هذه كدفع لإبطال شرط الاستقالالية في العقد

ب: ما اضافته اللائحة وخالفت به القانون:

ورغم سعي اللائحة التنفيذية لإيجاد توازن بين الالتزامات والضمانات الخاصة بـ ‹مسئول حماية البيانات الشخصية›، يُلاحظ تعارض اللائحة مع النص القانوني فيما يتعلق بباقي تنظيم هذه المهنة -وهو ما يمكن في جزء كبير منها ارجاعه لتوسع اللائحة الملحوظ في اختصاصات ‹مركز حماية البيانات الشخصية› بما يتجاوز النطاق الذي رسمه القانون كما سيُفصل لاحقا -، ويمكن رصد تلك التعارضات كالاتي

1: مركزية آليات التأهيل والاعتماد:

تبنت اللائحة التنفيذية في مادتها السابعة مساراً شديد المركزية فيما يتعلق بقيد وتأهيل واعتماد مسئولي حماية البيانات الشخصية؛ حيث احتكر المركز المراحل الثلاث الحاكمة لمسار المهنة (التأهيل، والاعتماد، والقيد)، مما يمنحه ابتداءً سلطة هيمنة واسعة على المسئولين منذ الخطوة الأولى في مسارهم الوظيفي

ورغم الوجاهة التنظيمية لاشتراط التأهيل والقيد لضمان الكفاءة، إلا أن المقاربة اللائحية قد فرضت هندسة شديدة المركزية تنفرد بها وتُجافي النماذج الدولية الرائدة. فالممارسات الفضلى تتجه نحو نهج مرن و»لامركزي» يعزز ديناميكية السوق؛ إما من خلال اعتماد مناهج تأهيلية استرشادية مع ترك عبء الامتثال للمسئولية اللاحقة (كالنموذج الأسترالي)[٤١]، أو عبر تصميم هيكل تدريبي تتولى فيه جهات مستقلة مختصة مهام الاختبار والاعتماد (كالنموذج الإسباني)[٤٢]، أو من خلال بناء شراكات استراتيجية واعتمادات خارجية (كالنموذج السعودي)[٤٣]. إن تبني هذا النهج اللامركزي من شأنه أن يُرسي مبادئ الشفافية، ويُشجع على خلق سوق مؤسسية وتنافسية لعمليات التدريب قادرة على استيعاب الاحتياج المتنامي للكوادر، فضلاً عن أنه يُعزز من هيبة المركز الرقابية كـ «سلطة إشراف لاحقة» تتنزه عن شبهات السيطرة المركزية المُسبقة التي تعيق تطور واستقلالية المهنة

---

٤١ النموذج الأسترالي (الامتثال الاسترشادي): يتبنى مكتب مفوض المعلومات الأسترالي (OAIC) أسلوب التوجيه الرقابي؛ حيث يُصدر «إطار عمل إدارة الخصوصية» (Privacy Management Framework) والأدلة الإرشادية التي تُعين الكيانات على تأهيل مسؤولي الخصوصية داخلياً، دون فرض اختبارات حكومية مركزية، تاركاً عبء إثبات كفاءة المسئول لمدى التزام الكيان الفعلي بمبادئ الخصوصية (APPs) عند التفتيش اللاحق. (يُراجع الموقع الرسمي للمكتب: www.oaic.gov.au).

٤٢ النموذج الإسباني (الاعتماد المستقل): أطلقت الوكالة الإسبانية لحماية البيانات (AEPD) مخططاً مرجعياً يُعرف بـ (Esquema AEPD-DPD). وبموجب هذا المخطط، تكتفي الوكالة بوضع المعايير الفنية، بينما تتولى الهيئة الوطنية للاعتماد (ENAC) اعتماد جهات تصديق خارجية مستقلة (Certification Entities) لتقوم هي بتدريب واختبار مسئولي حماية البيانات، مما يمنع احتكار السلطة الرقابية ويضمن حيادية التقييم. (تُراجع تفاصيل المخطط على موقع الوكالة: www.aepd.es).

٤٣ النموذج السعودي (الشراكات الاستراتيجية): يعتمد نظام حماية البيانات الشخصية السعودي، وتوجهات الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) ممثلة في مكتب إدارة البيانات الوطنية (NDMO)، على استراتيجية «بناء القدرات الوطنية»؛ وذلك من خلال عقد الشراكات مع الجامعات ومعهد الإدارة العامة والجهات المتخصصة لتقديم برامج تدريبية وتأهيلية معتمدة، دون أن ينص النظام أو لائحته على احتكار الهيئة لعقد اختبارات إلزامية بمقابل مادي كشرط وحيد لممارسة المهنة. (يُراجع موقع الهيئة: www.sdaia.gov.sa).

2: التوسع في صلاحيات المركز وسلطاته اتجاه مسئولي حماية البيانات الشخصية:

جاءت اللائحة التنفيذية في مادتها العاشرة لتنص على أنه: (وللمركز إيقاف مسئول حماية البيانات الشخصية المقيد وطلب تغييره، حال إخلاله بأي من شروط القيد، وعلى الممثل القانوني في هذه الحالة قيد مسئول حماية بيانات شخصية بديل مؤقت... لحين تعيين مسئول دائم في مدة يتم تحديدها من قِبل المركز)

ويُمثل هذا الاتجاه التنظيمي تجاوزاً وتوسعاً في صلاحيات المركز لم يرد في قانون حماية البيانات الشخصية، ولم تعهده النظم القانونية المقارنة، كما انه أيضا بافتراض -جدلا- وجود مسوغ قانوني لهذه السلطة فإنه طبقا لضمانات التأديب والمساءلة الإدارية، فإن المركز -كجهة الرقابة الإدارية- لا يملك أن يُوقع جزاء الإيقاف أو يُلغي قيد المسئول بقرار تحكمي، دون إرساء قواعد إجرائية واضحة تكفل ضمانات التأديب والتحقيق (والتي تنتظم وجوباً في مسار متصل يبدأ بإخطار المسئول صراحةً بطبيعة المخالفة المنسوبة إليه، ومروراً بتمكينه من حق الدفاع والمواجهة أمام جهة تحقيق محايدة، مع التزام الإدارة بمبدأ تدرج الجزاء ليتناسب طردياً مع جسامة الإخلال، وانتهاءً بكفالة حقه الأصيل في التظلم والطعن على القرار)، وهو الإطار الإجرائي الذي خلت منه نصوص القانون واللائحة التنفيذية خلواً تماماً

كما أن إذا ما اقترن هذا التوسع بمجمل التنظيم اللائحي لمهنة مسئولي حماية البيانات الشخصية، فإنه يكشف عن توجه نحو تحويل دور هؤلاء المسئولين من (مستشاري امتثال داخليين) إلى ما يُشبه (التابعين الإداريين) للمركز الرقابي، وهو تحول هيكلي من شأنه أن يُربك علاقتهم المؤسسية، ويهدم جدار الثقة مع الكيان الذي يعملون فيه

3: تغيير في فلسفة الوصف الوظيفي لالتزامات المسئول عن حماية البيانات الشخصية:

يظهر الاتجاه القائم على إعطاء مركز حماية البيانات الشخصية دورا أكبر فيما يتعلق بمسئولي حماية البيانات الشخصية في تكييف اللائحة لماهية رفع التقارير المذكورة في القانون والتي ذكرنا انها موجهة من المسئول للإدارة العليا، وفي خطوة لاحقة ابلاغ من المسئول للمركز حال عدم استجابة الإدارة العليا لكيان المتحكم أو المعالج لتقرير المسئول

وفي تغيير لهذا الترتيب فسر التقرير أنه من المسؤول للمركز مباشرة وهو ما جاء في البند الأول من المادة الثانية عشر من اللائحة والذي نص على (١- مراقبة تطبيق السياسات التأمينية الصادرة عن المركز والخاصة بتأمين عملية المعالجة والحفظ والتداول وتقديم تقرير سنوي للمركز بحالة حماية الخصوصية عند المتحكم أو المعالج أو عند طلب ذلك)، وهو ما يتعارض مع النص القانوني في المادة التاسعة من القانون والتي نصت على (٢ – العمل كنقطة اتصال مباشرة مع المركز وتنفيذ قراراته، فيما يخص تطبيق أحكام هذا القانون.)

وبجمع هذا مع سلطة المركز في الغاء القيد بشكل مباشر، فنجد أن اللائحة تخلق عبء إضافي -بجوار التنظيم المتشدد للقانون واللائحة لمهنة المسؤول، مما يزيد التأثير السلبي على العلاقة بين المسؤول والكيان الذي يعمل به

4: قصر الالتزام القانوني لمسئول حماية البيانات (DPO) على (تأمين البيانات):

في إكمال لتحليل التوصيف الذي أتى في اللائحة لمسئول حماية البيانات الشخصية، نجد تأثراً واضحاً في رؤية اللائحة وواضعها لماهية حماية البيانات الشخصية عامة، وهو الأثر المتناثر في كافة أركان اللائحة من ناحية التركيز على (التأمين والحماية) و(السرية)، والتي على الرغم من أهميتها البالغة كأحد

أهم الالتزامات والحقوق المنصوص عليها في القانون ونظم حماية البيانات الشخصية عامة، إلا أنها لا تتعدى جزءاً من كل، لا يمكن التركيز عليها بدون تجاهل توازنها مع منظومة الحماية عامة

ويتبدى هذا الأثر هنا في جزئية أساسية، وهي نص اللائحة في المادة الثانية عشرة على التزام مسئول حماية البيانات الشخصية بـ: (١- مراقبة تطبيق السياسات التأمينية الصادرة عن المركز والخاصة بتأمين عملية المعالجة والحفظ والتداول وتقديم تقرير سنوي للمركز بحالة حماية الخصوصية عند المتحكم أو المعالج أو عند طلب ذلك)، وهو ما يخالف ما جاء في القانون في المادة التاسعة الخاصة بالتزامات مسئول حماية البيانات الشخصية في البند الأول أيضاً، والتي نصت على: «١ – إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها». فنلاحظ هنا الفارق بين النص القانوني والنص اللائحي من حيث كلمة (مراقبة تطبيق السياسات التأمينية الصادرة عن المركز والخاصة بتأمين عملية المعالجة والحفظ والتداول) و (إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها)

وهو ما يعني إما أن:

- هذا التزام آخر يُضاف على مهام المسئول الموجودة في القانون، ويتعلق فقط بنظم الحماية والتأمين الصادرة من المركز -وهي نقطة خلاف في حد ذاتها- وهو ما قد ينجم عنه تعارض وظيفي بين مهام المسئول كمراقب لنظم الحماية ومهن الأمن السيبراني داخل المؤسسات، والتي يُفترض انعزالهم عن بعض؛ حيث إن مسئول حماية البيانات الشخصية يراقب عمل مسئولي التأمين السيبراني فيما يتعلق بحماية البيانات الشخصية.
- أن اللائحة قصرت ما نُص عليه قانوناً بنظم حماية البيانات الشخصية على نظم تأمين البيانات، وهو قصور في رؤية ماهية حماية البيانات الشخصية وأيضاً دور مسئول حماية البيانات الشخصية كمسئول امتثال لحماية البيانات الشخصية داخل المؤسسة، لا موظف أمن سيبراني والذي تقتصر مهامه على الجوانب التقنية البحتة المطابقة لوظيفة (مسئول الأمن السيبراني CISO)، مُتجاهلاً المهام القانونية والإدارية الجوهرية للـ DPO، مثل إجراء تقييمات الأثر (DPIA)، وإدارة سجلات المعالجة، ونشر ثقافة الخصوصية؛ وهو ما يعكس قصوراً في استيعاب التميز النوعي لهذه المهنة المستحدثة.

5: تحميله بالتزامات مراكز قانونية أخرى:

يُظهر التحليل الموضوعي للمادة (١٢) من اللائحة التنفيذية وجود تداخل تنظيمي بين الالتزامات الواقعة على الكيان (المتحكم أو المعالج) والالتزامات الواقعة على مسئول حماية البيانات الشخصية، فضلاً عن وجود تعارض نَصي داخلي في تحديد مهام الوظيفة

فمن جهة، نصت المادة (١٢/بند ٤) على التزام المسئول بـ (عدم تعارض مهامه مع أي تكليفات أخرى من شأنها الإضرار بحماية البيانات الشخصية). غير أن التزام «منع تعارض المهام» يُعد من الناحية القانونية والإدارية التزاماً مؤسسياً يقع على عاتق الإدارة العليا (المتحكم أو المعالج) المعنية بتصميم الهيكل التنظيمي للكيان، وليس على الموظف الذي يخضع لمبدأ التبعية الإدارية ولا يملك سلطة الانفراد بتحديد مهامه الوظيفية أو رفض التكليفات الإدارية. ويتسق هذا المبدأ مع المعايير الدولية، وتحديداً اللائحة العامة لحماية البيانات (GDPR)، والتي ألزمت صراحةً (المتحكم أو المعالج) بضمان عدم أداء المسئول لمهام تؤدي إلى تضارب المصالح[٤٤].

ومن جهة أخرى، يبرز تعارض داخلي في نصوص اللائحة ذاتها؛ ففي حين يحظر البند (٤) من المادة (١٢) تعارض المهام، نجد أن البند (١) من المادة ذاتها قد أسند لمسئول حماية البيانات مهاماً ذات طبيعة تنفيذية وتأمينية تتمثل في (مراقبة وتطبيق السياسات التأمينية). ووفقاً للأدبيات التوجيهية في حوكمة البيانات، فإن الجمع بين المهام التنفيذية للأمن السيبراني أو تقنية المعلومات (IT/CISO) وبين مهام

٤٤ gdpr, article ٦)٣٨): «The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.»

الرقابة والامتثال لحماية البيانات (DPO) يُعد تطبيقاً صريحاً لتعارض المصالح؛ نظراً لعدم جواز تولي ذات الشخص لمهام التنفيذ والتدقيق المستقل عليها في آن واحد[٤٥]>

وبناءً على هذه الصياغة، تنشأ صعوبة عملية وقانونية في الامتثال؛ إذ يؤدي التزام المسؤول بمهام التأمين الواردة في البند (١) إلى وقوعه موضوعياً في حالة التعارض المحظورة بموجب البند (٤). ويُعد إلقاء عبء معالجة هذا الخلل التنظيمي وتجنب التضارب على كاهل المسؤول خروجاً عن القواعد المستقرة لتوزيع المسؤوليات في هياكل الحوكمة المؤسسية

خامسا: التوسع في صلاحيات المركز وتقرير سلطة الغرامات الإدارية للمركز:

رغم تضمن قانون حماية البيانات الشخصية تنظيماً واضحاً ومحدداً للجزاءات المالية والعقوبات المرتبطة بمخالفة أحكامه، يُلاحظ أن اللائحة التنفيذية قد اتجهت نحو استحداث مسار موازٍ لتوسيع سلطة «المركز» العقابية من بوابة «التراخيص»، وهذا من خلال استعمال «التراخيص والتصاريح» مصحوبة بسلطة المركز القانونية الموسعة لقبول أو رفض الطلبات بدون آليات مراجعة وتظلم واضحة

كما تضمن القانون أيضاً مساراً خاصاً بجزاءات إدارية يختص بها المركز؛ حيث خولت المادة (٢٩) المركز سلطة إلغاء الترخيص أو التصريح أو الاعتماد في عدة حالات، أبرزها: مخالفة شروط الترخيص، أو عدم سداد رسوم التجديد، أو تكرار عدم الامتثال لقرارات المركز، أو التنازل للغير دون موافقة، أو صدور حكم بإفلاس المتحكم أو المعالج

ويكتمل هذا المسار من الجزاءات الإدارية بما قررته المادة (٣٠) من القانون، والتي منحت الرئيس التنفيذي للمركز سلطة توجيه إنذار للمخالف للتوقف عن المخالفة وإزالة أسبابها خلال فترة زمنية محددة. وفي حال انقضاء المدة دون تنفيذ، يثبت لمجلس إدارة المركز صلاحية إصدار قرارات مسببة تتدرج في حدتها لتشمل: الإنذار بالإيقاف (الجزئي أو الكلي)، أو الإيقاف الفعلي، أو سحب الترخيص وإلغائه. وتجاوزت هذه الجزاءات الإدارية حدود التراخيص لتشمل تدابير أخرى ذات أثر مالي ومعنوي مباشر على الكيانات؛ حيث يحق للمركز نشر بيان بالمخالفات في وسائل الإعلام واسعة الانتشار على نفقة المخالف، فضلاً عن سلطة إخضاع المتحكم أو المعالج للإشراف الفني المباشر من قِبل المركز لتأمين البيانات، ويكون ذلك أيضاً على نفقة الجهة المخالفة

وعلى الرغم من هذا التأسيس القانوني لصلاحيات واسعة -وإن كانت متناسبة ولازمة- في صلاحيات المركز -دون تنظيمه وسنه لآلية تظلم واضحة-، فقد جاءت اللائحة بتوسع أكبر لسلطات المركز، من خلال اشتراطها في مادتها (٢١) الخاصة بتراخيص الأشخاص الاعتبارية، تقديم (إقرار بالالتزام بالجزاءات المالية التي يقرها المركز حال مخالفة شروط الترخيص أو التصريح)، وتزايد هذا التوسع اللائحي بشكل لافت وخطير في المادة (٤١) ضمن نماذج التراخيص، والتي اشترطت (إقرار بالوفاء بالجزاءات المالية والتعويضات التي يقرها المركز)

ويُمثل هذا المسلك تجاوزاً وتوسعاً غير مشروع في صلاحيات المركز بشكل لم ينص عليه القانون؛ يتجاوز القواعد العامة للقانون متمثلاً في الآتي

- تجاوزه لقواعد المشروعية والإحالة التشريعية والاختصاص والمبدأ الدستوري (لا جريمة ولا عقوبة إلا بنص قانوني)، حيث لم ينص القانون على إعطاء المركز سواء مجلس إدارته أو رئيسه التنفيذي سلطات الجزاءات المالية أو فرض تعويضات، وهو ما يصم اللائحة بعيب عدم الدستورية.
- مخالفته لقواعد الفصل بين السلطات، حيث نصت اللائحة على سلطة المركز وهو جهة إدارية لتقرير «غرامات مالية»، وأيضاً تقرير «تعويضات»، وهو تعدٍ و(غصب للسلطة)

٤٥ article ٢٩ Data Protection Working Party, Guidelines on Data Protection Officers (‹DPOs›), WP ٢٤٣ rev.٠١ (Adopted on ١٣ December ٢٠١٦, as last revised and adopted on ٥ April ٢٠١٧), p. ٢١ (Section: Conflict of Interests).

الأصيلة والدستورية للسلطة القضائية صاحبة الاختصاص بموجب (أحكام المسئولية التقصيرية في القانون المدني).

- عدم تحديد ماهية التعويضات ولا آلياتها ولا المخالفة المتعلقة بها، وهل هي مختلفة عن «الغرامات»، وهل هي متعلقة مثلاً بتظلمات الأفراد عن انتهاك حقوقهم، وكيف هذا واللائحة خلت تماماً من أي تنظيم لآليات التظلم والفصل فيها، وأيضاً هل هي تختلف أو تغني -وهو لا يجوز- عن الحق في التعويض القضائي المرتبط بالضرر المنصوص عليه في المادة الخامسة والثلاثين والتي تنص على حق المتضرر في التعويض.
- تحويله للتراخيص من أداة تنظيم إداري وتحقق مسبق لاشتراطات معينة ينص عليها القانون لتفادي أو تقليل الطبيعة الخطرة للنشاط، إلى أداة إذعان عقدية متمثلة في فرض التوقيع على إقرارات لم ينص عليها القانون وتتعلق باشتراطات وجزاءات لم ينص عليها القانون وتُربط لا بمخالفة القانون، بل بمخالفة شروط التراخيص.
- قواعد تحديد الجزاء، حيث إن اللائحة لم تضع قواعد معينة لتقدير تلك الجزاءات، سواء لحدها الأدنى أو الأقصى، أو تحديد جزاءات معينة لمخالفات معينة، بل جاءت في نصها عليها كإضافات معممة لنص يتكلم على عملية التراخيص.
- قواعد تناسب الجزاء، فاللائحة مع إضافتها لجزاءات قائمة على مخالفة شروط التراخيص -وهي موسعة للغاية كما سنشرح لاحقاً- على الجزاءات القائمة على مخالفة نصوص القانون ذاته، قد تخلق نوعاً من الجزاء المزدوج لنفس المخالفة بما يخل بقاعدة (عدم جواز معاقبة الشخص عن ذات الفعل مرتين)، أو سلطة تقديرية غير محددة قد تخلق نوعاً من عدم المساواة بين المراكز القانونية.
- خلقه لعدم تماثل قانوني بين المراكز القانونية المختلفة وإخلاله بمبدأ (المساواة أمام الأعباء العامة) نتيجة اقتصار تلك الغرامات على المرخص لهم فقط، دون غير المرخصين أو حتى المخالفين لأحكام القانون بالكلية، مما يخلق عبئاً على مركز قانوني ذي أفضلية نتيجة رغبته في الامتثال والترخيص، وهو ما يُقابل عادة بتسهيلات وحوافز تشجيعية لزيادة إقبال المخاطبين على الترخيص والتصريح.

فهذه الإضافة -غير المحمودة- لنص قانوني أسس لبنية متكاملة من الجزاءات ابتداءً من الجزاءات الإدارية والتي اختص بها المركز سلفاً، لجزاءات جنائية مالية وماسة بالحريات تختص بها السلطة القضائية -حسب قواعد المشروعية- حصراً بما يضمن أيضاً مشروعية إجراءات الجزاء من شفافية وحياد وطعن لاحق، وأيضاً تعويضات مدنية للمضرورين، لا يمكن تفسيرها طبقاً للقواعد المستقرة للعقوبات، وتلقي بظلال عدم المشروعية والتغول في استعمال السلطة بشكل جاد في أي جزاء أو إجراء يتخذه المركز مستقبلاً حيال المرخص لهم

سادسا: تغيير بنية الامتثال والمساءلة عبر التوسع في متطلبات التراخيص:

جاء قانون حماية البيانات الشخصية المصري ناصاً على منظومة من التراخيص والتصاريح تهدف إلى وضع إطار تنظيمي ورقابي لضبط حركة معالجة البيانات، لاسيما في الأنشطة ذات الطبيعة الخاصة كنقل البيانات عبر الحدود، أو التسويق الإلكتروني، أو التعامل على البيانات الحساسة، ولم يضع اطارا محددا أو صارما لآليات تنظيم تلك التراخيص، بل أحالها في معظمها للائحة التنفيذية

وبتحليل فلسفة القانون وهدفه من وضع معايير توافقية مع الأطر والقوانين المقارنة لحماية البيانات الشخصية، فقد هدف إلى تحقيق منظومة الامتثال اللاحق عن طريق اليات مثل مسؤول حماية البيانات الشخصية ومنصب جديد انفرد به ونص عليه يعرف باسم مستشار إجراءات حماية البيانات الشخصية، وهو ما لا يتحقق إلا بوضع اطر حاكمة عامة تضمن الحقوق وتحدد الالتزامات عامة مع ترك مساحة للمتحكم والمعالج في وضع وتحديد نظمه الداخلية للمعالجة والامتثال

وقد انتهجت اللائحة في تنظيمها لهذه البنية منهجاً قائماً على التدقيق والفحص لكل مراحل وتفاصيل البنية (الفنية) للمتحكم والمعالج، بشكل يحول عملية الترخيص لعملية اعتماد وتدقيق مسبق أثناء الترخيص. وهو في المُستقر عليه من قواعد حماية البيانات الشخصية، عملية منفصلة تماماً عن عملية الترخيص؛ حيث

تقوم جهة مستقلة بعملية فحص تشابه في إجراءاتها ما جاء في اللائحة التنفيذية[٤٦].

فقد تطلبت اللائحة في جميع موادها العديد من الاشتراطات والتفاصيل الفنية، مع الأخذ في الاعتبار ما جاء مسبقا من توسع اللائحة في الاحالات المستقبلية لقرارات إدارية تصدر من المركز لمعايير واشتراطات فنية وتأمينية غير واضحة المعالم حتى تاريخه

أما بالنسبة لمواد التراخيص واجراءاتها، فقد فصلت وطالبت اللائحة في مستندات واشتراطات التراخيص -وهي مركبة على بعضها البعض- مستندات وبيانات تتطلب شرحا وتفصيلا دقيقا لجميع دقائق بنية المعالجة، فمثلا اشترطت المادتان (٢١) و(٢٢) تقديم بيان تفصيلي مسبق بالآلية المستخدمة للحصول على موافقة الشخص المعني، وآليات ممارسة حقوقه. وتعمق هذا التدقيق في المادة (٣٠) الخاصة بالتسويق الإلكتروني عبر اشتراط تحديد آليات تمكين الشخص من رفض الاتصال أو العدول عن موافقته، وإلزامه بتقديم سجلات إلكترونية مسبقة بذلك

أما على الصعيد التقني والفني، فقد اشترطت المادة (٣٥) من اللائحة على مقدم التراخيص او التصاريح استيفاء كافة البيانات عن البنية التحتية، وتصنيف مركز البيانات، وأنواع الأجهزة المستخدمة، ومطابقتها الحرفية لاشتراطات المركز. وامتد هذا التدقيق للمادة (٢٤) باشتراط بيان نظم التأمين وأماكن التخزين المؤقتة والنهائية عند النقل عبر الحدود. ويكتمل هذا الطوق الرقابي بما فرضته المادة (٤١) من إقرارات إلكترونية ملزمة لمراجعة آليات محو وتعديل البيانات وسجلات الإفصاح

هذا التدقيق في المستندات والاشتراطات يقلب بنية الاجراء ليقارب بشدة حدود عملية الفحص والتدقيق والاعتماد الفنية فلا ينقصها إلا عملية الفحص الواقعي والتي جاءت اللائحة التنفيذية بمقابلها القانوني في المادة الواحدة والأربعون من خلال طلبها لمجموعة من الاقرارات التي يلتزم المرخص بها منها (٥- إقرار بالالتزامات الخاصة بأمن البيانات الشخصية)، وهو ما قد ينجم عنه ان يتحول الترخيص لدفاع ضد أي اجراء في حق المرخص له، حيث يتم تقديم الترخيص بما يتضمنه من موافقة على نقاط تفصيلية حال ليثبت المرخص أو المصرح له أنه امتثل لجميع المتطلبات القانونية المطلوبة منه -سواء كانت صحيحة أم خاطئة-، فمثلا في حالة وقوع ضرر نتيجة تسريب البيانات -دون حالات الاختراق- فيقدم المرخص أو المصرح له ما يفيد التزامه بقواعد تأمين البيانات والتزامه بسرية البيانات هو والمتعاملين معه، مما يخلق شبه استحالة قانونية أمام المضرور لإثبات «ركن الخطأ التقصيري» أو الانحراف عن معيار العناية الواجبة لكيان يعمل وفق منظومة دقيقة اعتمدتها السلطة الرقابية وصرحت بها مسبقاً

سابعاً: الاختلافات المتعلقة بتحديد المراكز القانونية والتزاماتها:

تتناثر في مواد اللائحة عددا من الاختلافات الدقيقة والتي تثير غموضا وتعارضا في تحديد المراكز القانونية المخاطبة من ناحية والتزاماتها من ناحية اخري، مما قد ينتج عنه تعارضا في الامتثال والمراقبة مما قد يفضي لجزاءات وغرامات وعقوبات بالمخالفة لأحكام القانون، أو صعوبة في الامتثال نتيجة تعارض تلك الالتزامات مع المستقر عالميا، ومنها

أ: استحداث مراكز قانونية غير منصوص عليها تشريعياً (الوسيط التسويقي):

تضمنت المادة (١٨) من اللائحة تنظيماً لمركز قانوني تحت مُسمى (الوسيط التسويقي)، وهو كيان لم يرد

٤٦ يعتبر الفارق هنا هو كمية التفاصيل المطلوبة في اللائحة التنفيذية، فالتراخيص عادة ما تطلب في إجراءاتها مجموعة من المستندات والأدلة
التي تدل على الاشتراطات العامة للتراخيص، أما عملية الاعتماد والتدقيق الفني فهي التي يطلب فيها ويتم فحص كامل النقاط التفصيلية للعمليات، للمزيد gdpr, article ٤٢, European Data Protection Board (EDPB), Guidelines ٢٠١٨/١ on certification and identifying certification criteria in accordance of the Regulation, Version ٤٣ and ٤٢ with Articles ٣,٠ (Adopted on ٤ June ٢٠١٩), p. ٦.

لـه تنظيم مقابل في نصوص القانون الأم. ويُثير هذا الاستحداث إشكاليات عميقة في هيكل المسؤولية؛ فقد نصت اللائحة في مادتها الثامنة عشرة الخاصة بالتسويق الإلكتروني المباشر على مركز قانوني لم يُنص عليه في القانون وهو «الوسيط التسويقي»، وتعاملت معه كمركز قانوني منفرد عن المتحكم والمعالج. فقد نصت المادة الثامنة عشرة على: «٣- على المتحكم أو المعالج أو الوسيط التسويقي محو البيانات الشخصية في الحالتين الآتيتين:»، و «٣- يتعين على المرسل، حال كونه وسيطاً تسويقياً، التأكد من حصول المتحكم أو المعالج على...»، وهو ما ينجم عنه عدد من النتائج، كالآتي

- مخالفة التكييف القانوني والفقهي السليم لهذا المركز: حيث إنه ببساطة «معالج بيانات» لأغراض التسويق الإلكتروني، وهو ما يكشف عن نظرة قاصرة من واضعي اللائحة للمعالج بأنه كيان تقني صرف، وليس كياناً تشغيلياً أو أي كيان يقوم بأي نوع من أنواع العمليات على البيانات الشخصية لصالح المتحكم.
- استحداث مركز قانوني غير ممثل في بقية مواد القانون واللائحة: يخلق هذا الاستحداث ثقباً أسودَ في بيئة «التسويق الإلكتروني المباشر»؛ فما هي التزامات هذا «الوسيط التسويقي» غير التأكد من موافقة الشخص المعني على استعمال بياناته لأغراض التسويق الإلكتروني المباشر، وأيضاً الاحتفاظ بمصدر الحصول على البيانات الشخصية وكذا محو البيانات الشخصية؟ فهل هو ملتزم بالحصول على ترخيص أو تصريح؟ وكيف نُفرق بينه وبين المعالج؟ وأيضاً ماذا عن التزامات التصحيح والتأمين والاقتصار على الغرض؟ وماذا عن التزاماته تجاه حقوق الشخص المعني بالبيانات؟
- نقل عبء تدقيق مشروعية المعالجة: يؤدي هذا النص إلى نقل عبء تدقيق المشروعية إلى الكيان المُنفذ (الوسيط) تجاه الكيان الأصيل (المتحكم). هذا التوجه يُربك تطبيق مبدأ «المساءلة» (Accountability) المُلقى بالأساس على عاتق المتحكم.

ب: تداخل المراكز القانونية واضطراب التزامات (المتحكم) و(المعالج):

تكشف المقارنة الدقيقة بين نصوص القانون واللائحة عن وجود تداخل صريح في الالتزامات يُخل بالتمايز الفقهي والعملي بين المركز القانوني للمتحكم والمركز القانوني للمعالج، فضلاً عن بتر اللائحة لبعض الضمانات الجوهرية، ويتجلى ذلك في المظاهر الآتية

- مخالفة الطبيعة الفنية لسجل المعالج: ما نصت عليه اللائحة (في المادة ٤) والتي ألزمت المعالج في سجلاته بقيد (فئات البيانات الشخصية) بدلاً من (فئات المعالجة) كما نص القانون (مادة ٥/بند ٩)؛ وهو تناقض جوهري يعكس عدم إلمام بطبيعة دور المعالج الفني الذي يُعنى بنوع «العملية» (كالتشفير مثلاً) وليس بنوع «البيانات».
- نقل اختصاصات وأعباء «المتحكم» إلى «المعالج»:
  - في النقل عبر الحدود: في خلط إجرائي آخر، نقلت اللائحة عبء الالتزام بقيد (بيانات النقل عبر الحدود) إلى سجل المعالج، رغم أن القانون نص عليها صراحة ضمن التزامات المتحكم (مادة ٤) كونه صاحب القرار الأصيل.
  - في الإخطار والشفافية: كما نصت اللائحة أيضاً في المادة الرابعة (البند الثاني) الخاصة بالتزامات «المعالج» -مُغفلةً ذلك في المادة الثالثة الخاصة بالتزامات «المتحكم»- على التزام المعالج بتقديم: «ما يفيد إخطار المتحكم والشخص المعني بالبيانات وكل ذي صفة بالمدة اللازمة للمعالجة». وهو التزام يقع بالضرورة وبطبيعة الحال على عاتق «المتحكم» وليس «المعالج»؛ حيث تُفترض الطبيعة الفنية والمحايدة لدور المعالج، وعدم وجود صلة أو اتصال مباشر بينه وبين الشخص المعني بالبيانات. بل يُفترض في العديد من الأحوال -إعمالاً لمبدأ تقليل البيانات- ألا يعرف المعالج هوية الشخص المعني ولا يقوم بالتواصل معه. كما يتجاهل هذا النص أسس السوق القائمة على تعدد المعالجين لمتحكم واحد، وتعدد المتحكمين لمعالج واحد؛ مما سيُلقي بعبء تشغيلي ضخم على المعالج من ناحية، ويُغرق الشخص المعني بالبيانات بإخطارات من جهات وكيانات لا يعرفها، ولا يُفترض وجود رابطة قانونية تجمعه بها من ناحية أخرى.
- بتر التزامات المعالجة والتعليمات المكتوبة: أسقطت اللائحة في التزامات المتحكم (مادة ٣) ما نص عليه القانون في المادة (٤/بند ٣) من حقه في «وضع طريقة وأسلوب ومعايير

المعالجة»، وهو إهدار لمبدأ (المسؤولية الذاتية). كما أغفلت في التزامات المعالج (مادة ٤) شرط العمل بناءً على «تعليمات مكتوبة» من المتحكم (المادة ٥ قانون)، مكتفية بالإشارة للالتزام بالغرض.

- إغفال التزامات الإفصاح وحظر الإتاحة: أسقطت اللائحة التزام (المتحكم) بأن يتضمن سجله «تحديد من سيفصح لهم عن البيانات وسند ذلك» (المادة ٤/بند ٩ قانون). الأخطر من ذلك، أنها أغفلت النص صراحة على التزام المتحكم والمعالج بـ «الامتناع عن إتاحة البيانات إلا في الأحوال المصرح بها»، مكتفيةً بالإشارة القاصرة إلى «سرية العاملين»، وهو ما لا يغطي كافة صور الإتاحة غير المشروعة.

المطلب الثاني

الكفاية التنظيمية والجاهزية للإنفاذ

يُعد مبدأ «الكفاية التنظيمية» حجر الزاوية في تقييم مدى جاهزية التشريعات الفرعية للانتقال من حيز التنظير إلى حيز الإنفاذ الفعلي. وفي هذا المطلب، سنُخضع اللائحة التنفيذية لتحليل هيكلي دقيق؛ لاختبار مدى التزامها وتغطيتها للإحالات التشريعية والتفويضات التي أوردها القانون الأم. ولا يقتصر هذا التقييم على مجرد المطابقة النصية، بل يمتد لقياس الأثر العملي والمؤسسي لهذه الإحالات على جاهزية المنظومة القانونية لمرحلة الامتثال، وتداعيات ذلك على استقرار السوق الرقمي والمراكز القانونية للأطراف الفاعلة

ولتحقيق هذا التقييم الموضوعي والمحايد، سيتم تفكيك هذه الإشكالية ودراستها من خلال خمسة محاور بحثية متكاملة، كالآتي

أولاً: قياس مدى استيفاء اللائحة التنفيذية للتفويضات والإحالات الصادرة عن التشريع الأصلي.

ثانياً: التكييف القانوني لنهج «الإحالات المركبة» واختبار مدى مشروعيته الدستورية والتنظيمية في صياغة اللوائح

ثالثاً: الفحص النقدي للبنية اللغوية والاصطلاحية للنص اللائحي لاختبار مدى انضباط الصياغة ودقتها التشريعية

رابعاً: دراسة انعكاسات الإحالات التشريعية الممتدة على مبدأ الشفافية واستقرار التنظيم القانوني والمراكز المستقرة

خامساً: التقييم الموضوعي للتوجهات التنظيمية المفترضة في اللائحة، ومساءلة مدى ضرورتها التشريعية والعملية

أولا: تقييم ايفاء اللائحة بالإحالات:

أ: تقييم التطابق المبدئي للإحالات:

أحال قانون حماية البيانات الشخصية المصري خمسة عشر موضوعاً —وردت في ثمانية عشر موضعاً نصياً ضمن مواده— إلى اللائحة التنفيذية لتتولى تنظيمها. وتُمثل هذه المواضيع العصب الحقيقي والركيزة الأساسية لجعل القانون قابلاً للإنفاذ العملي، ويُمكن حصرها وتصنيفها موضوعياً على النحو الآتي

١. تنظيم دورة حياة البيانات والمراكز القانونية:

أ. المعالجة والتأمين: تحديد السياسات والإجراءات والضوابط والمعايير القياسية لدورة حياة البيانات من جمع، ومعالجة، وحفظ، وتأمين (المادة ٣).

ب. المتحكم والمعالج: تفصيل الالتزامات الفنية والقانونية لمركزي «المتحكم» و«المعالج»، بالإضافة إلى رسم آليات وإجراءات تعيين ممثليهم القانونيين داخل الجمهورية حال وجودهم بالخارج (المادتان ٤ و٥).

٢. تأسيس هيكل الامتثال والرقابة والأدلة:

أ. مسئول حماية البيانات (DPO): رسم الهيكل الرقابي الداخلي للكيانات عبر تحديد شروط القيد في سجل مسئولي حماية البيانات، وتفصيل التزاماتهم ومهامهم (المادتان ٨ و٩).

ب. إدارة الحوادث السيبرانية: وضع الإجراءات التفصيلية الخاصة بالإبلاغ والإخطار عن الخروقات الأمنية وانتهاك البيانات (المادة ٧).

ج. الإثبات الجنائي والمدني: تحديد المعايير والشروط الفنية والموضوعية لإسباغ الحجية القانونية على الدليل الرقمي (المادة ١١).

٣. تأطير الممارسات الاستثنائية وعالية المخاطر:

أ. البيانات ذات الطبيعة الخاصة: وضع المعايير والضوابط الصارمة لمعالجة البيانات الشخصية الحساسة، وآليات الحصول على موافقة ولي الأمر لمعالجة بيانات الأطفال (المادة ١٢).

ب. التسويق المباشر: تنظيم القواعد، والشروط، والضوابط الحاكمة لعمليات التسويق الإلكتروني المباشر (المادة ١٨).

٤. ضبط تدفق البيانات عبر الحدود:

أ. النقل والإتاحة الخارجية: تحديد الاشتراطات، والسياسات، والاحتياطات، والقواعد اللازمة لنقل، أو تخزين، أو مشاركة، أو إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج حدود الدولة (المادتان ١٤ و١٦).

٥. بناء البنية الإجرائية والتنظيمية:

أ. التراخيص والتصاريح: التأسيس الكامل لمنظومة التراخيص، والتصاريح، والاعتمادات؛ بما يشمل تحديد أنواعها، وفئاتها، ومستوياتها، وإجراءات وشروط إصدارها وتجديدها، والنماذج الفنية المستخدمة لها (المادتان ١ و٢٦).

وبمراجعة نصوص اللائحة نجد أن اللائحة قد نصت على جميع هذه الاحالات، بل يمكن القول بان واضع اللائحة قد اعتمد على سرد هذه الاحالات لتكون هي هيكل اللائحة وموادها، وهو ما يمكن حصره كالآتي

1. في شأن «جمع البيانات الشخصية ومعالجتها وحفظها وتأمينها» والتزامات «المتحكم» و«المعالج»:
   a. «السياسات والإجراءات والضوابط والمعايير القياسية لجمع البيانات الشخصية ومعالجتها وحفظها وتأمينها»: الإحالة الواردة في (المادة ٣ من القانون) تم استيفاؤها نصياً في (المادتين ٢ و٣ من اللائحة).
   b. «التزامات المتحكم» و«آلية تعيين ممثل له»: الإحالة الواردة في (المادة ٤ من القانون) تم استيفاؤها نصياً في (المادة ٣ «للالتزامات» والمادة ٥ «للممثل» من اللائحة).
   c. «التزامات المعالج» و«آلية تعيين ممثل له»: الإحالة الواردة في (المادة ٥ من القانون) تم استيفاؤها نصياً في (المادة ٤ «للالتزامات» والمادة ٥ «للممثل» من اللائحة).
2. في شأن «مسئول حماية البيانات الشخصية» و«الإبلاغ عن خرق البيانات» و«الدليل الرقمي»:
   d. «الإجراءات الخاصة بالإبلاغ والإخطار عن خرق أو انتهاك البيانات الشخصية»: الإحالة الواردة في (المادة ٧ من القانون) تم استيفاؤها نصياً في باب مستقل يشمل (المواد ٨، ٩، ١٠ من اللائحة).
   e. «شروط القيد بسجل مسئولي حماية البيانات الشخصية» و«الالتزامات والإجراءات والمهام الأخرى»: الإحالة الواردة في (المادتين ٨ و٩ من القانون) تم استيفاؤها نصياً في (المادتين ١١ و١٢ من اللائحة).
   f. «المعايير والشروط الفنية لاعتبار الدليل الرقمي المستمد من البيانات الشخصية حجة في الإثبات»: الإحالة الواردة في (المادة ١١ من القانون) تم استيفاؤها نصياً في (المادة ١٣ من اللائحة).
3. في شأن «البيانات الشخصية الحساسة» و«التسويق الإلكتروني المباشر»:
   g. «المعايير والضوابط لمعالجة البيانات الشخصية الحساسة» و«بيانات الأطفال»: الإحالة الواردة في (المادة ١٢ من القانون) تم تفصيلها واستيفاؤها نصياً في (المادة ١٤ «لبيانات الأطفال» والمادة ١٥ «للبيانات الحساسة» من اللائحة).
   h. «القواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر»: الإحالة الواردة في (المادة ١٨ من القانون) تم استيفاؤها نصياً في (المادتين ١٨ و١٩ من اللائحة).
4. في شأن «نقل أو تخزين أو مشاركة أو إتاحة البيانات الشخصية عبر الحدود»:
   i. «السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية» (عبر الحدود): الإحالة الواردة في (المادتين ١٤ و١٦ من القانون) تم استيفاؤها نصياً في (المادتين ١٦ و١٧ من اللائحة).
5. في شأن «التراخيص والتصاريح والاعتمادات»:
   j. «أنواع التراخيص والتصاريح والاعتمادات وفئاتها ومستوياتها وإجراءات وشروط إصدارها وتجديدها ونماذجها»: الإحالة الواردة في (المادة ١ «التعريفات» والمادة ٢٦ من القانون) تم استيفاؤها نصياً عبر إفراد باب

كامل يمتد من (المادة ٢٠ وحتى المادة ٤١ من اللائحة التنفيذية).

ب: نقد تطابق الاحالات:

وعلى الرغم من هذا التطابق الشكلي والمبدئي بين اللائحة والقانون في استيفاء مواضع الإحالات، إلا أنه بإمعان النظر التحليلي، تبرز لنا حزمة من الإشكاليات المنهجية العميقة التي ألقت بظلالها السلبية؛ ليس فقط على مدى كفاءة اللائحة في تفعيل تلك الإحالات، بل امتدت لتعصف بمدى اتساق أحكام اللائحة ذاتها وتوافقها مع التشريع الأم. وتتبدى أولى وأخطر هذه الإشكاليات في الآتي

1: النظرة المجزأة وتجاهل الروابط بين نصوص القانون:

يُمكن القول إن السمة الأبرز التي أثرت بشكل جذري على هيكلية اللائحة التنفيذية هي اعتمادها الحرفي والآلي على نصوص الإحالات. فقد صيغت اللائحة بغرض الوفاء الشكلي بتلك الإحالات، متجاهلةً حقيقة أن نصوص القانون لا تأتي منعزلة عن بعضها، بل ترتبط ببعضها ارتباطاً وثيقاً؛ حيث تتضمن بعض المواد استثناءات تُقيد أحكاماً أخرى (كالمادة الخامسة عشرة من القانون التي تسرد بعض الاستثناءات للمادة الرابعة عشرة)، بينما تأتي مواد أخرى لتُكمل قواعد عامة في مواد أخرى (كالمادة السادسة من القانون التي تُكمل المادة الثانية من القانون)، هذه الارتباطات التي كان يجب أخذها في الاعتبار عند وضع اللائحة واكمال نصوص الاحالات لتأتي اللائحة متسقة من نصوص القانون بالشكل الواجب

بيد أن واضع اللائحة اقتصر في صياغته على المادة التي تتضمن الإحالة الصريحة فقط، مُغفلاً النظر إلى المواد القانونية المرتبطة بها والمكملة لها. ويبرز هذا الخلل المنهجي بوضوح في التنظيم اللائحي لنقل البيانات عبر الحدود؛ حيث استندت المادة (١٦) من اللائحة التنفيذية حصرياً إلى المادة (١٤) من القانون —بوصفها المادة الحاملة لنص الإحالة والمنظمة للقواعد العامة— متجاهلةً تماماً المادة (١٥) من ذات القانون والتي تتضمن استثناءات جوهرية لا غنى عنها

ونتيجةً لهذا الاجتزاء والاعتماد الحرفي، وُلدت نصوص اللائحة مُحملة بمتعارضات شديدة وتناقضات صريحة مع أحكام القانون، وهي التعارضات التي سنُفرد لها مساحة تحليلية مفصلة في موضعها المخصص لاحقاً من هذه الدراسة

2: عدم اكتمال الإيفاء بالإحالات:

على الرغم من أن اللائحة نصت على جميع الاحالات التي نص عليها القانون، إلا انه يجب التفرقة بين الإيفاء النصي بها والايفاء العملي من حيث جاهزية النصوص للإنفاذ واعطاؤها منهجية متكاملة لمريدو الامتثال ليشرعوا في عملية تكييف نظمهم الداخلية لتحقيق معدل امتثال جيد للائحة

فقد جاءت جميع تلك الاحالات والتي تشكل كامل نص اللائحة محيلة في لقرارات ستصدر من المركز للإيفاء بالمتطلبات الفنية للإجراءات والمعايير التي نصت عليها ، وهو ما يمكن حصره في أكثر من ٢٥ إحالة من اللائحة لقرارات مستقبلية ستصدر من مركز حماية البيانات الشخصية، والتي يمكن حصرها في الآتي

1. القرارات الإدارية المستقبلية المتعلقة بالمعايير التقنية والأمنية (Cybersecurity & Technical Standards):
   a. البرامج التأمينية الواجبة (المادة ٢): إصدار المركز لقائمة المعايير والبرمجيات المعتمدة (مثل التشفير Encryption، ومنع تسريب البيانات DLP، والجدران النارية Firewalls) التي تُعد «كافية» لدرء المسئولية.
   b. معايير تأمين البيانات الحساسة (المادة ١٥): إصدار «بروتوكولات حماية خاصة» تختلف عن معايير البيانات العادية.
   c. مواصفات الدليل الرقمي (المادة ١٣): تحديد المواصفات الفنية للبرامج والأدوات والأجهزة المستخدمة في استخراج الأدلة لضمان حجيتها أمام القضاء.

d. ضوابط تأمين المراقبة البصرية (المادة ٣١): إصدار الإجراءات الفنية لتأمين تسجيلات الكاميرات (CCTV) وحمايتها من الاختراق أو التسريب.
e. الاشتراطات الفنية والتشغيلية للبنية التحتية (المادتان ٣٥ و٣٧): تحديد المعايير القياسية لمراكز البيانات (Data Center Tiers) المطلوبة لكل فئة من فئات التراخيص.
f. معايير حالات المعالجات الناشئة (المادة ٤): وضع المبادئ التقنية الحاكمة لاستخدام البيانات في تدريب نماذج «الذكاء الاصطناعي» والتقنيات المبتكرة لضمان درء الضرر.

2. القرارات الإدارية المستقبلية المتعلقة بالتنظيم الموضوعي لمشروعية المعالجة والجمع والحقوق والالتزامات
A. دليل آليات الموافقة (المادة ٢): تحديد واعتماد ماهية «الموافقة الإلكترونية» المقبولة، من عدد كبير من الخيارات التقنية مثل الاكتفاء بالنقر أو النشر بعد إتمام الوصول لأخر المستند، النقر المخصص على مربعات اختيار محددة وأيضا التحقق متعدد المستويات.
B. آليات موافقة ولي الأمر والتحقق من العمر (المادتان ١٤ و١٥): اعتماد الوسائل التقنية والرقمية لإثبات عمر الطفل (دون ١٥ عاماً، ومن ١٥ إلى ١٨ عاماً) وطرق التحقق من هوية ولي الأمر.
C. منهجية ممارسة الحقوق (المواد ٣، ٤، ٢١): اعتماد النماذج والآليات التي تُمكّن الشخص المعني من ممارسة حقوقه (الاطلاع، التصحيح، المحو، العدول) وتحديد مساراتها التقنية
D. آلية تحديد الحجم والغرض (المادة ٤): المعايير التي سيستند إليها المركز للموافقة على آليات عمل «المعالجين».

2. القرارات الإدارية المستقبلية المتعلقة بإدارة الحوادث والامتثال والمراقبة:
a. آليات تصنيف الخروقات (المادة ٦): إصدار معايير واضحة لتقييم المخاطر وتصنيف طبيعة الخرق (Low, Medium, High) لتحديد أولويات البلاغات.
b. آليات ووسائل الاخطار بحوادث الاختراق الماسة بالأمن القومي: (المادة ٦): وضع آليات التنسيق المباشر للإخطار الفوري بالخروقات الماسة بـ «الأمن القومي».
c. أدلة التقييم والفحص الدوري (المادة ١٠): إصدار «دليل التدقيق التقني» الذي تلتزم الشركات بتنفيذه دورياً لتقييم سلامة بياناتها.
d. تأهيل مسئول حماية البيانات (المواد ١١ و٣٢): وضع المنهج العلمي للاختبارات، وتحديد الكفاءات والمؤهلات المهنية المقبولة للقيد في السجل.
e. مصفوفة الضوابط والتدابير المفتوحة (المادة ٤١): صلاحية مجلس إدارة المركز في إضافة وإقرار أية متطلبات إضافية للحصول على التراخيص (تفويض مفتوح).

3. محور الأطر التنظيمية العابرة للحدود والتعاقدية (Cross-Border & Contracts):
E. القائمة البيضاء للدول (المادة ١٦): إصدار قرار بالدول التي تضمن مستوى كافٍ من الحماية (White List) بناءً على تقييم تشريعاتها لشرعنة نقل البيانات إليها.
F. النماذج التعاقدية القياسية (المادتان ١٧ و٢٤): إصدار واعتماد «البنود التعاقدية القياسية» (SCCs) الحاكمة للعلاقة بين المتحكمين والمعالجين والأطراف الخارجية.

4. القرارات الإدارية المستقبلية المتعلقة بالإجراءات:
a. نصت اللائحة على التزام المركز بإصدار وانشاء عدد من الاليات ووسائل الإيفاء بالإجراءات وخاصة فيما يتعلق ب:
b. بوابات الإبلاغ والتنظيم: بوابة الإخطار بالخروقات (م٦)، وبوابة سجلات قيد مسئولي الحماية (م١١)، وبوابة إخطار فصل المسئول (م١٢)، وبوابة الشكاوى من التسويق الإلكتروني (م١٨).
c. المنصة التفاعلية للتراخيص (م٤١): وتتفرع منها بوابات لتقديم رخص نقل البيانات (م٢٦)، والرخص العامة للأشخاص الاعتبارية (م٣٦) والطبيعية (م٣٨).

d. لم تنص اللائحة على أليات مماثلة فيما يتعلق بقيود اعتماد مستشاري الامتثال ولا اصدار تراخيص وتصاريح المراقبة البصرية.

ونتيجة لهذا العدد الضخم من الاحالات الموجودة في اللائحة لقرارات المركز فيجب أن يتم الالتفات لتلك الإشكاليات الجوهرية والتي تمس قانونية تلك النصوص من ناحية وأثرها على اللائحة والمخاطبين بأحكامها من ناحية أخرى

ثانيا: مدي مشروعية نهج الاحالات المركبة:

تُثير هذه الإحالات المتسلسلة والمكثفة لقرارات المركز إشكاليات جوهرية تمس مشروعية النص اللائحي ومدي دستوريته؛ فهي في ذاتها تثير مسالة حدود سلطة التفويض التشريعي الممنوحة من قبل القانون لمُصدر اللائحة (وزير الاتصالات وتكنولوجيا المعلومات). فالقانون حينما أحال تنظيم هذه المسائل للائحة التنفيذية، فإنه قد أصدر ‹تفويضاً موضوعياً› (Objective Delegation) موجها للأداة القانونية ذاتها بوصفها التشريع الفرعي المختصة دستوريا بتفسير واكمال النص التشريعي الأصلي، وليس ‹تفويضاً شخصياً› (Personal Delegation) للوزير بصفته. وعليه، فإنه فهو -كمركز قانوني مفوض- لا يملك سلطة الإحالة والتفويض التابع للتفويض التشريعي في تسلسل من التفويض الذي قد يفرغ اللائحة من مضمونها ويوزع تلك الاختصاصات الموكلة إليه ليصدرها في اللائحة التنفيذية ليتم إصدارها في هيئة قرارات مستقبلية يصدرها بصفته رئيساً لمجلس إدارة المركز؛ كما أن كمية الاحالات الموجودة في اللائحة تفرغ النص المفوض في إصداره من مضمونه بما يخل بقواعد التفويض ذاتها[٤٧].

وقد يتم تفسير هذا الاتجاه في التفويض بما ورد في نص المادة (١٩) من القانون، والتي أناطت بالمركز اختصاص ‹وضع وتطبيق القرارات والضوابط والتدابير... والسياسات والخطط الاستراتيجية›. نظرا للتقارب اللفظي في الصياغة، والذي قد يستخدم للدفاع عن مسلك اللائحة في إحالة التفاصيل الفنية لقرارات المركز انفاذاً لتلك المادة. غير أن هذا التفسير -من وجهة نزرنا- به تجاوز لمبدا ‹تدرج القواعد القانونية› وهو من المبادئ العامة التي يجب أن تفسر جميع النصوص القانونية بناء عليها بما فيها هذه المادة التي يجب أن ينحصر نطاقها في المسائل ‹التشغيلية والإدارية› البحتة التي تمس ولا تسلب اللائحة التنفيذية اختصاصاتها التفسيرية والمكلمة الأساسية

فالمسائل التي احيلت لقرارات المركز على الرغم من طابعها التقني الظاهر إلا انها في مجملها تمس جوهر الإحالات التي نص القانون أن تختص بها اللائحة، والتالي لا يجوز للجهة المُنوط بها إصدار اللائحة أن تتنصل من التزامها الدستوري بإصدارها متكاملة، أو أن تعيد تفويض هذه الصلاحيات التشريعية (Sub-delegation) لجهة أدنى متمثلة في مجلس إدارة المركز، إعمالاً للقاعدة الفقهية والإدارية المستقرة القاضية بأن ‹الاختصاص المفوَّض لا يُعاد تفويضه› (Delegata potestas non potest delegari)[٤٨].

ثالثا: تضارب الصياغة وعدم وضوحها:

كما أنه نتيجةً لهذا الكم الهائل من الإحالات المفصلية والمحورية، يُمكن القول إن اللائحة التنفيذية في وضعها الراهن تُعد غير قابلة للامتثال الكلي؛ ويتعمق هذا الاستعصاء التنفيذي بسبب «الاضطراب المصطلحي» في صياغة نصوص تلك الإحالات، حيث تأرجحت لغة المشرع اللائحي بين النقيضين. فتارةً تعتمد اللائحة صياغات حصرية توحي بالجمود المطلق والمركزية الإدارية الشديدة التي تقطع الطريق أمام أي اجتهاد أو امتثال ذاتي للمخاطبين، وهو ما يمكن أن ندلل عليه في اشتراط اللائحة المتكرر لاستخدام آليات وبرامج «يعتمدها المركز» (المادتان ٢ و٤)، أو تعليق نقل البيانات عبر الحدود على «السياسات التي يعتمدها المركز» لتحديد القائمة البيضاء للدول الآمنة (المادة ١٦)، وهو نهج تقريري يفرض حالة من الشلل التام لحين صدور تلك الاعتمادات.

٤٧ عاطف عبد الله المكاوي، العلوم الإدارية، القاهرة، مؤسسة طيبة للنشر والتوزيع، ٢٠١٢، ص: ٩٣.

٤٨ عبد العزيز بن محمد الصغير، القانون الإداري بين التشريعي المصري والسعودي، القاهرة، المركز القومي للإصدارات القانونية، ٢٠١٥، ص: ٦٣.

وتارةً أخرى، تعتمد اللائحة صياغة مرنة ومفتوحة تمنح المركز سلطة تقديرية غير منضبطة، كما يظهر بوضوح في إحالته ضوابط استخدام البيانات في تدريب نماذج الذكاء الاصطناعي إلى «المبادئ المتعارف عليها محلياً ودولياً» (المادة ٤)، وهي معايير فضفاضة تفتقر للتحديد الفني الصارم، وأيضا تكرار عبارة «أي معايير أو ضوابط أو تدابير أخرى يرى اعتمادها» لإصدار التراخيص في أكثر من موضع، مما يزيد من حالة التضارب التنظيمي الداخلي للائحة

رابعا: تأثير الاحالات على شفافية واستقرار التنظيم القانوني:

علاوة على ما سبق، فإن هذا الكم غير المسبوق من الإحالات لقرارات المركز يعصف بمبدأ "الأمن القانوني" (Legal Certainty) ويقوض استقرار القاعدة التشريعية وشفافيتها. فالآليات والأدوات القانونية لتعديل أو إلغاء "القرارات الإدارية" الصادرة عن المركز تتسم بمرونة مفرطة تختلف جذرياً عن الآليات المنضبطة لتعديل "اللائحة التنفيذية"؛ وهو ما يضع المراكز القانونية للمخاطبين بأحكام القانون تحت وطأة التغيير المستمر والتقلب الإداري، ويسلب تشريعاً حيوياً ومؤثراً كقانون حماية البيانات الشخصية مـ يجب أن يتمتع به من استقرار تشريعي ووضوح معياري مُسبق.

وتتضاعف خطورة هذا التفويض المفتوح عند وضعه في ميزان التقييم الواقعي والمؤسسي لمدى التزام الجهة المُفوَّضة (مركز حماية البيانات الشخصية) بمبادئ الحوكمة الرشيدة والشفافية. فالممارسة العملية كشفت عن غياب مقلق للشفافية المؤسسية؛ حيث باشر المركز تشكيله وعمله لفترات ممتدة دون إفصاح أو إعلان رسمي عن هياكله التنظيمية، فضلاً عن افتقار عمليات استقطاب وتعيين كوادره إلى مبدأي «العلانية» و»تكافؤ الفرص». هذا الواقع الإداري المتسم بالضبابية يطرح تساؤلات مشروعة ـــ وذات وجاهة قانونية ـــ حول مدى التزام هذا المركز مستقبلاً بإعمال مبدأ «الشفافية والعلانية» في نشر قراراته وإجراءاته التنظيمية، ومدى قدرته المؤسسية على فرض الامتثال لقواعد وُلدت في بيئة تفتقر للإفصاح المسبق

خامسا: مدي ضرورة الاتجاه المفترض من اللائحة:

وفي الختام، لكي ننتهي من تقييم هذا الاتجاه الذي تبنته اللائحة ـــ والمتمثل في فرض ‹معايير قياسية موحدة› ومركزية لتقييم كافة الجوانب التفصيلية لعملية الامتثال، وهو الاتجاه الذي دفعها للتوسع المفرط في الإحالة لقرارات إدارية مستقبلية تصدر عن المركز ـــ يجب أن نطرح تساؤلين محوريين: هل فرض القانون هذا الاتجاه الجامد على اللائحة؟ وهل يتسق هذا المسلك مع المعايير العالمية المتبعة في حماية البيانات؟، وهو ما يمكن الإجابة عنه كالآتي

فبالرجوع إلى نصوص القانون المصري لحماية البيانات الشخصية، يتبين بوضوح أنه لم يُلزم اللائحة التنفيذية بانتهاج هذا المسار المركزي الجامد. فقد استخدم المشرع صياغات مرنة ومجردة (مثل مطالبة اللائحة بوضع «السياسات» أو «المعايير القياسية»)، وهي صياغات مرنة وواسعة تمنح السلطة التنفيذية حرية الحركة لاستيعاب التطورات التكنولوجية. ولكن اللائحة اختارت مسار التضييق لا التوسع من خلال وضع مادة تنص على مبادئ التأمين المتسق مع المخاطر وحجم العمليات مثلا، فتحولت المرونة التشريعية إلى قيود بيروقراطية، من حيث اشتراط «الاعتماد المسبق» من المركز في كل تفصيله إجرائية وتقنية، فارضاً مركزية إدارية لم يشترطها القانون صراحة

كما أن هذا الاتجاه اللائحي يتصادم كلياً مع الاتجاهات التشريعية العالمية الحديثة. التي تخلت عن فكرة الاعتماد المسبق لتتبني ما أرسته اللائحة العامة من الاتجاه القائم على «النهج القائم على المخاطر» (Risk-Based Approach) و»مبدأ التناسب الفردي» (Proportionality).

فطبقا لأليات الامتثال الفردي يُترك للكيانات مساحة للتقييم الذاتي لمخاطرها، لتختار التدابير التأمينية التي تتناسب مع حجمها وتكلفة التنفيذ وطبيعة بياناتها؛ فما يُطلب من بنك عملاق يختلف جذرياً عما يُطلب من شركة ناشئة. أما اللائحة المصرية، فقد فرضت نهجاً إلزامياً موحداً يعامل الجميع بمستوى واحد من الاشتراطات وينتظر «كتالوجاً حصرياً» من المركز، وهو ما يُعد ارتداداً عن فلسفة الامتثال المرنة، ويخلق أعباءً اقتصادية تُعيق الابتكار ونمو الاقتصاد الرقمي

وأخيرا لا يمكننا الحكم على تلك النقطة بالتفصيل إلا بعد صدور تلك القرارات المكملة والتي نأمل أن تأتي بما يتناسب مع المعايير الدولية وحاجات السوق وحسن الامتثال

المبحث الثاني

تقييم التوازن الداخلي للائحة والأثر الاقتصادي والتقني

بعد الانتهاء من التحليل التفصيلي لنصوص اللائحة التنفيذية، لا يمكن الاكتفاء بالنقد الجزئي للمواد دون تقييم "الهندسة التشريعية" الكلية للائحة ومدى قابليتها للتطبيق العملي في سوق يتسم بالديناميكية.

ولهذا، نهدف في هذا المبحث إلى إجراء تقييم شامل لاختبار مدى "التوازن الداخلي" للائحة فلسفيا وتنظيمياً من جهة، وقياس "أثرها الخارجي" تقنياً واقتصادياً من جهة أخرى، كوسيلة لبناء رؤية نقدية متكاملة لبيئة الامتثال الرقمي.

وهذا في مطلبين كالآتي:

المطلب الأول: تقييم التوازن والاتساق الداخلي للائحة وأثره على بيئة الامتثال والمساءلة.

المطلب الثاني: الكلفة والتكاملية التقنية والاقتصادية للائحة.

المطلب الأول
تقييم التوازن والاتساق الداخلي للائحة وأثره على بيئة الامتثال والمساءلة

يعتبر التوازن والاتساق بين الغايات التشريعية وآلياتها التنفيذية أحد أهم معايير نجاح وحسن صياغة التنظيم القانوني الحديث. ومن ناحية أخرى، لا يمكن إنكار حاجات المشرع لفرض إجراءات إدارية ورقابية لضمان الامتثال، وأيضاً وضع منظومات للتراخيص وتدابير أمنية مجردة لضبط بيئة معالجة البيانات والسيطرة عليها. ولكن نتيجة لهذه الحاجات، تزداد خطورة الوقوع في اختلال هيكلي يُغلِّب النزعة البيروقراطية على حساب التعزيز الفعلي للضمانات الحقوقية، مما قد يخلق بيئة امتثال معقدة تثقل كاهل الكيانات بأعباء إجرائية لا تنعكس بالضرورة على رفع مستوى حماية الأشخاص المعنيين بالبيانات.

وفي هذا المطلب، سنُخضع اللائحة التنفيذية لتقييم موضوعي ومحايد لاختبار مدى نجاحها في تحقيق هذا التوازن الداخلي وتجنب الخلل المنهجي، وذلك من خلال دراسة وتحليل أربعة محاور رئيسية، كالآتي:

أولاً: دراسة هيكلية منظومة الرخص والتصاريح وآليات تحقيق الامتثال.

ثانياً: تقييم التوازن الفلسفي والعملي بين متطلبات التنظيم الإداري والضمانات الحقوقية.

ثالثاً: تحليل النطاق المفاهيمي لـ "حماية البيانات" بين ضوابط التأمين التقني والمظلة الشاملة لحوكمة المعالجة.

رابعاً: فحص مدى التوافق المنهجي والتشغيلي بين التزامات اللائحة والامتثال للقوانين القطاعية الموازية.

أولا: ما يتعلق بالرخص والتصاريح وهيكلية عملية الامتثال:

أ. الازدواجية المعيارية في تصنيف التراخيص واحتساب الرسوم:

اعتمدت اللائحة التنفيذية في تقسيم فئات التراخيص والتصاريح على فهم جامد للأنواع الواردة في المادة

(٢٦) من القانون، وذلك في المواد من (٢١ إلى ٤١). ثم أوردت جداول الرسوم الأساسية المقتطعة في المواد (١٩-٢٠). وتتسم منظومة التراخيص هذه ببنية مزدوجة تفتقر للاتساق؛ إذ توجد تراخيص «تَبَعِيّة» كالنقل عبر الحدود والتسويق الإلكتروني المباشر، وهما تصريحان يُبنيان بالضرورة على وجود ترخيص عام مسبق لمعالجة البيانات، في مقابل تراخيص «مستقلة» كترخيص المراقبة البصرية (CCTV) الذي لا يُشترط لتأسيسه الحصول على الرخصة العامة

ويكمن العوار الأبرز في هذا التنظيم المزدوج في أن تقدير الرسوم لم يُبنَ على معيار (طبيعة النشاط) أو (درجة المخاطر ونوع البيانات)، بل اعتمد حصرياً على معيار (حجم معاملات النشاط على البيانات الشخصية أو حجم السجلات). وهو معيار يفتقر للتناسب مع الفلسفة الحمائية لقانون البيانات؛ حيث إن العبرة في تقييم أثر المعالجة تكون بـ «طبيعة وحساسية» البيانات وليس بـ «حجمها» المطلق

وتأسيساً على هذا المعيار الحجمي، أوردت اللائحة التزاماً معيباً حين اشترطت على (المعالج) دون (المتحكم) [إعداد آلية يتم اعتمادها من المركز تحدد حجم البيانات الشخصية والغرض من المعالجة م ٢/٤]. وهذا الالتزام يتصادم تشغيلياً وقانونياً مع نظم حماية البيانات في عدة محاور

- أولاً (مخالفة طبيعة المراكز القانونية): أُلقي هذا الالتزام على عاتق «المعالج»، في حين أن «المتحكم» هو الأصيل الذي يقرر الغرض وتتم المعالجة لصالحه. وبما أن هذه الآلية مرتبطة بتقدير الرسوم، فكان الأجدر والأصح قانوناً أن يتحمل (المستفيد/المتحكم) هذا العبء وليس (المنفذ/المعالج).
- ثانياً (تجاهل الطبيعة التشابكية للسوق): تفترض اللائحة وجود علاقة خطية وحصرية بين المتحكم والمعالج، في حين أن واقع الأعمال يقوم على تعاقد المتحكم مع عدة معالجين، وعمل المعالج لحساب جهات متعددة. ومن الناحية التقنية، يصعب على المعالج في أحيان كثيرة فصل سجلات متحكم عن آخر استناداً إلى البنية الفنية المشتركة التي يعمل عليها.
- ثالثاً (إسقاط نموذج الفوترة الخاص بقطاع الاتصالات): يُعزى هذا الخلل -في اعتقادنا- إلى نظرة واضعي اللائحة القاصرة لـ «المعالج»؛ حيث تم تكييفه كمسئول مطلق عن البنية الفنية، ومُلزم بتوفير آليات لقياس وتحديد حجم المعاملات لأغراض الرسوم. وهو ما يُعرف بـ (آليات الفوترة Billing Mechanisms) التي تتناسب وتُطبق في قطاع «الاتصالات»، ولكنها لا تتناسب إطلاقاً مع قطاع معالجة البيانات الشخصية الذي يتسم بدورات معالجة متزامنة ومعقدة لا تتبع نسقاً خطياً قابلاً للقياس الحجمي المجرد.

وقد أدى هذا التضارب المعياري إلى خلق «مصفوفة رياضية مركبة» لاحتساب رسوم الامتثال، تُلزم المُخاطبين بالرجوع لجداول الحجم الاقتصادي أولاً، ثم استقطاع نسب مئوية بحسب نوع الرخصة. كما أسفر ذلك عن ظاهرة «التراخيص المتراكمة»؛ حيث يُلزم الكيان باستخراج رخصة عامة، ثم تكديس رخص إضافية (Add-on Licenses) فوقها لمهام لصيقة بطبيعة العمل، كنقل البيانات عبر الحدود أو التسويق الإلكتروني

ب. إشكالية بنية التراخيص والتصاريح:

1: إشكالية تعقيد بنية التراخيص والتصاريح:

على الرغم من سعي اللائحة التنفيذية لتقديم واجهة عصرية ومبسطة لعملية الحصول على التراخيص والتصاريح، عبر إقرارها في المادة (٤١) إنشاء بوابة إلكترونية تفاعلية لتوجيه المتقدمين بناءً على المستندات المقدمة، إلا أن هذا الطموح الرقمي وقع رهينة للعقلية الإدارية الجامدة التي تهيمن على نصوص اللائحة. فقد أسس المشرع اللائحي بنية صارمة تعتمد على آليات التفتيش الاستباقي والقيود التقليدية، مما أنتج «جبلاً خفياً ومتراكماً» من الالتزامات المستندية المعقدة التي تتوارى خلف الواجهة الإلكترونية المُشجعة والمبسطة لعملية التقديم

وهو ما يختلف عن المعايير العالمية المعاصرة الحاكمة لنظم حماية البيانات الشخصية، والتي تتبنى فلسفة «المساءلة اللاحقة» (Accountability). فالممارسات الدولية الفضلى تشجع على الامتثال الذاتي

المتناسب مع القواعد القانونية، عبر منح الكيانات مساحة من المرونة في «التصميم الفردي» لنظم حمايتها بما يتوافق مع طبيعة مخاطرها؛ وهو ما ينعكس إيجاباً على تقليص الأعباء المستندية المسبقة، خلافاً لما انتهجته اللائحة من تعقيد إداري مفرط يقوض مرونة الأعمال

2: غياب الية موحدة لبنية التصاريح والتراخيص:

تبنت اللائحة نهجاً مزدوجاً وغير مبرر؛ في تفسيرها لعلاقات الرخص ببعضها البعض، فمثلا:

- تبنت اللائحة ضرورة وجود رخصة عامة للمتحكم والمعالج للبيانات الشخصية والبيانات الشخصية الحساسة، ونصت على إمكانية منحها إما لمتحكم أو معالج مع دفع نصف الرسوم بالنسبة لهذه الرخصة المجزأة (م ١٩)، دون أن تحدد آلية للفصل ومن يحتاج لرخصة مجمعة ومن يحتاج لرخصة منفردة، وخاصة في ظل إشكالية تعريف المعالج في قانون حماية البيانات الشخصية المصري.
- عدم تقديمها لموقف موحد في ما يتعلق بتراتبية الرخص ففي حين نصت اللائحة بشكل مباشر على ضرورة حصول المتحكم والمعالج الراغب في الحصول على رخصة لأغراض التسويق الاليكتروني المباشر (-2 الحصول على ترخيص تصريح متحكم أو المعالج)، لم تنص اللائحة على هذا بالنسبة ل (ترخيص تصريح لنقل البيانات الشخصية عبر الحدود)، وأيضا عامل (ترخيص تصريح استخدام وسائل المراقبة البصرية في الأماكن العامة) كحالة منعزلة تماما كأنها رخصة منفصلة بشكل كامل عن جميع أحكام القانون واللائحة، وتكرر الأمر بالنسبة ل (اعتماد تقديم الاستشارات الخاصة بإجراءات حماية البيانات الشخصية)، كما يلاحظ أيضا أنه لم يضمن هذه الرخصة وهذا الاعتماد في الإجراءات الإليكترونية.
- نتيجة اعتماد اللائحة على أليتان مفصلتان لتنظيم الرخص والتصاريح منهم الية تحديد الرسوم على أساس حجم المعاملات وتحديدها لفئات متصاعدة فقد جاءت المادة ٣٩ ملزمة الكيانات بالتقدم للمركز لتعديل الترخيص (في حالة زيادة أعداد سجلات البيانات الشخصية عن البيانات الصادر عنها الترخيص). هذا النص يتعارض جذرياً مع الطبيعة المتغيرة للأنشطة التجارية الرقمية التي تتسم بتذبذب حجم البيانات (كالمواسم التجارية أو التوسع المفاجئ). إن ربط صلاحية الترخيص بسقف رقمي جامد، يحول عملية الترخيص من «إطار تنظيمي للمساءلة» إلى «عداد استهلاك» يعرقل نمو الأعمال، ويُغرق الجهة الإدارية بطلبات تعديل مستمرة، دون توضيح للوضع القانوني للكيان أو عملياته التشغيلية أثناء فترة طلب التعديل.

3: إشكالية رخصة أو تصريح المراقبة البصرية للأماكن العامة:

أفردت اللائحة التنفيذية في المادة (٣١) تنظيماً مستقلاً لاستخدام وسائل المراقبة البصرية في الأماكن العامة. وقد أدى هذا الفصل إلى عزل هذا النشاط عن القواعد العامة لحماية البيانات المنصوص عليها في اللائحة، بالإضافة إلى خلق تداخل مع تشريعات أخرى سارية. ويمكن تفصيل الملاحظات القانونية والعملية على هذا التنظيم في النقاط الآتية

- غياب التكييف القانوني كـ «متحكم» أو «معالج»: أغفلت اللائحة التكييف القانوني الدقيق للكيان القائم بعملية المراقبة البصرية؛ حيث تعاملت معه كمجرد «مستخدم لوسائل المراقبة» بدلاً من تكييفه المنضبط كـ «متحكم» أو «معالج» لبيانات شخصية. ونتيجة لعدم التكييف هذا، لم يُشترط حصول الكيان على التراخيص والتصاريح العامة المسبقة (كمتحكم أو معالج) أسوة بما اشترطته اللائحة في أنشطة أخرى كالنقل عبر الحدود والتسويق الإلكتروني. ويؤدي هذا القصور إلى إعفاء القائمين بالمراقبة البصرية -عملياً- من حزمة الالتزامات المؤسسية والقانونية الصارمة المفروضة على المتحكمين والمعالجين في باقي أحكام اللائحة، رغم أن تسجيل مقاطع الفيديو يمثل «معالجة» صريحة لبيانات شخصية.
- غياب ضوابط الاحتفاظ وحقوق الأشخاص المعنيين: نتيجة الهيكلية المنفصلة للمراقبة البصرية للأماكن العامة، خلت المادة من تنظيم حقوق الأفراد الخاضعين للمراقبة (مثل الحق في النفاذ أو

طلب المحو)، ولم تتضمن التزاماً واضحاً بالإبلاغ عن الاختراقات الأمنية لتلك الأنظمة. لم تحدد المادة حداً أقصى لمدة الاحتفاظ بتسجيلات الكاميرات، في حين أن اشتراطات المحال العامة حددت الحد الأدنى (١٥ يوماً)، مما قد يؤدي عملياً إلى الاحتفاظ بالبيانات لمدد غير محددة بالمخالفة لمبدأ تقليل البيانات. كما خلت

- التداخل مع قانون المحال العامة: اشترطت المادة الحصول على التراخيص والموافقات من الجهات المختصة، وهو ما يتقاطع مباشرة مع قانون المحال العامة والقرارات المنفذة له (مثل قرار وزير التنمية المحلية رقم ٣٩ لسنة ٢٠٢٢)، والتي تفرض تركيب كاميرات المراقبة كشرط أساسي لترخيص المحل نفسه. هذا الوضع يخلق ازدواجاً إجرائياً، ولا يوضح كيفية الربط بين ترخيص المركز وتراخيص الجهات الأخرى، وما إذا كان التفتيش سيتم بشكل متكامل أم منفصل.
- صعوبة الرقابة على تقنيات تمييز الوجوه: حظرت اللائحة استخدام تقنيات تمييز الوجوه (Face Recognition) إلا بموافقة صريحة أو سند قانوني. ورغم أهمية هذا النص، إلا أن تطبيقه يواجه صعوبة عملية؛ حيث تُباع العديد أنظمة المراقبة الحديثة مزودة بهذه التقنيات افتراضياً. وإلقاء عبء الامتثال على المشغل النهائي وحده، دون وضع قواعد تنظيمية لسوق استيراد وبيع وتركيب هذه الأنظمة، يجعل الرقابة على هذا الالتزام غير فاعلة.
- نصت المادة في بندها السادس على التزام طالب الترخيص باتباع الإجراءات والتدابير الصادرة عن المركز لتأمين التسجيلات وحمايتها من الاختراق، وهو ما يمثل إحالة لقواعد لم تصدر بعد. وعلاوة على ذلك، فإن تحميل طالب الترخيص عبء حماية هذه الأنظمة من الاختراق يتجاهل الطبيعة العملية والتقنية لها؛ إذ تُباع أنظمة المراقبة عادة كمنظومات متكاملة من قبل الشركات المصنعة والموردين، ولا يملك المشغل النهائي (كأصحاب المحال أو الكيانات غير التقنية) القدرة أو الصلاحية لتعديل برمجياتها لسد الثغرات الأمنية. وكان من الأنسب أن يتم وضع ضوابط ملزمة على جهات استيراد وبيع وتركيب هذه الأنظمة لضمان توافر معايير الأمان بها، بدلاً من تحميل المستخدم النهائي التزامات فنية تخرج عن نطاق سيطرته الفعلية.
- الغموض في استثناء محال الإقامة: استثنت المادة الكاميرات الخاصة بمحال إقامة الأفراد بشرط «ألا تتجاوز حدودها المكانية». هذا المعيار يطرح إشكالية في التطبيق العملي بسبب قدرات التقريب الرقمي (Zoom) للكاميرات الحديثة، ولم توضح اللائحة آلية تحديد أو قياس هذه المسافات، أو كيفية رصد التجاوزات وإثباتها.
- الفراغ الإجرائي المستندي: جاءت المادة (٣١) خالية من تحديد دقيق للمستندات المطلوبة لاستخراج هذا الترخيص. كما لم يتم إدراج هذا المسار ضمن المنظومة الإلكترونية أو النماذج المحددة في المادة (٤١)، مما يتركه دون إطار إجرائي واضح يوجه المتقدمين.

ج: إشكالية عدم وضع معيار محدد للتخفيف والاستثناء من أحكام التراخيص والتصاريح

بالنظر إلى تفرد المشرع المصري بتبني «نظام التراخيص المسبقة» في مجال حماية البيانات، تبرز صعوبة المقارنة الهيكلية المباشرة مع التشريعات المقارنة. إلا أن التقييم الموضوعي يوجب الإشارة إلى الاتجاه التشريعي العالمي المعاصر الذي يتبنى «النهج القائم على المخاطر» (Risk-Based Approach)؛ حيث تتدرج الالتزامات صعوداً وهبوطاً بناءً على (طبيعة المعالجة، ونوعية البيانات وحساسيتها، وحجم المعاملات، والمخاطر المحتملة على حقوق وحريات الأشخاص المعنيين)[٤٩]. وهو النهج المرن الذي لم يعتمده القانون المصري صراحةً في بنيته الأساسية، مفضلاً فرض قوالب التزام موحدة

ومحاولةً منها لوضع بعض صورٍ من التخفيف أو الإعفاء لبعض الفئات المخاطبة، قدمت اللائحة بعض أنواع الاستثناء والتخفيف في مواد التراخيص دون أن ينعكس هذا إطلاقاً على «نصوص الالتزامات الموضوعية» التي ظلت سارية على الكافة دون تفرقة. كما جاء هذا التوجه مفتقراً إلى نظرية عامة أو

49 Gdpr, Article 24(1) & Recital 74, Article 29 Data Protection Working Party (WP29), «Statement on the role of a risk-based approach in data protection legal frameworks», Adopted on 30 May 2014 (WP 218), pp. 2-3, Centre for Information Policy Leadership (CIPL), «A Risk-based Approach to Privacy: Improving Effectiveness in Practice», Hunton & Williams LLP, 2014, pp. 4-6.

معيار حاكم يوحد آلياته، حيث تناثرت أحكامه وتطبيقاته بشكل غير متسق في مواضع متفرقة من اللائحة، وهو ما يمكن تتبعه واستعراضه على النحو الآتي

1: عدم امتداد الاستثناء المالي للشروط والمستندات:

جاءت المادة التاسعة عشرة من اللائحة ناصةً على إعفاء من الرسوم بالنسبة للمتحكمين والمعالجين ذوي حجم السجلات البسيطة، والتي لا تزيد عن مائة ألف سجل لتراخيص الأشخاص الاعتبارية، وخمسة وعشرين ألف سجل لتصاريح الأشخاص الطبيعية والاعتبارية. وعلى الرغم من حُسن هذا التوجه المالي، إلا أنه كان من الأوجب أن يمتد هذا الاستثناء إلى الجانب الأهم والذي يمثل العبء الأكبر على المخاطبين، وهو جانب تحضير «ملف الترخيص» نفسه. فقد احتفظت اللائحة باشتراطات إجرائية صارمة تتجاهل تنوع طيف المخاطبين بأحكامها، لا سيما الأشخاص الطبيعيين والشركات والأنشطة الصغيرة والمتوسطة والناشئة[٥٠].

ويبرز هذا التجاهل بوضوح في تعامل اللائحة مع المهنيين المستقلين (كالأطباء والمحامين) الذين يديرون أعمالهم عادةً عبر حواسيب شخصية أو هواتف ذكية، بمنطق «المؤسسات الكبرى»؛ وذلك من خلال عدة إشكاليات متراكمة، منها:

- تعجيز «البنية التحتية» والشهادات الفنية: بالرجوع إلى المادة (٣٧) المنظمة لمستندات تصريح الأشخاص الطبيعية، نجدها تلزم طالب التصريح باستيفاء (كافة البيانات الفنية عن البنية التحتية المستخدمة ومنها أنواع الأجهزة)، فضلاً عن تقديم (الشهادات والاعتمادات الفنية الحالية التي حصل عليها في شأن تأمين الاحتفاظ بالبيانات مع تحديد الجهات المانحة لها). إن هذا المتطلب يفرض عائقاً عملياً يصل إلى حد الاستحالة في التنفيذ؛ فالمهني المستقل لا يسعى عادةً، ولا يُفترض به، الحصول على شهادات اعتماد فنية متخصصة في أمن المعلومات والجودة (مثل ISO 27001) لممارسة مهنته الأصلية. كما أن مطالبة الفرد بسرد وتوثيق تفاصيل بنيته التحتية تقنياً يفرض عليه واقعياً الاستعانة بخبراء متخصصين، مما يضيف تكلفة مالية باهظة وغير متناسبة لنشاط محدود النطاق[٥١].
- جمود معايير التأمين وتجاهل تقييم المخاطر: لم تضع اللائحة نظاماً مخففاً (Light-touch Regime) للأفراد، بل أحالتهم في المادة (٢٢) إلى ضرورة التوافق مع «المعايير العامة» الصادرة عن المركز لتأمين البيانات. هذا الإطلاق يسوي في المسطرة التأمينية بين «عيادة طبيب مستقل» و»شركة تأمين كبرى»، متجاهلاً الفروق الشاسعة في حجم وطبيعة البيانات. وهو ما يثير مخاوف حقيقية من فرض برمجيات واشتراطات تقنية مكلفة (مثل أنظمة الجدران النارية المتقدمة أو أنظمة منع تسرب البيانات DLP) تفوق تكلفتها العائد المادي لنشاط المهني الصغير.
- تحميل أعباء معرفية وازدواجية المراكز القانونية: وإلى جانب الأعباء التقنية، حمّلت اللائحة الأشخاص الطبيعيين أعباءً معرفية وقانونية مزدوجة؛ حيث افترضت وجوب توافر المراكز القانونية المختلفة (متحكم ومسئول حماية بيانات في آن واحد) في حالة الشخص الطبيعي. إن إلقاء هذا العبء الفني والقانوني المتخصص على كاهل الفرد يؤدي حتماً إلى «صورية الامتثال» (بأن يُعين نفسه شكلياً كمسئول)، فضلاً عن إشكالية «ازدواجية العقوبة» عبر معاقبة ذات الشخص بصفته متحكماً وبصفته مسئولاً عن نفس الخطأ.
- غموض التصنيف وفخ «المنشأة الفردية»: امتدت إشكاليات المادة (٣٧) لتشمل معايير تقييم طالب التصريح نفسه؛ فقد طلبت في بندها الخامس تقديم (صورة من المؤهلات الدراسية)، وهو شرط إداري قد يكون منعدم الصلة بالنشاط التجاري الفعلي المعالج للبيانات. كما غاب عن اللائحة وضع معيار فاصل يحدد ما إذا كان صاحب «المنشأة الفردية» (الذي يملك سجلاً

50 GDPR, Recitals 13 & 98. ENISA (European Union Agency for Cybersecurity), «Guidelines for SMEs on the security of personal data processing», 2021, pp. 15-16.

٥١ في دليله الرسمي لتوجيه المشروعات الصغيرة، أقر مكتب مفوض المعلومات البريطاني (ICO) صراحةً بأن «تكلفة التنفيذ» يجب أن تكون عاملاً حاسماً في تقييم مدى التزام الكيان، وأن مستوى الأمان المطلوب من ممارس مستقل يختلف جذرياً عن المطلوب من مؤسسة كبرى Information Commissioner's Office (ICO), "Security - Guide to the UK GDPR". Avail-able at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/security-a-guide-to-data-/

تجارياً) سيُعامل إجرائياً كشخص طبيعي أم اعتباري، مما يفتح الباب لتأويلات إدارية قد تلزمه بمتطلبات الشركات ذات السقف الأعلى رغم كونه فرداً.

2: الاستثناء بناءً على ماهية المرخص لا طبيعة نشاطه والمخاطر المترتبة عليه:

اللائحة أثناء محاولتها لتطبيق نوع من الاستثناء والتخفيف بين المراكز القانونية المخاطبة، قامت باتباع نهج انفردت به، وهو تقديم بعض الاستثناءات وتخفيف بعض الشروط للأشخاص الطبيعية فقط دون الأشخاص الاعتبارية، وهو ما يقوم حسب طبيعة المستثنى لا حسب مخاطر نشاطه على البيانات. وهو خطأ منهجي واضح؛ فقد تُشكل أنواع معالجةٍ يقوم بها ممارس حر (Freelancer) متخصص في نوع من أنواع المعالجة المتقدمة على البيانات الشخصية، مخاطر أكبر مما قد تمثلها -مثلاً- شركة صغيرة تختص بتوزيع أو بيع سلع غذائية بسيطة

ويمكن أن نبين هذا الاتجاه في أكثر من موضع في اللائحة، كالآتي:

- إسقاط شرط (الإمساك بالسجلات الإلكترونية) في المادة (٢٢) الخاصة بشروط الأشخاص الطبيعية، والمادة (٣٧) الخاصة بمستندات الأشخاص الطبيعية، والتي نُص عليها في مواد اشتراطات ومستندات الأشخاص الاعتبارية (م ٢١، م ٣٦)، رغم الأهمية القصوى لإمساك سجل المعاملات كونه مفتاح عملية الإثبات وتتبع المعاملات في دورة معالجة البيانات الشخصية. كما أن هذا التمييز يثير تعارضاً داخلياً مع مواد التزامات المتحكم (م٣) والمعالج (م٤) والتي اشترطتا إمساك السجلات دون تفرقة بين المتحكم أو المعالج الطبيعي أو الاعتباري.
- وعلى الرغم من إسقاط الالتزام بالسجل -رغم أهميته القصوى والسهولة النسبية للالتزام به في أكثر من صورة- فقد جاءت مواد اشتراطات ومستندات الرخص الخاصة بالأشخاص الطبيعية ذاتها ناصةً على التزامهم بتقديم (شهادات واعتمادات فنية عن البنية التحتية المستخدمة لتأمين البيانات)، وهو التزام تقني ومادي ضخم يتناسب مع المؤسسات الكبرى ويتناقض مع طبيعة وحجم المهنيين المستقلين، والذين عادة ما لا تتجاوز عملياتهم على البيانات الشخصية حد الإعفاء الرسومي المذكور في اللائحة وهو مائة ألف سجل. ونرى تفسير هذا في تركيز اللائحة الكبير على سرية البيانات وتأمينها، كما أنها لائحة لقانون أمن سيبراني لا قانون حماية بيانات شخصية.
- وأيضاً طالبت اللائحة في اشتراطات تراخيص المتحكم والمعالج للبيانات الشخصية والبيانات الحساسة للأشخاص الاعتبارية (تقديم عقد مسئول حماية البيانات الشخصية) وهو شرط طبيعي، ولكنها في نفس الوقت حاولت أن تستثني الأشخاص الطبيعية من هذا الالتزام عن طريق اشتراطها أن يكون المتحكم أو المرخص هو مسئول حماية البيانات الشخصية (م ٣٨)، وهو ما يطرح أسئلة عن الجدوى والدافع؛ فالمتحكم هو في كل الأحوال -حتى لو كان هناك مسئول لحماية البيانات الشخصية- هو المسئول عن إنفاذ أحكام القانون.

د: تعقد وخفاء الهيكلية المستندية:

فإذا حللنا البنية المستندية الموجودة في اللائحة يتجلى أمامنا طبقات معقدة من المستندات والاشتراطات، والتي وإن حتى تم تصميم البنية النهائية للبوابات الإليكترونية والواجهة التفاعلية على تقليلها وتبسيطها، فإن عملية الترخيص ستصطدم بعملية الامتثال المعقدة، والتي ينجم عنها بالتبعية تراكم وتعقد مستندات، واشتراطات الامتثال، والتراخيص والتصاريح

هذا التعقد لا يقف فقط على مجرد الكم ولا الكيف، بل أيضا الوضوح ومدى نجاح اللائحة في تقديم دليل تشغيلي شمولي كامل لكل طبقات المستندات المطلوبة في عملية التراخيص والتصاريح أو اثناء الامتثال، وهو ما يمكن تحليله بتقسيم اللائحة تشغيليا لثلاث طبقات تمثل الطبقات المستندية والاشتراطات في اللائحة، كالآتي

- الطبقة الأولى (الواجهة الإجرائية التفاعلية): تتمثل في المادة (٤١) التي تؤسس

للواجهة الإلكترونية الموحدة للتقديم باعتبارها أولى المراحل وأبسطها شكلياً. ورغم اقتصار تفاصيلها الظاهرية على (٤ بيانات و٤ إقرارات)، إلا أنها تتضمن إحالة مبهمة لضرورة استيفاء «كافة المستندات المطلوبة» دون حصرها الدقيق.

- الطبقة الثانية (الهيكل الإجرائي المتناثر والاشتراطات الوسيطة): وتغطي المواد من (٢١ إلى ٤٠) والخاصة بالمستندات والإجراءات، ملحقاً بها تفاصيل فئات التراخيص والرسوم في المادتين (١٩ و٢٠). وتتطلب هذه الطبقة بيانات أكثر تعقيداً مما ورد في المادة (٤١)، حيث تتوزع نصوصها صعوداً وهبوطاً بحسب نوع الرخصة؛ فترخيص الأشخاص الاعتبارية يتطلب تتبع المواد (٢١، ٣٥، ٣٦، ٤١)، والأشخاص الطبيعية في المواد (٢٢، ٣٧، ٣٨، ٤١). ويمتد هذا التشتت للرخص المضافة، كالنقل عبر الحدود (المواد ٢٤، ٢٥، ٢٦، ٤١)، والتسويق الإلكتروني (المواد ٢٩، ٣٠، ٤١)، فضلاً عن المراقبة البصرية (٣١، ٤١)، والاستشارات (٣٢-٣٤، ٤١)، وقيد مسئول حماية البيانات (٧-١٠).
- الطبقة الثالثة (العمق التشغيلي والالتزامات المبطنة): وهي الطبقة الخفية والأكثر عمقاً وتأثيراً؛ إذ تُمثل الترجمة المستندية وهندسة إثبات الامتثال للمواد الموضوعية الواردة في القسم الأول من اللائحة (المواد من ٢ إلى ١٨). ففي هذه الطبقة تختفي متطلبات مستندية ضمنية داخل «الالتزامات الموضوعية والفنية»؛ كالتزامات المتحكم والمعالج (المواد ٣، ٤، ٥)، وضوابط البيانات الحساسة وبيانات الأطفال (١٤، ١٥)، وسياسات الإتاحة (١٦، ١٧). وتفرض هذه المواد واقعياً إنتاج مستندات وسياسات معقدة لضمها لملف الترخيص، دون النص على ذلك صراحة في القسم الإجرائي.

وبتحليل هذه المواد فإننا سنجد بعض الإشكاليات الناجمة من عدم اتساق مواد اللائحة، ومنها:

1: عدم اتساق وتماثل كل طبقة والأخرى مستنديا:

فهناك العديد من المستندات التي توجد في طبقة ولا تؤصل في بقية الطبقات، مثل مثلا ما نص عليه في الطبقة الثانية في المادة الواحدة والعشرون والتي تختص ب (شروط ترخيص / تصريح المتحكم و المعالج من الأشخاص الاعتبارية للبيانات الشخصية و البيانات الشخصية الحساسة) بضرورة (٥- تقديم سند العلاقة التعاقدية مع مسئول حماية البيانات الشخصية والمتضمنة صراحة قبوله تحمل مسئوليات مسئول حماية البيانات الشخصية ، وما يفيد التزام المتحكم أو المعالج بمنح مسئول حماية البيانات الشخصية الاستقلالية في تنفيذ مهامه بالقدر الذي يسمح له القيام بها) وهو ما اسلفنا سابقا شرط غير موجود لا في القانون ولا في اللائحة، وهو ما يتكرر في المادة الخامسة والثلاثون حيث اكتفت في البند (٨) بطلب (تحديد مسئول حماية البيانات) ، وفي البند (١) بطلب (الهيكل التنظيمي). ولم تُشر المادة إطلاقاً إلى ضرورة تقديم «عقد العمل» أو «وثيقة إثبات الاستقلالية» التي اشترطتها المادة (٢١). هذا التباين يخلق «فجوة حوكمة»؛ إذ قد يتقدم الكيان بهيكل تنظيمي يحدد اسماً لمسئول حماية البيانات مستوفياً بذلك متطلبات المادة (٣٥) شكلياً، ولكنه يُرفض موضوعياً لعدم إثبات «استقلالية» هذا المسئول وفقاً للمادة (٢١)

ويمتد هذا التعارض النصي إلى مسار نقل البيانات عبر الحدود؛ حيث تتصادم الالتزامات الموضوعية الجوهرية (التي تستلزم إعداد دراسة تقييم أثر النقل لإثبات توافر مستوى حماية مكافئ في دولة المقصد)، مع ما ورد في المادتين (٢٤) و(٢٥) الخاصتين بالاشتراطات الإجرائية، واللتين اكتفتا بطلب بيانات وصفية ومجردة (كتحديد وجهة النقل، ونظم التأمين، وأماكن التخزين). ويتعمق هذا القصور بالرجوع إلى المادة (٤١) التي جاءت صيغتها بالغة التجريد باكتفائها بطلب (أي بيانات أخرى متعلقة بنقل البيانات الشخصية عبر الحدود)، مما يفرز تعارضاً بين حتمية الالتزام الموضوعي وهشاشة المتطلب المستندي

2: السهولة الخادعة لعملية التراخيص والتصاريح:

إن اعتمدنا على واجهة المادة الواحدة والأربعون والتي تكتفي باشتراط إقرارات وبيانات أساسية مبدئية (كبيان نوع البيانات والغرض، مدد الاحتفاظ، إثبات إمساك سجل أنشطة، وبيانات النقل عبر الحدود) وأربع اقرارات منها الامتثال لقرارات المركز وغراماته وتوفير الإمكانيات التي تتيح للمركز القيام بعمليات التفتيش وضمان التزام المتعاملين بسرية البيانات، فهذا سيخلق اصطدام داخلي في بنية التراخيص

والالتزامات داخل اللائحة، كالآتي

- المادة ذاتها تنص أيضا على (يصدر النموذج إلكترونياً بعد مراجعة المتطلبات والمستندات والبيانات اللازمة)؛ مما يجعل من هذه المنصة خطوة تمهيدية تستلزم بالضرورة استيفاء التزامات أكثر تفصيلاً في المواد اللاحقة، وهو ما قد يحد من فاعلية التبسيط الإجرائي المرجو من التحول الرقمي لمنظومة التراخيص.
- لو تم تفسير هذا مع ما تم توضيحه سابقا من السلطات الموسعة للمركز حال عملية التراخيص من الرفض بدون ابداء أسباب أو طلب مستندات أو تغيير متطلبات الرخصة فإن هذا يعني للأعمال التي تريد الامتثال والترخيص الاصطدام بحواجز بيروقراطية وإدارية قد تسبب شلل في أساس تشغيلي مهم مثل معالجة البيانات الشخصية، والذي وإن كان في معظم الأحوال ليس الغرض الرئيسي للكيان، ولكنه جانب تشغيلي مهم لا يمكن ممارسة الأنشطة بالشكل الحديث بدونه.
- لو تم تصميم الواجهة والاكتفاء بإقرارات وبيانات مبسطة تفيد نية الامتثال لا التدقيق في عملية الامتثال ذاتها، فإن هذا يعني حال عدم تأسيس بنية الامتثال المعقدة ابتداء قبل الاقدام على الترخيص أن يعرض نفسه لمخاطر الوقوع في عملية ترخيص زائفة والتوقيع على اقرارات قد تعرضه لعقوبات متعددة، نتيجة عدم وجود مقابل واقعي للإقرارات والبيانات.

3: الغموض التنظيمي في آليات الوفاء بالمتطلبات:

تبرز إشكالية «الغموض التنظيمي في آليات الوفاء بالمتطلبات» كواحدة من أعمق عيوب الصياغة التشغيلية في اللائحة التنفيذية. فبينما تعاملت المواد الإجرائية (الخاصة بنماذج التراخيص) مع الالتزامات الموضوعية بشكل موحد ومبسط تحت مسميات عامة، شتتت المواد الموضوعية داخل اللائحة هذه الآليات إلى عشرات الأشكال المعقدة التي تتباين باختلاف نوع البيانات والفئة العمرية وطبيعة النشاط. هذا التناقض يضع الكيانات أمام حيرة تشغيلية بالغة: هل يُكتفى إدارياً بتقديم سياسة عامة واحدة تُغطي نشاط الكيان ضمن ملف الترخيص؟ أم يُلزم طالب الترخيص تشغيلياً بتقديم تصميمات هندسية وقانونية منفصلة لكل مسار؟

ويمكن تفصيل هذا التعقيد التشغيلي في المحورين الآتيين:

١- متاهة «آليات الموافقة» (Consent Mechanisms Labyrinth):

تعاملت اللائحة في موادها الإجرائية لطلب التراخيص مع «الموافقة» كبند إجرائي واحد؛ حيث اشترطت المادة (٤١/بند ٤) والمادة (٣٥) تقديم (بيان بآلية الحصول على موافقة الشخص المعني). بينما فرضت اللائحة في موادها الموضوعية مسارات قانونية وتقنية مختلفة للموافقات، لا يمكن دمجها فنياً في آلية مبسطة واحدة، ومنها

- الموافقة العامة: لجمع البيانات الأساسية لتلقي الخدمة (وفقاً للمادة ٢ من القانون).
- الموافقة الكتابية للبيانات الحساسة: اشترطت اللائحة في المادة (٢٤/أولاً/بند ١) موافقة صريحة «كتابية»، وهو مستوى مشدد يتطلب تقنيات متقدمة لإثبات التوثيق الرقمي.
- موافقة النقل عبر الحدود: فرضت المادة (١٦/بند ٢) الحصول على موافقة منفصلة تُضاف إلى متطلبات الكفاية الأمنية.
- موافقة التسويق الإلكتروني: اشترطت المادة (١٨) من اللائحة والمادة (٢٨) من القانون موافقة مستقلة تتطلب توفير آلية تقنية فورية للعدول (Opt-out).
- الموافقة على التتبع البصري: فرضت المادة (٣١) موافقة صريحة لاستخدام تقنيات المراقبة.
- الموافقة على المعالجة لتدريب «الذكاء الاصطناعي»: فرضت اللائحة في المادة (٤/أولاً/بند ٨) التزامات خاصة عند استخدام البيانات في «عمليات تدريب الذكاء الاصطناعي»، مما يتطلب تقنياً إفراد موافقة مستقلة أو آلية عزل للبيانات (Data Segregation).
- الموافقة للأغراض الإحصائية والبحث العلمي: وهي متطلبات استثنائية تفرض هندسياً إما إجراء تجهيل كامل (Anonymization) أو أخذ موافقة صريحة منفصلة.

٢. تعقيد وتشعب «الآليات التقنية والتنظيمية»:

لم يقتصر الغموض على الموافقات، بل امتد لـ «الآليات التقنية» التي تطلبها نماذج الترخيص بأسماء مجردة، بينما تُمثل هندسياً بنى تحتية متشابكة تشكل صعوبة غير محمودة في عملية الامتثال، ومنها

- **آليات التأمين والحماية:** تطلب المادة (٣٥/بند ٧ و٩) في مستندات التراخيص تحديد (إجراءات التأمين وطريقة التخزين). لكن اللائحة تعود لتفرض معايير متباينة؛ كالتأمين العام في المادة (٣)، والتأمين المشدد للبيانات الحساسة في المادة (٢٤)، وتأمين مسارات النقل في المادتين (٢٤ و٢٥)، وتأمين الكاميرات في المادة (٣١). بالتالي، فإن «آلية التأمين» ليست مستنداً إدارياً واحداً، بل منظومة أمنية متدرجة ومعقدة يصعب حصرها في خانة ورقية واحدة بنموذج الترخيص.
- **الآلية المجهولة لـ «تحديد الحجم والغرض» (للمعالجين):** ألزمت اللائحة (المعالج) صراحة في المادة (٤/أولاً/بند ٤) بـ (إعداد آلية يتم اعتمادها من المركز تحدد حجم البيانات الشخصية والغرض من المعالجة). هذا النص يمثل قمة الغموض الهندسي؛ فهل هو مجرد «نظام فوترة» (Billing System) لاحتساب الرسوم الإدارية؟ أم هو تطبيق فني لمفهوم «الخصوصية بالتصميم» لضمان عدم تجاوز تعليمات المتحكم؟ وكيف يتم احتساب أو تقييد هذا «الحجم» سلفاً في ظل تدفق البيانات الضخمة (Big Data) وتوسع الحوسبة السحابية؟
- **آليات ممارسة الحقوق ومحو البيانات:** ألزمت المادة (٣/أولاً/بند ٩) المتحكم بـ (وضع آلية معتمدة من المركز تتيح للشخص المعني ممارسة حقوقه). كما اشترطت المادة (٤١/بند ٣) الخاصة بنماذج التراخيص تقديم بيان بـ (آليات محو البيانات أو تعديلها). ويتساءل الواقع التقني: كيف سيتم إثبات واعتماد هذه الآلية إدارياً في الأنظمة الحديثة التي تعتمد على تقنيات «البيانات غير القابلة للتعديل» (مثل سلاسل الكتل Blockchain)، أو في ظل انتشار النسخ الاحتياطية (Backups) عبر خوادم موزعة جغرافياً يصعب محو البيان منها لحظياً؟

ثانيا: غلبة ميزان التنظيم الإداري على التعزيز الحقوقي:

نتيجة هيكلية اللائحة التنفيذية التي اعتمدت على ترتيب موادها طبقا للإحالات المباشرة في القانون للائحة، أفرز هذا عن بعض النتائج منها اختلال في ميزان التنظيم اللائحي والتشريعي، حيث خلت اللائحة بشكل كامل من أليات تنظيم مباشرة حقوق الأشخاص المعنية بالبيانات إلا فيما جاء في مواد الالتزامات والتراخيص من التزام المتحكم في توفير اليات تمكن الشخص المعني من ممارسة حقوقه المنصوص عليها قانونا، وعلى الرغم من النص على ضرورة موافقة المركز على هذه الأليات إلا أن هذا لا يمنع ضرورة وضع قواعد معيارية أساسية لتنظيم هذه الطلبات مفسرة أكثر للمادتين ٣٢ و ٣٣ تتعلق بالقواعد المعيارية لأليات استيفاء تلك الطلبات والحالات الأكثر تعقيدا مثل الطلبات التعسفية والمعقدة، بدلا من أن تركز اللائحة بشكل مطلق على الإحالة لقرارات إدارية تنظم وتهتم فقط بمعايير فنية للتأمين المعلوماتي

ولكنها خلت بشكل كامل من تنظيم كيفية التقدم بالشكاوى ضد المتحكم حيال اخلاله بتلك الحقوق وعدم تمكين الشخص المعني بالبيانات من ممارسة حقوقه لمركز حماية البيانات الشخصية، ونص فقط في المادة ١٨ الخاصة بالتسويق الإليكتروني المباشر على (وفي جميع الأحوال يخصص المركز وسيلة اتصال لتلقي شكاوى المواطنين المتعلقة بالتسويق الإلكتروني المباشر سواء من خلال موقعه الإلكتروني أو أرقام هاتفية مختصرة)، وهو خلل جوهري حيث حصر التزام المركز بتوفير ألية للشكاوى على هذه الحالة المحددة

كما لم تنص هذه اللائحة على أي أليات لحماية الحق في البيانات الشخصية والحقوق المكونة له كحقوق لصيقة بالشخصية بالاستفادة من المادة الواحدة والخمسون من القانون المدني المصري، مثل اليات انفاذ قرار مباشر من المركز لوقف معالجة البيانات الشخصية بشكل فوري لحين البت في الطلب المقدم من الشخص المعني بالبيانات

وهناك أيضا انعدام وجود أليات للتظلم من قرارات المركز في حين توسعت اللائحة خارج نطاق القانون في صلاحيات المركز، وهو ما يزيد من خلل الميزان الحقوقي الموجود في القانون واللائحة

ثالثاً: اختزال مفهوم "حماية البيانات" في الجانب الأمني (السرية والتأمين) وإهمال دورة المعالجة:

من أبرز مظاهر الخلل الهيكلي في اللائحة التنفيذية، اختزالها لمفهوم «حماية البيانات الشخصية» (Data Protection) في جانبه التقني الضيق المتمثل في «أمن وسرية البيانات» (Data Security & Confidentiality)، متجاهلةً أن الأمن هو مجرد أداة واحدة من أدوات الحماية الشاملة. فقد طغى الهاجس الأمني ومكافحة الاختراق على صياغة الغالبية العظمى من مواد الالتزامات والتراخيص، مما حول اللائحة إلى ما يشبه «تعليمات تشغيلية للأمن السيبراني» بدلاً من تشريع متكامل لضمان حماية البيانات الشخصية والحق في الخصوصية في كافة مراحل دورة حياة البيانات (جمع، معالجة، مشاركة، إتلاف)

ويمكن الاستدلال على هذا التكييف القاصر وما يمثله من «اختزال تقني» (Technological Reduction-ism) من خلال تتبع تركيز اللائحة المكثف على تفاصيل البنية التحتية والتدابير التقنية في المواد الآتية

- **المواد (٢، ٣، ٤) - طغيان الطابع الهندسي وتحويل المفتشين لمدققين أمنيين:** ركزت الإجراءات والسياسات الخاصة بالمتحكم والمعالج على حفظ البيانات بصورة (غير مقروءة مشفرة)، وتأمين الأجهزة والوسائط؛ متجاهلة الأنظمة الإدارية ومبادئ «الخصوصية بالتصميم» (Privacy by Design). وامتد هذا الخلل ليُحول دور مفتشي المركز إلى دور «المدقق التقني الأمني» (Technical Security Auditor)؛ حيث حصرت المواد (٣ و٤) مهامهم التفتيشية في التأكد من تطبيق المعايير القياسية لتأمين البيانات والأجهزة، بدلاً من تكريس دورهم الأصيل كـ «مراقبي امتثال قانوني» (Legal Compliance Officers) يتحققون من مشروعية الغرض وسلامة الإجراءات.
- **المادتان (٥ و ٦) - التكييف الأمني الجنائي لاختراقات البيانات:** تم تكريس التزامات المتحكم والمعالج والمركز لكيفية الإبلاغ والتدابير العاجلة لمواجهة خرق البيانات بمنظور أمني يربط الحوادث الكبرى بجهات الأمن القومي، متجاهلة المعيار الحقوقي الأهم وهو تقييم «الضرر الواقع على حقوق وحريات الأفراد» جراء الاختراق لتحديد آليات الإبلاغ.
- **المواد (٧، ٩، ١١، ١٢) - العقلية الهندسية في تقييم مسئول حماية البيانات:** تعاملت اللائحة مع «مسئول حماية البيانات» (DPO) وكأنه مهندس شبكات يُقاس عمله بـ «الحجم»؛ حيث اشترطت هذه المواد تحديد «حجم وطبيعة البيانات المسموح له التعامل عليها» كشرط لقيده وتحديد نطاق عمله. هذا يمثل تعارضاً مهنياً جسيماً واختزالاً لدوره؛ فعمل المسئول هو وظيفة رقابية وقانونية لضمان الامتثال، ولا يقوم فيها بمهام فنية مادية لتأمين البيانات لكي يتم تقييدها بالسعة أو الحجم.
- **المادة (١٣) - الخلط مع قوانين مكافحة الجرائم السيبرانية:** غلب الطابع الجنائي والأمني على اللائحة حيث خصصت هذه المادة بالكامل لاشتراطات «الدليل الرقمي» الجنائية بمعرفة جهات التحقيق. هذا الدمج المأخوذ من قانون مكافحة جرائم تقنية المعلومات يؤكد نظرة اللائحة للموضوع من زاوية جنائية، متجاهلة وجود تحديد دقيق لتلك المعايير في اللائحة التنفيذية ل قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، مما كان من الأجدى اسقاط الإحالة القانونية اللازمة على الدليل المدني والتجاري المستقى من البيانات الشخصية لتفادي التعارض أو التكرار التشريعي، واكمال الفجوة التشريعية المصرية[٥٢].
- **المواد (١٦، ٢٤، ٢٥) - النظرة المادية لنقل البيانات عبر الحدود:** قصرت اللائحة معايير تراخيص نقل البيانات للخارج على «التتبع المادي الجغرافي»، مشترطة بيان نظم التأمين وأماكن التخزين المؤقتة والنهائية (كأصول مادية)، وتجاهلت الجانب القانوني الحقوقي الأهم كاستيفاء «القواعد المؤسسية الملزمة» (BCRs) التي تضمن التزام الشركات بحقوق الأفراد قانونياً بغض النظر عن مكان الخادم الفعلي.
- **المادة (٣١) - المراقبة البصرية كأداة أمنية خالصة:** كيفت اللائحة استخدام كاميرات المراقبة (CCTV) من منظور أمني بحت يركز على تأمين مداخل المحال وحماية التسجيلات من الاختراق، وأهملت تماماً حقوق الأشخاص المعنيين (كحق الفرد في النفاذ للفيديو الذي يظهر فيه، أو وضع حد أقصى لمدة الاحتفاظ بالتسجيلات يراعي الخصوصية).

٥٢ قرار رئيس مجلس الوزراء ١٦٩٩ لسنة ٢٠٢٠ باللائحة التنفيذية للقانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، م ٩، ١٠.

- **المادتان (٣٥ و ٣٧) - تحويل التراخيص إلى تدقيق فني (IT Audit):** اشترطت للحصول على التراخيص والتصاريح تقديم تفاصيل فنية معقدة عن (أنواع الأجهزة المستخدمة، تصنيف مركز البيانات، والشهادات والاعتمادات الفنية للبنية التحتية، وتحديد طرق التخزين بشكل ساكن يتجاهل الطبيعة السحابية). وهي تفاصيل تتعلق بتأمين البنية التحتية المادية والبرمجية، وتُرسخ فكرة أن الامتثال هو مجرد امتلاك أجهزة معتمدة، متجاهلة أن جوهر حماية البيانات يتعلق بتكييف عقلية وسلوكيات القائمين على المعالجة التزاماً بالمنظومة القانونية.

في المقابل، جاءت صياغة اللائحة مبسترة وضعيفة جداً فيما يتعلق بباقي المبادئ الحاكمة لدورة حياة البيانات، مثل: آليات ضمان (جودة ودقة البيانات)، ضوابط حقيقية تمنع الكيانات من خرق مبدأ (تقليل البيانات - Data Minimization) عبر جمع بيانات تزيد عن الحاجة الفعلية، أو وضع أطر تنظيمية تضمن فاعلية ممارسة (حقوق الشخص المعني) في الوصول والاعتراض، مما يفرغ الحماية من مضمونها الحقوقي والإداري لحساب الإجراءات التقنية المجردة

رابعاً: التناقض المنهجي بين الامتثال لـ "القوانين القطاعية" ومعالجة "البيانات الإضافية":

يُعد التنظيم اللائحي للعلاقة بين أحكام قانون حماية البيانات والقوانين القطاعية الخاصة من أبرز مواضع التناقض الداخلي في اللائحة التنفيذية؛ حيث أفرزت الصياغة إشكالية منهجية توسع من سلطة الكيانات في جمع البيانات بدلاً من تحجيمها التزاماً بمبدأ المشروعية وتقليل البيانات

ويبرز هذا التناقض بشكل متطابق في المادة (٣/أولاً/بند ٨) الخاصة بالضوابط الفنية لـ «المتحكم»، والمادة (٤/أولاً/بند ٨) الخاصة بالتزامات «المعالج». فقد ألزمت اللائحة كليهما بجمع (حجم ونوعية البيانات الشخصية التي يتيح القانون المنظم لنشاطه الحصول عليها). ورغم وجاهة هذا المبدأ، إلا أن اللائحة نقضته في الشطر الثاني من ذات المادتين بالنص على: (وأن تطبق القواعد والضوابط المقررة في القانون على أي بيانات شخصية إضافية حال طلبه لها بما في ذلك قواعد الحفظ والتأمين والنقل، وذلك حال خلو القانون المنظم لنشاطه من تلك القواعد والضوابط)

وبالتحليل القانوني والفني لهذا النص، تتكشف عدة إشكاليات تشريعية يمكن إجمالها في النقاط الآتية

أ. شرعنة جمع البيانات الإضافية وتجاوز مبدأ "التقليل":

إن منح الكيانات ترخيصاً لائحياً بطلب «بيانات شخصية إضافية» تتجاوز نطاق ما تتيحه قوانينها القطاعية، يُفرغ مبدأ «تقليل البيانات» (Data Minimization) من مضمونه. فهذا التناقض الداخلي يمنح غطاءً لجمع بيانات غير ضرورية للنشاط الأصلي للكيان

ب. تجزئة المظلة الحمائية للبيانات:

بإعمال قاعدة «مفهوم المخالفة»، فإن قصر تطبيق ضوابط قانون حماية البيانات على (البيانات الإضافية فقط) وفي حالة (خلو القانون القطاعي منها)، يوحي باستبعاد «البيانات الأساسية» -التي تُجمع بموجب القوانين القطاعية- من المظلة الكاملة لقانون حماية البيانات. ففي القطاعات الحيوية (كالقطاع الطبي أو قطاع الاتصالات)، قد تُحرم البيانات الأساسية الحساسة من معايير الحماية الحديثة بحجة خضوعها لقانون قطاعي قديم ومتقادم، وهذا نتيجة واحدية بنية شرعية المعالجة في اللائحة على الموافقة واهمالها للتوسع القانوني الخصا بالغرض الشرعي نتيجة الالتزام القانوني او المعالجة لأغراض قانون معين، وهو ما كان سيعني مؤامة حقوق الشخص المعني في البيانات طبقا لأغراض هذا القانون القطاعي الأساسي، لا استبعاد مجمل حقوق الشخص المعني بالبيانات

ج. قصور التكييف الفني لعمل "المعالجين":

إن سحب هذا الالتزام بحذافيره على «المعالج» (في المادة ٤/أولاً/بند ٨) يعكس قصوراً في إدراك الطبيعة الفنية لعمل مقدمي الخدمات التقنية (مثل مزودي الحوسبة السحابية). فالمعالج لا يخضع بطبيعته لقانون قطاعي يحدد له «حجم ونوعية» البيانات المسموح بجمعها، بل يقتصر دوره فنياً وتعاقدياً على معالجة البيانات التي يعهد بها إليه «المتحكم»؛ مما يجعل تطبيق هذا النص على المعالجين غير قابل للتصور من الناحية التشغيلية والفنية

المطلب الثاني

الكلفة والتكاملية التقنية والاقتصادية للائحة

تعتبر معايير الموازنة بين سلاسة سير الأعمال والحقوق الفردية أحد أهم معايير حسن التشريع الرقمي الحديث. ومن ناحية أخرى، لا يمكن إنكار حاجات الدول للتوسع الاستثماري وجذب الاستثمارات الرقمية والتقنية الناشئة لتعزيز الأعمال، وأيضاً تقديم تلك التقنيات لحلول لإشكاليات عديدة يمكن حلها بسهولة أكبر فور تبني منظومات تقنية حديثة. ونتيجة لهذه الحاجات، زادت حاجة الدول للتوائم مع تلك المعايير الدولية المستقرة لأقصي درجة ممكنة لتحقيق عامل جذب استثماري من خلال قوانين تلق نوع من التوائم مع تلك المعايير بأقصى درجة لا تخل بأسس التنظيم التشريعي الوطني

وفي هذا المطلب سنلقي نظرة عن مدي نجاح اللائحة في التحقيق هذه التوافقية، في نقطتين كالاتي:

أولا: قياس الاتساق مع المعايير الفنية العالمية (قابلية الامتثال الفني وأثرها):

ثانيا: قياس الاتساق مع معايير الاقتصاد الرقمي العالمية وسير الاقتصاد الرقمي (قابلية الامتثال الاقتصادي وأثره):

أولا: قياس الاتساق مع المعايير الفنية العالمية (قابلية الامتثال الفني وأثرها):

تكشف القراءة الفاحصة للائحة التنفيذية عن وجود فجوة حقيقية بين النصوص القانونية والطبيعة الفنية والتقنية المعاصرة لنظم معالجة البيانات الشخصية. ويُعد غياب مبدأ «الحياد التقني» (Technological Neutrality) من أبرز مظاهر هذا القصور؛ حيث تبنت نصوص اللائحة منظوراً هندسياً تقليدياً وجامداً يتجاهل واقع التشغيل الرقمي. وقد أفرز هذا التوجه نصوصاً تتصادم مباشرة مع الواقع، وتخلق حالات من «الاستحالة العملية» في الامتثال، وهو ما يتضح من خلال تحليل الإشكاليات الآتية

أ. مركزية القرار الفني والجمود التشغيلي:

تبرز إحدى أهم إشكاليات اللائحة في تماشيها مع البنية الفنية للأنظمة الرقمية؛ حيث اعتمدت على آلية «الإحالة لتنظيمات مستقبلية»، ملزمةً الكيانات باتخاذ برامج تأمينية وإجراءات سيصدرها «المركز» لاحقاً (المادة ٢٢). هذا الربط التنظيمي يخلق فجوة زمنية خطيرة بين التهديد السيبراني اللحظي والقرار الإداري البطيء، ويتعارض جذرياً مع مبادئ «المرونة السيبرانية» (Cyber Resilience) التي تتطلب تكتيكات متغيرة[٥٣]. فضلاً عن ذلك، فإن فرض أساليب تقنية محددة يطرح إشكالية قانونية حول مسئولية المركز الإدارية (الخطأ المرفقي التنظيمي) حال ثبوت ضعف هذه المعايير أمام الهجمات[٥٤].

53 ENISA (European Union Agency for Cybersecurity), «Guidelines on assessing the security of personal data processing», 2021. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Online%20Platform%20for%20Security%20of%20Personal%20Data%20Processing.pdf

54 Rebecca Crootof, International Cybertorts: Expanding State Accountability in Cyberspace, 103 Cor-

وامتد هذا الجمود لاشتراط الموافقة المسبقة على استيفاء بيانات تفصيلية عن (أنواع الأجهزة المستخدمة) وطرق التخزين (المادتان ٣٥ و٣٧). هذا الشرط يُحوّل العمليات التقنية الروتينية لفرق تكنولوجيا المعلومات (كتحديث الخوادم لزيادة السعة Scalability) إلى إجراء قانوني معقد، ويتعارض مع الاتجاه العالمي الذي يمنح الشركات مرونة استخدام «أحدث ما توصلت إليه التقنية» (State of the Art) وتحديث دفاعاتها فوريا[٥٥].

ب. الاختزال التقني وغياب مبدأ "الخصوصية بالتصميم" (Privacy by Design):

تعاني اللائحة التنفيذية في مجملها من ظاهرة «الاختزال التقني» (Technological Reductionism)؛ حيث حصرت مفهوم حماية البيانات الشخصية في شقه الفني الضيق المتمثل في «السرية والتأمين» ومكافحة الاختراقات. وهذا التوجه يتصادم مع المفهوم المعاصر لحماية البيانات، والذي لا يقتصر على تأمين الخوادم، بل يعتمد على «تكامل متوازن» بين ثلاثة مسارات متوازية (هندسية، وإدارية، وقانونية)، وهو ما فشلت اللائحة في استيعابه على النحو الآتي

١. المسار التقني والهندسي (معمارية النظم بدلاً من الأقفال اللاحقة):

لا يقتصر الامتثال التقني على التشفير أو الجدران النارية اللاحقة، بل يتطلب دمجاً مسبقاً لضوابط الخصوصية في البنية المعمارية للنظم منذ المراحل الأولى لتطويرها، وهو ما يُعرف بمبدأ «الخصوصية بالتصميم» (Privacy by Design)[٥٦]. غاب هذا المبدأ تماماً عن اللائحة، كما غاب الإلزام بإجراء «التقييم المسبق للمخاطر» (DPIA)[٥٧].

فتبني هذه المفاهيم الهندسية هو ما يضمن تحقيق الالتزامات الجوهرية كـ «تقليل البيانات»، و»الحد من الغرض»، وتصميم آليات التتبع، واللجوء للتخزين البارد (Cold Storage) بعد انتهاء الغرض. فالأمر هنا لا يقتصر على شراء برامج حماية جاهزة، بل يتعلق بـ «هندسة عقلية المعالجة ومساراتها» بشكل استباقي ووقائي

٢. المسار الإداري والبشري (حوكمة دورة العمليات):

يتكامل الجانب الهندسي حتمياً مع بناء مسار إداري شامل؛ يعتمد على وضع سياسات تنظيمية داخلية، وتدريب مستمر للعناصر البشرية، وتصميم آليات لاحتساب المخاطر وتقييم الأثر التشغيلي على الأعمال. هذا الجانب لا علاقة له بالتشفير أو أمن الشبكات، بل يتعلق بـ «إدارة وحوكمة» دورة حياة البيانات (Data Lifecycle Management) وضمان وعي العنصر البشري الذي يُعد أضعف حلقات سلسلة حماية البيانات[٥٨]، وهو بُعد تجاهلته متطلبات التراخيص اللائحية التي ركزت على «الآلات» وأهملت «السياسات والأفراد».

٣. المسار القانوني (المظلة الحاكمة للامتثال):

أخيراً، يمثل المسار القانوني حجر الزاوية والمظلة التي ترسم الطريق لباقي الأطراف. فالتشريع هو الذي يضع حدود المشروعية، ويحدد فترات الاحتفاظ، ويُعرّف حقوق الأشخاص المعنيين. وبدون إطار قانوني حقوقي واضح ينظم «شرعية الجمع» ذاته (كغياب آليات الموافقة الصحيحة أو التوسع في الاستثناءات)، تصبح كافة التدابير التقنية والإدارية السابقة بلا قيمة؛ لأن النظام قد يكون «آمناً ومشفراً» من الناحية السيبرانية، ولكنه في الوقت ذاته «منتهكاً للخصوصية» من الناحية القانونية

---

nell L. Rev. 565 (), Available at: https://scholarship.law.cornell.edu/clr/vol103/iss3/2
55 GDPR, Article 32
56 GDPR, Article 25
57 GDPR, Article 35
58 NIST. (2020). The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0, pp. 2-3

ج. إغفال "حيادية البنية التحتية" وتجاهل معمارية الحوسبة السحابية (CloudComputing):

تصطدم مواد اللائحة -لا سيما المادة (٢٦) لنقل البيانات عبر الحدود، والمادة (٤) لالتزامات المعالج- بالطبيعة الفنية لخدمات الحوسبة السحابية؛ حيث تعاملت مع البيانات بمنطق «الحيازة المادية» الثابتة. هذا النهج يتجاهل آليات «توزيع الأحمال» (Load Balancing) التي تعتمد على التغيير الجغرافي اللحظي للخوادم[٥٩]. كما أن إلزام مقدمي البنية التحتية كمعالجين بتقديم آليات تحدد «الغرض من المعالجة» يتصادم جذرياً مع مبدأ «حيادية البنية التحتية» (Infrastructure Neutrality)[٦٠]. فمزود الخدمة السحابية (IaaS) يوفر بنية قياسية موحدة (Resource Pooling)[٦١]، ولا يملك عادةً صلاحية النفاذ لمعرفة محتوى البيانات لمعرفة الغرض منها، مما يجعل هذا الالتزام خلطاً تشريعياً بين الوسيلة التقنية وغرض المتحكم

د. تقادم اليات الامتثال للحقوق وعدم تناسبها مع التقنيات الأحدث:

تفرض اللائحة في المادة (٣) والمادة (٦) التزاماً حرفياً بـ «المحو الفوري» للبيانات كمسار وحيد لإنهاء الاحتفاظ بها. هذا التوجه المادي يتجاهل التقنيات الحديثة القائمة هندسياً على «استحالة التعديل» أو الحذف، كسلاسل الكتل (Blockchain) ووسائط القراءة لمرة واحدة (WORM)[٦٢]، حيث يستحيل تقنياً حذف سجل بيانات واحد دون إتلاف السلسلة الرقمية بالكامل. وفي حين تعتمد المعايير العالمية مفهوماً مرناً يتيح بدائل كالتحييد أو «الوضع خارج الاستخدام» (Put Beyond Use) وإعدام مفاتيح التشفير[٦٣].

وأيضا يمتد بوضوح إلى أنظمة الذكاء الاصطناعي (AI) وتدريب نماذج «تعلم الآلة» (Machine Learning). فبمجرد معالجة البيانات الشخصية لتدريب الخوارزميات، تندمج خصائص تلك البيانات وتتحول إلى «أوزان ومعلمات رياضية» داخل الشبكات العصبية للنموذج. وإذا طلب الشخص محو بياناته، فإنه يُمكن تقنياً حذف السجل من قاعدة البيانات الخام، ولكن يستحيل عملياً استخلاص أو محو «الأثر الرياضي» لتلك البيانات من النموذج المُدرب سلفاً -وهي معضلة تُعرف هندسياً بـ (Machine Unlearning)- دون الاضطرار لإعادة تدريب النموذج بالكامل من الصفر، وهو أمر باهظ التكلفة وشبه مستحيل تشغيلياً[٦٤].

ه. إشكاليات ألية احتساب الرسوم وتقدير رسوم الرخص:

تبنت اللائحة في المادة (٤) التزاما على المعالج بتنبي ألية لتقدير حجم البيانات الشخصية والغرض من المعالجة، وهي ما ترجمته (المواد ١٩ و٢٠) الخاصة بجداول الرسوم بنهج يعتمد على ربط الرسوم « عدد السجلات الخاصة بالبيانات الشخصية للأفراد»، وهو ما يثير عددا من الإشكاليات، من أهمها

59 Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), Special Publication 800-145, p. 6,

60 ibid

61 European Data Protection Board (EDPB). (2020). Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, p. 25-28

62 Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?. European Parliamentary Research Service (EPRS), PE 634.445, pp. 66-70

63 CNIL (Commission Nationale de l›Informatique et des Libertés). (2018). Solutions for a responsible use of the blockchain in the context of the GDPR, p. 8-9.

64 European Data Protection Supervisor (EDPS). TechSonar: Machine Unlearning. Technology Monitoring. Available at: https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/machine-unlearning_en

لم تحدد اللائحة المقصود بعدد السجلات هل هي المعالجة الجارية أم كم السجلات بما فيها سجلات الأرشيف البارد أو المجهلة أو المشفرة التي يتم الاحتفاظ بها خارج مسار دورة المعالجة لأغراض الامتثال القانوني أو غيرها

يمثل هذا التوجه عائقاً تشغيلياً بالغ الصعوبة؛ ففي ظل تقنيات إنترنت الأشياء (IoT) والتدفق السحابي المستمر، يستحيل عملياً إحصاء حجم البيانات بشكل دقيق وثابت ومسبق[٦٥].

يتعارض هذا مع النهج في شقيه بطبيعة البيانات المشفرة والمجهلة فهل يجب فك تشفيرها لتحديد الغرض منها وطبيعتها[٦٦].

يُعد تجميع وتخزين «خريطة البيانات الواصفة» في نظام فوترة مركزي بمثابة خلق «بؤرة استهداف عالية القيمة» للمخترقين (High-Value Target). فبدلاً من أن تُسهم اللائحة في تشتيت وتأمين البيانات، فإنها تُجبر الكيانات على بناء مستودع مركزي يكشف للمخترق ماهية البيانات الموجودة، وأين تقع، وما هو حجمها؛ مما يجعله بمثابة كنز معلوماتي أو نقطة إخفاق مفردة (Single Point of Failure) تُسهل على المهاجمين رسم خطط الاختراق وتحديد الأهداف بدقة بالغة. وهو ما يتناقض جذرياً مع مبادئ «التقليل» و»الفصل الشبكي» (Network Segmentation) المعتمدة لحماية قواعد البيانات[٦٧].

وقد كان يمكن تفادي هذا بأكثر من طريقة بدلا من تلك الطريقة الفنية والتي قد تتناسب مع عمليات الفوترة في قطاع الاتصالات مثلا، ولكن لا تتناسب مع طبيعة قوانين حماية البيانات الشخصية ومعالجتها، حيث أن نظم الفوترة عادة ما تعتمد على الاحتفاظ الطويل بالبيانات الواصفة وهو ما وصفه حكم محكمة العدل الدولية (Digital Rights Ireland Ltd v Minister for Communications) بانه خرق لقواعد حماية البيانات الشخصية[٦٨].

و. الخطأ التقني في معالجة طلبات إيقاف "التسويق الإلكتروني":

ألزمت المادة (٢٨) المُرسل بمحو بيانات العميل «فوراً» عند طلبه وقف الاتصال. ورغم وجاهة الهدف، إلا أن هذا النص يخلق أثراً عكسياً؛ فعملية «المحو التام» تمنع الكيان من إدراج العميل في «قوائم الحظر» (Suppression Lists)[٦٩]. وهذه القوائم ضرورة هندسية لضمان تذكر النظام لقرار العميل. ومحو البيانات تماماً يرفع خطر إعادة استهداف العميل ومراسلته مجدداً بالخطأ إذا تم جمع بياناته لاحقاً من مصدر آخر.

ن: الجمود التشغيلي وعرقلة قابلية التوسع (Scalability):

اشترطت المادتان (٣٥) و(٣٧) ربط الموافقة على التراخيص والتصاريح باستيفاء بيانات فنية تفصيلية عن البنية التحتية، ومنها التحديد المسبق لـ (أنواع الأجهزة المستخدمة). يُسفر هذا الشرط التنظيمي عن تحويل العمليات التقنية الروتينية لفرق تكنولوجيا المعلومات -كتحديث الخوادم أو ترقية نوعية الأجهزة لزيادة القدرة الاستيعابية- إلى «إجراء قانوني معقد» يستوجب بالضرورة تعديل الترخيص

يُمثل هذا التوجه عبئاً إدارياً مفرطاً يخنق التطور التقني للشركات ويحد من ديناميكية الأعمال، لتصادمه

65 NIST. (2015). NIST Big Data Interoperability Framework: Volume 1, Definitions, Special Publication 1500-1, p. 4.

66 GDPR Recital 26.

67 ENISA. (2014). Privacy and Data Protection by Design – from policy to engineering, Section 3.1.3 (Strategy: Separate), p. 16, Available at: https://www.enisa.europa.eu/sites/default/files/publications/Privacy%20and%20Data%20Protection%20by%20Design.pdf

68 Court of Justice of the European Union (CJEU), Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, [2014] ECLI:EU:C:2014:238, paras 26-27, 37.

69 nformation Commissioner›s Office (ICO). (2018). Direct Marketing Guidance, Section: «What should we do if someone objects to marketing?», Available at: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/respect-peoples-preferences/#whatdowe1

مع المبدأ العالمي المستقر لـ «الحياد التقني» (Technological Neutrality) في قوانين حماية البيانات؛ والذي يرفض تقييد الكيانات بقوائم مادية جامدة، ويكتفي بإلزامها باتخاذ التدابير التقنية والتنظيمية المناسبة للمخاطر[٧٠].

وتبرز خطورة هذا الجمود التشريعي في وضعه للشركات أمام «معضلة قانونية وتشغيلية» حقيقية؛ فإذا بادرت الشركة بتحديث بنيتها التحتية لتوفير حماية سيبرانية أكبر، أو لتوسعة أعمالها استجابةً لمتطلبات السوق والتعاقدات التقنية المستحدثة، فإنها ستُجبر إما على الدخول في غمار الدورة البيروقراطية المعقدة لتعديل الرخصة، أو المخاطرة بالوقوع تحت طائلة العقوبات المالية الجسيمة المقررة بموجب (المادة ٤١) من القانون الأم، وذلك لمجرد مخالفتها الإدارية لـ «اشتراطات وبيانات الرخصة»

و: الصعوبة الهندسية في التتبع المكاني للبيانات:

ألزمت المادة (٢٤ / البند ٤ و ٧) طالب الترخيص بتقديم بيانات تفصيلية تحدد «الوجهة النهائية» للبيانات، و»أماكن التخزين المؤقتة» (Temporary Storage) أو مسارات العبور. وهو شرط لا يمكن تحقيقه عملياً إلا في حالات «النقل الخطي المباشر» (Point-to-Point Transfer)، وهو نموذج تقني متقادم لم يعد يُعتمد عليه بشكل كبير في الوقت الراهن؛ وذلك نتيجة تزايد الاعتماد على بيئات «الحوسبة السحابية الموزعة» (Distributed Cloud Computing) وشبكات توصيل المحتوى (CDNs)

ولتحيق الامتثال لهذا في سيناريوهات الحوسبة السحابية صعوبة هندسية بالغة؛ حيث تعتمد هذه التقنيات الحديثة على التوجيه الديناميكي اللحظي (Dynamic Routing) لحزم البيانات، وتوزيع الأحمال جغرافياً (Geographic Load Balancing) لضمان سرعة وموثوقية الخدمة. هذا الواقع المعماري للشبكات يجعل «التحديد المسبق والدقيق» لأماكن التخزين المؤقتة أو خوادم العبور أمراً مستحيلاً من الناحية التقنية[٧١]، مما يُحمل الشركات التزاماً قانونياً لا تملك هندسياً القدرة على الوفاء به[٧٢].

كما أن اشتراط اللائحة لترخيص يقوم على التحديد المسبق لـ «الوجهة النهائية» لنقل البيانات -بدلاً من تنظيم معايير «انسيابها الحر»- يتنافى جذرياً مع الطبيعة الهندسية لبيئات «الربط الشبكي التكاملي للأعمال» (B2B Network Integration). ففي البنى التحتية السحابية الحديثة، لم يعد النقل يتم بشكل خطي لجهة واحدة؛ بل يتم نقل وتخزين ومعالجة البيانات الشخصية عبر آليات «المزامنة اللحظية» (Re-al-time Synchronization) في أكثر من موقع جغرافي ومركز بيانات في ذات الوقت (Multi-region Architecture)، وذلك لضمان استمرارية الأعمال وتوافرية الخدمة. وبالتالي، فإن فرض إطار تنظيمي يفترض النقل لجهة محددة سلفاً هو تنظيم يفتقر للحياد التقني، ولا يستوعب واقع الشبكات التكاملية التي تعتمد على التوزيع المتزامن للبيانات عبر الحدود[٧٣].

ثانيا: قياس الاتساق مع معايير الاقتصاد الرقمي العالمية وسير الاقتصاد الرقمي (قابلية الامتثال الاقتصادي وأثره):

جاءت اللائحة في موادها الخاصة بالرسوم ناصة على منح الأنشطة ذات العدد المحدود من السجلات الدالة على نشاط محدود على البيانات الشخصية اعفاء من الرسوم، فيماي دل على اتجاه محمود في تقليل عبء الدخول للسوق وتشجيع الشركات المشائية والصغيرة والنشطة الفردية على الامتثال، وهو إن كما قلنا اتجاه محمودا يراعي البعد والأثر الاقتصادي لهذا التوجه التشريعي المصري في فرض منظومة

70 Regulation (EU) 2016/679 (GDPR), Recital 15 & Article 32, ENISA. (2021). Guidelines on assessing the security of personal data processing, Section: «The continuous nature of security and risk assessment», pp. 14-15.

71 Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), Special Publication 800-145, p. 2.

72 Cloud Security Alliance (CSA). (2017). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Domain 5 (Information Governance), pp. 48-55

73 World Economic Forum (WEF). (2020). A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Digital Economy, White Paper, Geneva, p. 12-14.

من التراخيص والتصاريح على معالجة البيانات الشخصية، إلا أن هذا التوجه حقيقة جابه وقلل من أقل الأثار فداحة لجبل الالتزامات والامتثال الموجود في اللائحة واتجاها المتشدد لفرض سيطرة انفردت بها اللائحة على جميع تفاصيل منظومة الامتثال والتراخيص والانفاذ المتعلقة بمعالجة البيانات الشخصية في مصر، وهو ما يمكن تمثيله في بعض النقاط السريعة فيما يتعلق بالأثر والقدرة الاقتصادية على الامتثال كالآتي

أ: أثر منظومة التراخيص والربط القيمي لفئات التراخيص على قدرة الشركات على التوسع

على الرغم من ترك اللائحة في المادة التاسعة عشر لمساحات بين فئات التراخيص والتصاريح تتراوح بين مائة الف بين كل فئة، ولكن نتيجة لعدم التفسير الكامل للمقصود بالملف وهل هو ينطبق على الملف المؤقت أو الدائم أم المأرشفة فإن نتيجة معايير انسياب البيانات وفروق المعاملات بين فئات الممتثلين المختلفة وأيضا بين المتحكم والمعالج (حيث يعالج المعالج كميات اكبر من البيانات الشخصية لعدد كبير من المتحكمين) قيد يكون الأثر والعائق الأكبر لهذا التكييف في النهاية هو عدم استقرار حجم البيانات والزيادة spike التي قد تحدث في سيناريوهات مؤقتة واليت قد تترك حالة من عدم اليقين التشريعي، وهو ما قد يؤذي طبيعة الاستثمار في مصر نتيجة لقل الشركات من مخاطر الامتثال القانوني

وأيضا فإن تعقد هيكلية التراخيص والامتثال التي تم شرحها من قبل من خلال تبني اللائحة لسياسة الهرم المقلوب الذي تبدو بدايته بسيطة ومحددة ولكنها تخفي في طبقاتها الأعمق درجات من التعقيد المستندي الذي يبلغ حد استحالة التنفيذ، تطرح إشكالية وأثر أعمق على قدرة الشركات الصغيرة والأنشطة الفنية والمهنية الفردية على الامتثال والترخيص

وقد يكون الحل المقترح لتجاوز إشكالية قياس وهرمية التراخيص – وهو تنظيم محمود ولازم ابتداءً لضبط القطاع – لا يكمن في القياس الفني المعقد لحجم السجلات، بل في استكمال ما بدأته اللائحة من إعفاء مالي محمود لبعض الفئات، ليمتد هذا الإعفاء ويشمل «العبء المستندي والفني» لملف الترخيص ذاته

ويتحقق ذلك من خلال تبني آلية «الامتثال المخفف» للشركات الناشئة والفئات المعفاة، بحيث يعتمد الترخيص أو التصريح على آلية الإخطار الإلكتروني وتوفير بنية مستندية بسيطة ومخففة، ترفع عن كاهل تلك الكيانات التكاليف المستترة للامتثال الفني المعقد

أما بالنسبة لتصنيف باقي الشركات والأنشطة الفردية واحتساب الرسوم، فيجب التخلي عن القياس الكمي للسجلات، والاعتماد على معيار «النهج القائم على المخاطر» (Risk-based Approach). بحيث تكون نسبة المخاطر المتوقعة (الناتجة عن طبيعة عمليات الشركة وحساسية البيانات التي تعالجها) هي المعيار الأساسي والمحدد للرسوم. ويُفرق بين هذه الكيانات بناءً على «حجم الشركة المالي» أو «قيمتها السوقية» (في حال الشركات والتطبيقات المعتمدة على نماذج الأعمال المجانية) كدليل عملي يعكس الحجم الحقيقي لعملياتها، وقدرتها على تحمل الأعباء التنظيمية دون خنق مسار نموها الاقتصادي

ب: الأجال البيروقراطية وأثرها على الأعمال:

يأتي الأثر الثاني وعدم التوافقية في تبني القانون واللائحة لمسار التصريح والترخيص المسبق في الآجال البيروقراطية التي ترافق منظومة التراخيص، وما تمثله من عائق زمني غير متبع وقد يكون غير متوقع عالميا لأي نشاط يريد دخول السوق المصري أو يتعاقد مع نشاط مصري، وهو ما يحتاج لا تغيير اللائحة ولكن تغيير المنظومة القانونية المصرية لحماية البيانات الشخصية ككل

ويعتبر نموذج التراخيص نموذجاً متطرفاً في المنظومات القانونية العالمية لحماية البيانات الشخصية، مما يخلق ما يعرف بـ «المخاطر التنظيمية» للاستثمارات الأجنبية وهي من أهم عوائق الاستثمار الأجنبي، وأيضاً ما يعرف بـ «الصدمة التنظيمية» (Regulatory Shock) حيث يصطدم المستثمر بنص تشريعي غريب كما يعرف في الفقه التجاري الأمريكي مثلا ب بتشريعات «السماء الزرقاء» (Blue

(Sky Laws

ونتيجة لهذا تخلت اللائحة العامة عن نظام الإخطار المسبق (وهو أقل أثراً من التراخيص والتصاريح) والذي كان لا يشكل عائقاً زمنياً في التوجيه الأوروبي لعام ٩٥ لحماية البيانات الشخصية، لما أثبت من تمثيله لمتطلب قانوني خانق ليس له جدوى تبرر الآثار السلبية التي يخلقها، والاتجاه ناحية نموذج الامتثال اللاحق ذي الجاذبية الأكبر استثمارياً لما يمثله من إلغاء فكرة الحواجز الاستثمارية غير الجمركية[٧٤].

ج: واحدية الامتثال في مواجهة تعدد الممتثلين:

جاءت قوانين حماية البيانات العالمية بنصوص خاصة تشجع السوق وتنوعه وتدعم الشركات الناشئة من حيث تقليل أعباء الامتثال[٧٥]. وتأتي دائماً مراجعات قوانين حماية البيانات الشخصية المستمرة لتدعيم هذ الاتجاه، ومثال ذلك المراجعة المعاصرة لحزمة التشريعات الرقمية في الاتحاد الأوروبي (Digital Omnibus)، والتي تهدف أساساً إلى تقليل الأعباء الروتينية وتكلفة الامتثال المتراكمة على الشركات الأوروبية[٧٦].

وفي نفس الوقت، نجد أن اللائحة التنفيذية لقانون حماية البيانات الشخصية تفرض عبئاً متراكماً للامتثال على كافة الأشخاص الطبيعية والاعتبارية بغض النظر عن حجمها وقدرتها عليه، بدون تقديم بنية متدرجة من الامتثال (Tiered Compliance)، مثل ما يُتبع ويُنصح به عادةً عالمياً أثناء سن القوانين ذات الأثر الكبير على السوق والأنشطة المتنوعة كقانون حماية البيانات الشخصية

ويتجلى غياب مبدأ "التناسب الاقتصادي" بوضوح في المادة (٣٧ / البند ٨ و ٩)؛ حيث فرضت اللائحة على الأشخاص الطبيعيين (كالمحامين، الأطباء، أو المبرمجين المستقلين) استيفاء كراسة معقدة من البيانات الفنية عن بنيتهم التحتية، وأنواع الأجهزة، والشهادات والاعتمادات الفنية كشرط لمنحهم تصريح معالجة، وهو ما يمثل عائقا قانونيا كبيرا غير متوقع من قبل المهنيين لا يتناسب مع طبيعة عملياتهم على البيانات الشخصية

ويكمن الحل المقترح قبلا في تغيير بنية التراخيص بالنسبة للأنشطة قليلة المخاطر الحل الوحيد لتفادي المخاطر الاقتصادية الناجمة عن اللائحة

د: الحاجات اليومية لإنسياب البيانات الشخصية عبر الحدود في بيئة الأعمال الدولية

نتيجة لتطور نموذج الأعمال الدولي واعتماده على حزم برمجيات جاهزة (SaaS)، يعتبر انسياب البيانات -بما فيها البيانات الشخصية- جزءاً طبيعياً من العمل اليومي في تلك الشركات[٧٧]. ولهذا جاءت اللائحة العامة لحماية البيانات الشخصية (GDPR) بآلية تُعرف بـ «الضمانات المناسبة» (Appropriate Safe-guards)، وعلى رأسها «البنود التعاقدية القياسية» (Standard Contractual Clauses - SCCs)،

74 Regulation (EU) 2016/679 (GDPR), Recital 89, OECD. (2020). Trade and Cross-Border Data Flows, OECD Trade Policy Papers, No. 237, p. 15.

75 For example the exemption of (SMEs) from record keeping in gdpr, look: GDPR), Recital 13 & Article 30(5), look also: European Commission. (2023). SME Relief Package: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2023) 535 final), available in: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023DC0535

76 EDPB & EDPS. (2026, February 11). Digital Omnibus: EDPB and EDPS support simplification and competitiveness while raising key concerns. European Data Protection Board. Available at: https://www.edpb.europa.eu/news/news/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while_en

77 Regulation (EU) 2016/679 (GDPR), Recital 48 (Transfers within a group of undertakings for internal administrative purposes), and Article 47.

والـقواعد المؤسسيـة الملزمـة» (Binding Corporate Rules - BCRs)، تسمـح هذه الآليـة لـلشركات بتبـادل البيانـات فوراً بمجرد اعتمـاد الإدارة العليـا للشركـة أو مجموعـة الشركات لنظـام داخلـي مـلزم يوفر بنيـة توافقيـة تتمتـع بالصفـة الإلزاميـة عبر نموذج داخلـي يتم اعتمـاده من قبل الجهـة الرقابيـة لمرة واحدة، ولكن اللائحـة جـاءت فـي مادتهـا السـابعة عشر بنموذج غريب عن هذا الأصل التشريعـي كونـه صيـغ بشكل لا يتوافـق مـع النموذج العالمـي للأعمـال من ناحيـة، واضافـة شرط الترخيص من ناحيـة أخرى دون وجود نموذج للنـقل العـابر للحدود إلا نـفس النموذج القـائم علـى مبدأ الكفايـة لا النموذج القـائم علـى العـقود القياسيـة ولا والـقواعد المؤسسيـة الملزمـة» (Binding Corporate Rules - BCRs)

إن هذا النموذج لا يصطدم فحسب بالبنيـة التحتيـة للأعمـال، بل يتعـارض أيضـاً مـع متطلبـات الامتثـال فـي النظم القانونيـة الأخرى التـي تجـاوزت آليـة «الترخيص». وعلاوة علـى ذلك، ونظراً لـعدم استيعـاب القـانون المصري ولائحتـه لحـالات المعالجـة الداخليـة للبيانـات (كإدارة الموارد البشريـة)، فـإن هذا التوجـه يـعرقل عمل الأنظمـة الإداريـة والتقنيـة الأسـاسية لـلشركات -مثل أنظمـة (ERP) و(CRM)- والتـي تـقوم بمزامنـة البيانـات عبر الحدود آلياً ولحظياً[٧٨]، ممـا يُعرض الشركات لمخـاطر الوقوع فـي المخالفـة القانونيـة دون قصد

عامـة فـإن تـقييد وتشديد معـايير انسيـاب البيانـات عبر الحدود لـه اثـاره الضـارة علـى الاقتصـاد وقدرة الشركات علـى ممارسـة أعمالهـا عبر الحدود[٧٩]، بمـا يوجب تـغيير التنظيم التشريعـي لنـقل البيانـات عبر الحدود عامـة فـي اللائحـة لنسـق يتوافـق مـع القـانون المصري علـى الأقل من حيث وضـع معيـار الكفايـة كمعيـار رئيسـي مستـقل بذاتـه وبقيـة المعـايير كالالتزام التعـاقدي والموافقـة المسبقـة والاتفاقيـات الثنائيـة كأسبـاب استثنائيـة، وأيضـا وجوب ترخيص النـقل والاتاحـة للأسبـاب الداخليـة لـلشركات والأعمـال عن طريـق نموذج الاعتمـاد أو تـفسير النص القانونـي بـالترخيص انـه ترخيص اعتمـاد وثيقـة النـقل والشروط المنصوص عليهـا فـي نموذج ترخيص او تصريـح للإتاحـة منـفصل عن نموذج النـقل.

78 OECD. (2019). Trade and Cross-Border Data Flows, OECD Trade Policy Papers, No. 220, OECD Publishing, Paris, pp. 15-18 (The role of data flows in global value chains and SaaS).

79 UNCTAD. (2021). Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow, United Nations Publications, Geneva, Chapter 4 (Regulating Cross-Border Data Flows), p. 132.

الخاتمة:

تخلص هذه الدراسة النقدية للائحة التنفيذية لقانون حماية البيانات الشخصية ببعض النتائج سنقدمها كتقييم للأثر التشريعي والتطبيقي للائحة بناء على عدد من المحاور التي تناولنا تفاصيلها في متن الدراسة، ثم سنطرح بعض التوصيات لتقليل هذا الأثر وتحسين جودة النص، كالآتي

أولا: النتائج (الأثر التشريعي والاقتصادي للائحة):

أ: الأثر التشريعي ومدي الاتساق للائحة:

نتيجة لاقتصار اللائحة على هيكلية الإحالة المباشرة دون الأخذ في الاعتبار للعلاقات الداخلية بين نصوص التشريع الأصل، برزت عدة إشكاليات أساسية تغير من الهيكلية العامة للقانون وتثير مسالة عدم المشروعية للعديد من أحكامها، كالآتي:

١. على الرغم من الملاحظات العديدة التي أحاطت بالقانون المصري لحماية البيانات الشخصية، غلا أنه جاء في معظمه متبعا هدى اللائحة العامة لحماية البيانات الشخصية الأوروبية القائمة على الامتثال اللاحق دون التنظيم السابق الصارم، وهو ما حولته اللائحة من خلال بنية التراخيص والالتزامات والشروط المبالغ فيها لنص قانوني جامد غير قابل على تقديم اليات قابلة للتوسع وملائمة احتياجات العصر والتطور التقني.

٢. تجاوزت اللائحة حدود التفويض التشريعي بتعطيلها الضمني لأحكام المادة السادسة من القانون الأصلي؛ حيث حصرت مشروعية معالجة البيانات في «موافقة الشخص المعني» فقط. وتجاهلت اللائحة تماماً باقي أسباب المشروعية (كالضرورة العقدية، والالتزام القانوني، والدفاع عن الحقوق). هذا القصور امتد في البنية الإجرائية بأكملها؛ حيث اشترطت كافة نماذج التراخيص تقديم «آلية الحصول على الموافقة»، مما يهدد بإشكاليات مستقبلية في العديد من الأعمال التي تعتمد بطبيعتها على العقود أو الالتزامات القانونية، ويضعها في تعارض حتمي مع جهات الإنفاذ.

٣. استحدثت اللائحة مساراً موازياً لتوسيع سلطة «مركز حماية البيانات» من خلال استغلال «التراخيص» اذعانكأليةٍ ؛ حيث ألزمت طالبي التراخيص بالتوقيع على إقرارات بالوفاء بـ «الجزاءات المالية والتعويضات التي يقرها المركز». فميا يمثل هذا من تعارض مع اختصاصات السلطة القضائية ومخالفة للمبدأ الدستوري (لا عقوبة إلا بنص قانوني)؛ وتهدي على حدود الإحالة والتفويض والاختصاص، مما يثير اشكالية عدم المشروعية مرة أخرى ويفتح باباً واسعاً للطعون القضائية.

٤. أحدثت اللائحة ارتباكاً في تحديد المراكز القانونية؛ فاستحدثت مركزاً جديداً لم ينص عليه القانون وهو «الوسيط التسويقي»، وحملته التزامات غير واضحة المعالم. كما تداخلت التزامات «المتحكم» مع «المعالج» بشكل يخالف الطبيعة الفنية والنص القانوني الأصلي؛ حيث ألزمت المعالج بإخطار الشخص المعني بمدة المعالجة، وتحديد حجم وغرض المعالجة، وهي التزامات تقع أصيلاً على عاتق المتحكم بصفته صاحب القرار وبحكم نص القانون.

٥. حوّلت اللائحة مسئول حماية البيانات من مراقب امتثال قانوني إلى مجرد «مدقق للأمن السيبراني» وتابع إداري للمركز. فقد منحت المركز سلطة مطلقة لإيقافه وطلب تغييره دون ضمانات تأديبية، وفرضت عليه التزامات تتعلق بتطبيق السياسات التأمينية، مما يوقعه في فخ «تعارض المصالح» بين مهام التنفيذ ومهام الرقابة. كما حاولت اللائحة ترقيع غياب الضمانات التشريعية للمسئول بفرض «الاستقلالية» كبند تعاقدي في التراخيص، وهو التفاف إجرائي يفتقر للسند القانوني.

ثانياً: الأثر الاقتصادي والتقني:

بدلاً من أن توفر اللائحة بيئة جاذبة للاستثمار الرقمي، تبنت فلسفة بيروقراطية قائمة على الرقابة المسبقة، مما خلق تكلفة امتثال باهظة تُهدد تنافسية السوق المصري، وتتجسد هذه الآثار في:

٦. حصرت اللائحة مفهوم حماية البيانات في الشق الفني الضيق المتمثل في «التشفير والأجهزة»، مختزلة مفهوم حماية البيانات الشخصية الوسع القائم على هندسة بنية المعالجة الفنية والإدارية والقانونية من «الخصوصية بالتصميم» والتقييم المسبق للمخاطر مثلا، كما اشترطت تحديد أنواع الأجهزة وطرق التخزين مسبقاً في التراخيص، وهو ما يُعد «جموداً تشغيلياً» يعيق الشركات عن تحديث دفاعاتها السيبرانية فورياً، ويتصادم مع حيادية البنية التحتية للحوسبة السحابية الموزعة التي لا تعترف بالتخزين المادي الثابت، ويثير إشكاليات في مدي مسئولية المخاطبين والمركز ذاته حال الأضرار الناجمة عن الجمود والتدقيق التقني الناجم عن القرار الإداري الملزم.

٧. تبنت اللائحة نهجاً له اثاره السلبية بربط فئات التراخيص ورسومها بـ «حجم السجلات» (القياس الكمي)، مع إلزام الشركات بالتقدم لتعديل الترخيص فور زيادة عدد سجلاتها عن المصرح به. وهو ما قد ر يتناسب مع بني التقنية الحديثة من الحوسبة السحابية والبيانات الضخمة وانسيابية البيانات في عصر انترنت الأشياء والذكاء الاصطناعي.

٨. خالفت اللائحة القواعد الموجودة في القانون لنقل البيانات عبر الحدود؛ حيث دمجت بين شرط «الكفاية» و«الموافقة الصريحة» كشرطين متلازمين للنقل، متجاهلة الاستثناءات الحتمية كالعقود الدولية أو الطوارئ. كما اشترطت اللائحة التحديد الدقيق لـ «أماكن التخزين المؤقتة والنهائية» و«مسار البيانات»، وهو متطلب مستحيل هندسياً في بيئات الحوسبة السحابية المعاصرة التي توزع البيانات ديناميكياً. هذا التعقيد، مقروناً بعيوب الاتاحة عبر النماذج التعاقدية القياسية (SCCs) والقواعد المؤسسية الملزمة BCR، قد يؤثر على جاذبية السوق المصري وقدرته على جذب المستثمر الأجنبي.

٩. حددت اللائحة مدة (٩٠ يوم عمل) -أي ما يعادل أكثر من أربعة أشهر فعلية- للبت في طلبات التراخيص، مع اعتبار عدم الرد «رفضاً». هذا البطء البيروقراطي يُشكل «مخاطرة تنظيمية» تنفر رأس المال الجريء (VC) الذي يعتمد على السرعة (Time-to-market). علاوة على ذلك، فرضت اللائحة أعباء استخراج شهادات فنية معقدة عن البنية التحتية حتى على «الأشخاص الطبيعيين» (كالأطباء والمبرمجين المستقلين)، مما يدفع المهنيين والأعمال الصغيرة نحو الاقتصاد غير الرسمي هرباً من كلفة الامتثال المفرطة.

ثانيا: التوصيات:

لتقليل أثر اللائحة التشريعي والتطبيقي، ولضمان موازنة دقيقة بين الحق الدستوري في الخصوصية وجذب الاستثمارات الرقمية، تُوصي الدراسة بضرورة التدخل العاجل لتعديل اللائحة التنفيذية (أو تبني تعديلات تشريعية للقانون الأم) وفق المحاور الآتية:

١. على الصعيد التشريعي والحقوقي:

١) تفعيل تعدد أسباب المشروعية: تعديل المادة (٢) والمواد الإجرائية (كالنموذج في المادة ٤١) لتشمل كافة أسباب المشروعية المنصوص عليها في المادة (٦) من القانون الأصلي، وعدم قصر شرعية المعالجة وطلبات التراخيص على «آلية الموافقة» فقط، لضمان استقرار العقود والالتزامات القانونية للمؤسسات.

٢) إلغاء الغرامات اللائحية غير الدستورية: الحذف الفوري للإقرارات الواردة في المادة (٤١) والخاصة بموافقة طالب الترخيص على «الجزاءات المالية والتعويضات التي يقرها المركز»، التزاماً بمبدأ حصرية العقوبة بنص قانوني، واحتراماً لاختصاص القضاء المدني في تقدير التعويضات.

٣) إعادة هيكلة مهنة «مسئول الحماية (DPO)»: سحب سلطة المركز المطلقة في إيقاف المسئول دون ضمانات تأديبية (تعديل المادة ١٠). وتصحيح التزاماته في المادة (١٢) ليكون «مراقباً للامتثال القانوني ومستشاراً داخلياً»، وإعفاؤه من مهام «تنفيذ السياسات التأمينية» لمنع تعارض المصالح المهني.

٤) تأسيس آليات للتظلم والفصل في الشكاوى: سد الفراغ التشريعي باستحداث نصوص صريحة تنظم إجراءات تلقي شكاوى الأفراد في كافة الانتهاكات (وليس التسويق فقط)، مع إنشاء «لجنة تظلمات» محايدة للطعن على قرارات المركز (كرفض التراخيص أو إلغائها) قبل اللجوء للقضاء.

٢. على الصعيد التقني والمؤسسي:

٥) تبني «الخصوصية بالتصميم» وحيادية البنية التحتية: التخلي عن فرض قوائم جامدة بالبرامج وتحديد «أنواع الأجهزة»، واستبدالها بإلزام الكيانات بتبني مبادئ «الخصوصية بالتصميم» (Privacy by Design) وإجراء «تقييم الأثر المسبق» (DPIA).

٦) إعفاء مقدمي الخدمات السحابية من تحديد الغرض: تعديل المادة (٤) لإعفاء «المعالج» (كشركات التخزين السحابي) من التزام إعداد آليات لتحديد «الغرض من المعالجة»، نظراً للطبيعة المحايدة للبنية التحتية، ورد هذا الالتزام إلى صياحبة الأصيل وهو «المتحكم».

٧) تحديث آليات المحو للبيانات غير القابلة للتعديل: تعديل المادة (٣) لتسمح ببدائل تقنية لـ «المحو الفوري المادي»، مثل مفهوم «الوضع خارج الاستخدام» (Put Beyond Use) أو إعدام مفاتيح التشفير، لاستيعاب تقنيات «سلاسل الكتل» (Blockchain) وأنظمة الذكاء الاصطناعي.

٣. على الصعيد الاقتصادي والإجرائي:

٨) التحول نحو «النهج القائم على المخاطر» (Risk-Based Approach): الإلغاء الفوري لمعيار «القياس الكمي وحجم السجلات» في تصنيف التراخيص والرسوم، واستبداله بمعيار يعتمد على «حساسية البيانات ودرجة الخطورة». مع إلغاء المادة (٣٩) التي تلزم الشركات بتعديل الترخيص فور زيادة حجم بياناتها، لضمان استقرار ونمو الشركات الناشئة، والاكتفاء بالإخطار فور الحصول على الرخصة ومساواة الرسوم في دورة التجديد التالية مع وضع اليات للإعفاء حال الزيادة المؤقتة والموسمية كتشجيع للنمو.

٩) تخفيف أعباء الامتثال للمهنيين (Light-touch Regime): إعفاء «الأشخاص الطبيعيين» والأعمال الصغرى من متطلبات تقديم الشهادات الهندسية المعقدة لمركز البيانات (تعديل المادة ٣٧)، والاكتفاء بآلية «الترخيص المخفف فص صورة استمارات مبسطة مشابهة لنظام الاخطار» بدلاً من التراخيص المعقدة لتشجيع دمجهم في الاقتصاد الرسمي.

١٠) تعديل منظومة «النقل العابر للحدود»: تعديل المادة (١٦) لفك الارتباط بين «شرط الكفاية» و«موافقة الشخص»، وجعل الكفاية أساساً مستقلاً لانسياب البيانات. مع ضرورة الإسراع في اعتماد المعايير العالمية كـ «البنود التعاقدية القياسية» (SCCs) والقواعد المؤسسية الملزمة الحقيقية (BCRs)، وإلغاء متطلب التحديد المادي الجغرافي لـ «مسار البيانات ومراكز التخزين المؤقتة» للتوافق مع الطبيعة السحابية للتجارة الدولية.

قائمة المراجع

أولاً: المراجع باللغة العربية (Arabic References)

الكتب (Books)

١. الصغير م، القانون الإداري بين التشريع المصري والسعودي (المركز القومي للإصدارات القانونية ٢٠١٥).

٢. المكاوي ع، العلوم الإدارية (مؤسسة طيبة للنشر والتوزيع ٢٠١٢).

القوانين واللوائح (Laws & Regulations)

١. قانون رقم (٦٣) لسنة ٢٠٠٤ المتعلق بحماية المعطيات الشخصية (تونس)

٢. قانون رقم (٣٠) لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية (مملكة البحرين)

٣. قانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات (مصر)

٤. قانون رقم (١٥١) لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية (مصر)

٥. نظام حماية البيانات الشخصية بالمملكة العربية السعودية (المرسوم الملكي رقم م/١٩ وتاريخ ١٤٤٣/٢/٩هـ وتعديلاته)

٦. قرار رئيس مجلس الوزراء رقم (١٦٩٩) لسنة ٢٠٢٠ باللائحة التنفيذية للقانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات (مصر).
٧. قرار وزير الاتصالات وتكنولوجيا المعلومات رقم (٨١٦) لسنة ٢٠٢٥ بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية (مصر).
٨. قرار وزير العدل والشئون الإسلامية والأوقاف رقم (٤٣) لسنة ٢٠٢١ بشأن شروط وإجراءات تعيين مراقب حماية البيانات الشخصية (مملكة البحرين).
٩. اللائحة التنفيذية لنظام حماية البيانات الشخصية بالمملكة العربية السعودية (قرار رئيس مجلس إدارة سدايا رقم ٧٩٨ وتاريخ ١٤٤٥/٠٢/٢٣هـ).

ثانياً: المراجع باللغة الأجنبية (English References)

Books & Journal Articles

1. Crootof R, 'International Cybertorts: Expanding State Accountability in Cyberspace' (2018) 103 Cornell L Rev 565 https://scholarship.law.cornell.edu/clr/vol103/iss3/2 accessed 20 February 2026.
2. Hacker P, Engel A and Mauer M, 'Regulating ChatGPT and Other Large Generative AI Models' (2023) Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency.
3. Schwartz PM, 'Global Data Privacy: The EU Way' (2019) 94 NYU L Rev 771 https://www.nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-eu-way/ accessed 17 February 2026.
4. Trautmann K, 'Cloud Computing Evolution and Regulation in the Financial Services Industry' (2023) 2 ISACA Journal https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/cloud-computing-evolution-and-regulation-in-the-financial-services-industry accessed 18 February 2026.
5. Ustaran E and others, 'Data Protection and Privacy in the Age of Federated Learning' (2022) 14 Law, Innovation and Technology .
6. Veale M and Borgesius FZ, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law & Security Review https://www.semanticscholar.org/reader/8b165eba2d0b9308682fdc4d775c00d1d3907a59 accessed 18 February 2026.
7. Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2019 Columbia Business Law Review 494 https://doi.org/10.7916/cblr.v2019i2.3424 accessed 18 February 2026.

Reports, Working Papers & Institutional Guidance

1. Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP251rev.01, 2018).
2. Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers (DPOs)' (WP 243 rev.01, 2017).
3. Article 29 Data Protection Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP 218, 2014).
4. Carugati C, 'The interplay between the Digital Markets Act and the General Data Protection Regulation' (2023) Bruegel Working Paper 06/2023 https://www.bruegel.org/working-paper/interplay-between-digital-markets-act-and-general-data-protection-regulation accessed 18 February 2026.
5. Centre for Information Policy Leadership (CIPL), 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (Hunton & Williams LLP 2014).
6. Cloud Security Alliance (CSA), 'Security Guidance for Critical Areas of Focus in Cloud Computing v4.0' (٢٠١٧).
7. CNIL, 'Solutions for a responsible use of the blockchain in the context of the GDPR' (٢٠١٨).
8. de Streel A and others, 'The European Proposal for a Digital Markets Act: A First Assessment' (CERRE 2021) https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/ accessed 17 February 2026.
9. EDPB & EDPS, 'Digital Omnibus: EDPB and EDPS support simplification and competitiveness while raising key concerns' (European Data Protection Board, 11 February 2026) https://www.edpb.europa.eu/news/news/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while_en accessed 20 February 2026.
10. European Commission, 'Digital Omnibus Regulation Proposal' (Shaping Europe's Digital Future, 19 November 2025) https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal accessed 18 February 2026.
11. European Commission, 'SME Relief Package' (COM(2023) 535 final, 2023).
12. European Data Protection Board (EDPB), 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (Version 2.0, 2021).
13. European Data Protection Board (EDPB), 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation' (Version 3.0, 2019).
14. European Data Protection Supervisor (EDPS), 'Internet of behaviours' (TechSonar) https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/internet-behaviours_en accessed 18 February 2026.
15. European Data Protection Supervisor (EDPS), 'Machine Unlearning' (TechSonar) https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/machine-unlearning_en accessed 20 February 2026.
16. ENISA, 'Guidelines for SMEs on the security of personal data processing' (٢٠٢١).

17. ENISA, 'Guidelines on assessing the security of personal data processing' (2021) https://www.enisa.europa.eu/sites/default/files/publications/Online%20Platform%20for%20Security%20of%20Personal%20Data%20Processing.pdf accessed 20 February 2026.
18. ENISA, 'Privacy and Data Protection by Design – from policy to engineering' (2014) https://www.enisa.europa.eu/sites/default/files/publications/Privacy%20and%20Data%20Protection%20by%20Design.pdf accessed 20 February 2026.
19. Finck M, 'Blockchain and the General Data Protection Regulation' (European Parliamentary Research Service 2019).
20. Information Commissioner's Office (ICO), 'Direct Marketing Guidance' (2018) https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/respect-peoples-preferences/#whatdowe1 accessed 20 February 2026.
21. Information Commissioner's Office (ICO), 'Security - Guide to the UK GDPR' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ accessed 20 February 2026.
22. Mell P and Grance T, 'The NIST Definition of Cloud Computing' (National Institute of Standards and Technology 2011) Special Publication 800-145.
23. NIST, 'The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management' (Version 1.0, 2020).
24. NIST, 'NIST Big Data Interoperability Framework: Volume 1, Definitions' (Special Publication 1500-1, 2015)).
25. OECD, 'Trade and Cross-Border Data Flows' (OECD Trade Policy Papers No 220, 2019).
26. OECD, 'Trade and Cross-Border Data Flows' (OECD Trade Policy Papers No 237, 2020).
27. UNCTAD, 'Digital Economy Report 2021: Cross-border data flows and development' (United Nations Publications 2021).
28. World Economic Forum (WEF), 'A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Digital Economy' (White Paper 2020)).

Cases

1. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications [2014] ECLI:EU:C:2014:238.

Legislation

2. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1.
3. Regulation (EU) 2022/1925 (Digital Markets Act) [2022] OJ L 265/1.
4. Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L 277/1.
5. Regulation (EU) 2023/2854 (Data Act) [2023] OJ L 2023/2854.
6. Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 1689/1.
7. Regulation (EU) [2024] (European Health Data Space (EHDS) Regulation).