تقرير عن التحديث التشريعي لقانون مكافحة جرائم تقنية المعلومات وعلاقته بالذكاء الاصطناعي

بموجب المرسوم السلطاني رقم (٦١ / ٢٠٢٦) — نافذ اعتبارًا من ٢ يونيو ٢٠٢٦

مقدمة

أصدر حضرة صاحب الجلالة السلطان هيثم بن طارق المعظم المرسوم السلطاني رقم (2026/61) بإصدار قانون مكافحة جرائم تقنية المعلومات، والذي نُشر في الجريدة الرسمية رقم (1651) الصادرة في 7 يونيو 2026م، ويُعمل به اعتبارًا من اليوم التالي لنشره. يحل هذا القانون محل القانون السابق الصادر بالمرسوم السلطاني رقم (2011/12)، ويأتي في إطار مواكبة التحولات التقنية المتسارعة، وفي مقدمتها انتشار تطبيقات الذكاء الاصطناعي ومنصات التواصل الاجتماعي، وما صاحبها من أنماط إجرامية مستحدثة لم يكن التشريع السابق قد تناولها.

يهدف هذا التقرير إلى تقديم قراءة تحليلية شاملة للجوانب المتعلقة بالذكاء الاصطناعي والبيئة الرقمية في القانون الجديد، اعتمادًا على النص الرسمي المنشور في الجريدة الرسمية والتغطية الإعلامية الرسمية الصادرة عن وكالة الأنباء العُمانية ووسائل الإعلام الحكومية.

أولًا: الجهات الحكومية ذات العلاقة بتحديث التشريع

لم يصدر عن الجهات الرسمية بيان منشور يُسمّي على وجه التحديد قائمة الجهات التي شاركت في الأعمال التحضيرية لصياغة مشروع القانون قبل عرضه على مجلس عُمان وإصداره. غير أن النص الرسمي للقانون، وكذلك مسار إصداره الدستوري، يحدّدان بوضوح الجهات ذات الاختصاص المباشر في تطبيقه والتنسيق بشأنه:

- وزارة النقل والاتصالات وتقنية المعلومات (الوزارة): الجهة المسؤولة عن تطبيق أحكام القانون، ومنحها القانون صلاحية التنسيق مع الجهات المختصة للحصول على البيانات أو المعلومات الإلكترونية.
- مجلس عُمان: عُرض مشروع القانون عليه دستوريًا قبل إصداره، بحسب ما ورد صراحة في ديباجة المرسوم ("وبعد العرض على مجلس عُمان").
- الادعاء العام والمحكمة المختصة: الجهتان القضائيتان المخوّلتان بإصدار الأمر القضائي اللازم لحصول الوزارة على البيانات الإلكترونية من الجهات النظيرة.
- مركز الدفاع الإلكتروني (التابع لجهاز الأمن الداخلي): نصّ القانون صراحة على عدم الإخلال باختصاصاته باعتباره المرجع الوطني للدفاع الإلكتروني وحماية المصالح الحيوية في الفضاء الإلكتروني في السلطنة.
- الجهات الحكومية وغير الحكومية ("الجهات النظيرة") داخل السلطنة وخارجها: أشار القانون إليها بصفة عامة كأطراف يمكن تبادل البيانات الإلكترونية معها في إطار التحقيق في جرائم تقنية المعلومات، دون تسميتها بأسمائها.

ملاحظة: قائمة الجهات التي تحمل صفة "الجهات المختصة" المشار إليها في القانون (كهيئة تنظيم الاتصالات ووزارة العدل والشؤون القانونية والادعاء العام وشرطة عُمان السلطانية ومركز الأمن السيبراني، وغيرها) تُحدَّد عادة بموجب لوائح تنفيذية أو قرارات وزارية لاحقة للقانون، ولم يصدر حتى تاريخ إعداد هذا التقرير نص علني يسمّيها حصرًا. إن كان لدى الوزارة معلومة داخلية مؤكدة بشأن الجهات التي شاركت فعليًا في الصياغة، يُنصح بإدراجها بدقة بدلًا من الاعتماد على المصادر العلنية وحدها.

ثانيًا: النصوص القانونية المتعلقة بالذكاء الاصطناعي

يتضمن القانون الجديد، لأول مرة في التشريع العُماني، تعريفات صريحة للذكاء الاصطناعي وأنظمته، ويُدرج "أنظمة الذكاء الاصطناعي" ضمن مكوّنات "النظام المعلوماتي" الذي تُبنى عليه غالبية الجرائم المنصوص عليها في القانون. وفيما يلي النصوص ذات الصلة المباشرة كما وردت في المادة (١) من الفصل الأول (تعريفات وأحكام عامة):

المادة (١) — البند ٧: تعريف "النظام المعلوماتي"

> *مجموعة البرامج المعلوماتية أو التطبيقات أو منصات التواصل الاجتماعي أو أنظمة الذكاء الاصطناعي المعدة لإنشاء ومعالجة وإدارة البيانات أو المعلومات الإلكترونية المرتبطة مع بعضها البعض عبر الشبكة المعلوماتية.*

المادة (١) — البند ٨: تعريف "الذكاء الاصطناعي"

> *مجال من مجالات علوم الحاسوب، والذي يركز على تطوير تقنيات وخوارزميات وأنظمة تعمل على تحليل البيانات، والتعلم منها، ومحاكاة بعض القدرات الإدراكية البشرية مثل الرؤية، وفهم اللغة، وحل المشكلات، واتخاذ القرارات. كما يمكن لهذه الأنظمة أداء مهام معينة بناء على تحليل الأنماط واستنتاج الحلول من البيانات المتاحة.*

المادة (١) — البند ٩: تعريف "أنظمة الذكاء الاصطناعي"

> *برامج أو أجهزة حاسوبية تستخدم الذكاء الاصطناعي لأداء مهام محددة.*

الأثر العملي لهذه التعريفات: بما أن مصطلح "نظام معلوماتي" يتكرر في صياغة معظم مواد التجريم في القانون (مثل: "كل من استخدم موقعًا إلكترونيًا أو نظامًا معلوماتيًا أو وسيلة تقنية المعلومات...")، فإن إدراج "أنظمة الذكاء الاصطناعي" ضمن هذا التعريف يعني عمليًا أن جميع الجرائم التي يغطيها القانون — من التعدي على البيانات، إلى الاحتيال والتزوير، إلى جرائم المحتوى والابتزاز والانتحال — أصبحت تشمل صراحة الأفعال التي تُرتكب باستخدام أنظمة الذكاء الاصطناعي، دون الحاجة لإفراد مادة مستقلة لكل حالة استخدام.

المادة (٣٦) — الفقرة ٦ من الفصل السادس (جرائم المحتوى / الجرائم التي تمس الأسرة والمجتمع)

يُعد هذا البند الأكثر ارتباطًا المباشر بمخاطر التزييف الرقمي (Deepfake) والتلاعب بالمحتوى الذي تنتجه تقنيات الذكاء الاصطناعي، ونصه:

> *إجراء أي تعديل أو معالجة على مقطع صوتي أو مرئي أو صورة للغير، بقصد التشهير أو الإساءة إليه أو لإظهاره بطريقة من شأنها المساس بشرفه أو كرامته.*

وترد هذه الفقرة ضمن المادة (36) التي تُجرّم الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد، وتُقرّر لها عقوبة السجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على ثلاث سنوات، وغرامة لا تقل عن (1000) ريال عماني ولا تزيد على (5000) ريال عماني، أو بإحدى هاتين العقوبتين.

كما تتصل بذات السياق الفقرتان (١) و(٥) من المادة نفسها، واللتان تُجرّمان استراق السمع والتسجيل الصوتي أو المرئي دون وجه حق، وتتبع بيانات المواقع الجغرافية للغير — وهي أنماط اعتداء يتزايد ارتكابها أو تسهيلها عبر أدوات وتطبيقات ذكاء اصطناعي.

ثالثًا: صلاحيات التنسيق الأوسع مع الجهات المختصة بحماية البيانات

وردت هذه الصلاحية في المادة (٤) من الفصل الأول، ونصها الكامل:

> *مع عدم الإخلال باختصاصات مركز الدفاع الإلكتروني، يجوز للوزارة بالتنسيق مع الجهات المختصة – في حال وجود أسباب كافية بوقوع جريمة تقنية المعلومات – الحصول على البيانات أو المعلومات الإلكترونية من الجهات النظيرة، وغيرها من الجهات الحكومية وغير الحكومية في سلطنة عمان وخارجها، بناء على أمر قضائي صادر عن الادعاء العام، أو المحكمة المختصة بحسب الأحوال.*

المقصود بهذا النص عمليًا:

- الجهة صاحبة الصلاحية: وزارة النقل والاتصالات وتقنية المعلومات، وليس أي جهة تحقيق أخرى بمفردها.
- شرط التفعيل: وجود "أسباب كافية" ترجّح وقوع جريمة من جرائم تقنية المعلومات — أي أن الصلاحية ليست مطلقة، بل مرتبطة بشبهة جنائية قائمة.
- الضمانة القضائية: لا يجوز للوزارة الحصول على البيانات إلا بناءً على أمر قضائي صادر عن الادعاء العام أو المحكمة المختصة، وهو ما يوفر رقابة قضائية مسبقة على استخدام هذه الصلاحية.

- نطاق "الجهات المختصة" و"الجهات النظيرة": يشمل جهات حكومية وغير حكومية داخل سلطنة عُمان وخارجها، دون تسميتها حصرًا في نص القانون؛ ويُرجَّح أن تشمل عمليًا جهات مثل شرطة عُمان السلطانية، والادعاء العام، والجهات القطاعية المعنية بالبيانات (كالجهات التنظيمية للاتصالات والقطاع المالي)، إضافة إلى نظيراتها الدولية عبر قنوات التعاون القضائي والأمني الدولي.
- الاستثناء الصريح: نص القانون على عدم الإخلال باختصاصات مركز الدفاع الإلكتروني (الجهة الوطنية المرجعية للدفاع الإلكتروني وحماية المصالح الحيوية في الفضاء الإلكتروني، التابعة لجهاز الأمن الداخلي)، أي أن صلاحية الوزارة الجديدة مكمّلة لدوره لا بديلة عنه.

رابعًا: أهداف التحديث التشريعي

بحسب التغطية الرسمية لوكالة الأنباء العُمانية (عُمانية) التي نقلتها الصحف الحكومية عند صدور القانون، فإن القانون الجديد يأتي لتحقيق الأهداف التالية:

- تعزيز الأمن الرقمي الوطني.
- حماية المجتمع من الجرائم الإلكترونية المستحدثة.
- ضمان سرية وسلامة البيانات والمعلومات الإلكترونية.
- توفير الحماية القانونية للأدلة الرقمية.
- تحقيق الردع القانوني من خلال سنّ عقوبات رادعة للجرائم المرتكبة باستخدام وسائل تقنية المعلومات.

وتضيف قراءة النص القانوني نفسه أهدافًا ضمنية تعكسها بنية القانون، أبرزها:

- مواكبة التطور التقني: من خلال إدخال تعريفات لم تكن موجودة في قانون 2011، مثل الذكاء الاصطناعي وأنظمته، ومنصات التواصل الاجتماعي، والأدلة الرقمية، ووسيلة الدفع الإلكترونية.
- توسيع نطاق التجريم: بالانتقال من 6 فصول في القانون السابق إلى 9 فصول تضم 62 مادة في القانون الجديد، شملت أبوابًا مستحدثة مثل الجرائم المنظمة عبر تقنية المعلومات، وجرائم وسيلة الدفع الإلكتروني، وتوسيع جرائم المحتوى.
- سد الفجوة التشريعية بين النص القانوني وواقع الاستخدام: بحيث لا تبقى الأفعال التي تُرتكب عبر أدوات وأنظمة الذكاء الاصطناعي خارج نطاق التجريم بحجة عدم النص عليها صراحة.

خامسًا: طبيعة البيئة الرقمية التي أوجدتها هذه التحديثات

يمكن وصف البيئة الرقمية التي رسمها القانون الجديد بأنها بيئة أكثر تنظيمًا ووضوحًا من الناحية القانونية، تتسم بالخصائص التالية:

- بيئة معترف بها تشريعيًا بأنظمة الذكاء الاصطناعي كمكوّن فعلي من مكونات الفضاء الرقمي، لا كتقنية مستجدة خارج نطاق التشريع.
- بيئة تُدرج منصات التواصل الاجتماعي كفئة قائمة بذاتها ضمن "النظام المعلوماتي"، بما يعكس واقع أن جانبًا كبيرًا من الجرائم الرقمية اليوم يُرتكب عبرها.
- بيئة تُعلي من قيمة "الأدلة الرقمية" وتُفرد لها تعريفًا وفصلًا خاصًا (الفصل الرابع) يُجرّم الامتناع عن تقديمها أو العبث بها، بما يعزز موثوقية التقاضي في القضايا التقنية.
- بيئة تُشدد الحماية على الخصوصية الرقمية للأفراد في مواجهة أدوات التسجيل والتتبع والتعديل الرقمي للصور والمقاطع (المادة 36)، وهو ما يمس مباشرة إساءة استخدام أدوات الذكاء الاصطناعي التوليدي.
- بيئة تُتيح تعاونًا مؤسسيًا وقضائيًا منظمًا بين الوزارة والجهات المختصة محليًا ودوليًا لتبادل البيانات في إطار قضائي رقابي، بدلًا من التعامل الثنائي غير المنظم.

- بيئة توازن بين الانفتاح على أدوات التقنية الحديثة وحرية الاستخدام المشروع لها، وبين الردع القانوني الصارم لسوء استخدامها، عبر تدرّج واضح في العقوبات بحسب جسامة الفعل والجهة المتضررة (فردية أو حكومية أو مالية.

سادسًا: الأثر المتوقع للتحديثات التشريعية

فيما يلي قراءة تحليلية للآثار المتوقعة لهذه التحديثات على عدد من المحاور، استنادًا إلى مضمون النصوص القانونية ذاتها والسياق الرسمي المعلن لأهداف القانون:

١. أمن المعلومات

يعزز القانون منظومة الأمن الرقمي الوطني عبر توسيع نطاق التجريم ليشمل صراحة الأفعال المرتكبة بواسطة أنظمة الذكاء الاصطناعي ومنصات التواصل الاجتماعي، إلى جانب تشديد العقوبات على جرائم اختراق الأنظمة والبيانات الحكومية والمصرفية (المادتان 10 و11). كما يُرسّخ التكامل المؤسسي بين الوزارة ومركز الدفاع الإلكتروني والجهات القضائية، بما يحد من ازدواجية الاختصاص ويعزز سرعة الاستجابة للحوادث السيبرانية.

٢. حماية البيانات

يوفر القانون مستوى أعلى من الحماية القانونية للبيانات الشخصية والحكومية، من خلال تصنيف صريح لـ"البيانات أو المعلومات الإلكترونية الحكومية" (المادة 1، البند 4)، وتشديد العقوبة إذا كانت البيانات المعتدى عليها ذات طابع شخصي (المادة 5). كما يمنح إطارًا قانونيًا منضبطًا لتبادل البيانات بين الجهات الرسمية محليًا ودوليًا (المادة 4)، بما يوازن بين حاجة التحقيق الجنائي وضمانات الخصوصية عبر اشتراط الإذن القضائي.

٣. الاستثمار

من منظور بيئة الأعمال، يُسهم وضوح الإطار القانوني الناظم لجرائم تقنية المعلومات والذكاء الاصطناعي في رفع درجة اليقين القانوني (Legal Certainty) لدى المستثمرين والشركات العاملة في قطاع التقنية والاتصالات وريادة الأعمال الرقمية، إذ يحدد بدقة الأفعال المجرّمة والعقوبات المترتبة عليها، ويعزز ثقة المستهلكين والشركاء الدوليين في البيئة الرقمية العُمانية من خلال حماية أقوى للبيانات والملكية الفكرية (المادة 51) ووسائل الدفع الإلكترونية (الفصل السابع). في المقابل، يستلزم الأمر من الشركات، وبخاصة تلك التي تطوّر أو تستخدم أنظمة ذكاء اصطناعي، مراجعة ممارساتها للتأكد من توافقها مع الالتزامات الجديدة.

٤. الابتكار الرقمي

يرسل القانون إشارة تشريعية واضحة بأن الابتكار في مجال الذكاء الاصطناعي والتقنيات الرقمية مشمول بالاعتراف القانوني، لا مستبعد منه أو متروك لفراغ تشريعي، وهو ما يدعم استقرار السياسات الرقمية الوطنية المرتبطة بمستهدفات البرنامج الوطني للذكاء الاصطناعي والتقنيات الرقمية المتقدمة ورؤية عُمان 2040. وفي الوقت ذاته، يضع القانون حدودًا واضحة لإساءة استخدام هذه التقنيات (كالتزييف العميق والانتحال والاحتيال المعلوماتي)، بما يرسّخ مبدأ "الابتكار المسؤول" الذي يوازن بين تشجيع تطوير الحلول التقنية الجديدة وحماية الأفراد والمجتمع من مخاطرها.

خاتمة

يمثل قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61) نقلة نوعية في المنظومة التشريعية العُمانية للفضاء الرقمي، ليس فقط من حيث التوسع الكمي في عدد المواد والفصول، بل بشكل أهم من خلال دمج الذكاء الاصطناعي كمفهوم معرّف قانونًا ومندمج ضمن الأساس التعريفي الذي تُبنى عليه جميع الجرائم الواردة في القانون. وهذا النهج التشريعي – القائم على تعريف تقني جامع بدلًا من إفراد مواد خاصة لكل تقنية مستجدة – يمنح القانون مرونة أكبر لمواكبة التطورات المستقبلية في هذا المجال دون الحاجة لتعديلات متكررة.

يُوصى بمتابعة صدور اللوائح التنفيذية أو القرارات الوزارية المكمّلة للقانون، والتي يُتوقع أن تحدد بدقة أكبر الجهات المختصة المقصودة في المادة (4)، وآليات التنسيق العملي بين الوزارة والجهات النظيرة محليًا ودوليًا.

المصادر

- المرسوم السلطاني رقم (2026/61) بإصدار قانون مكافحة جرائم تقنية المعلومات — الجريدة الرسمية العدد (1651)، 7 يونيو 2026م، منشور على البوابة الرسمية للتشريعات العُمانية Qanoon.om
- جريدة عُمان الرسمية: "قانون مكافحة جرائم تقنية المعلومات.. تشريع متكامل وحماية أوسع للمجتمع"، 7 يونيو 2026م
- جريدة الرؤية العُمانية: "قانون مكافحة جرائم تقنية المعلومات يعزز الأمن الرقمي الوطني وحماية المجتمع من الجرائم الإلكترونية"، نقلاً عن وكالة الأنباء العُمانية، 1 يونيو 2026م
- موقع شؤون وطنية: "تفاصيل المرسوم السلطاني بإصدار قانون مكافحة جرائم تقنية المعلومات"، 7 يونيو 2026م
- المرسوم السلطاني رقم (2020/64) بإنشاء مركز الدفاع الإلكتروني وإصدار نظامه — Qanoon.om