دولة ليبيا

مسودة

قانون الجرائم الإلكترونية

وحماية الفضاء الرقمي

قانون رقم (___) لسنة 2026

يحلّ محل قانون رقم (5) لسنة 2022م بشأن الجرائم الإلكترونية

أعدّت هذه المسودة:

مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية

بقيادة مبادرة أنير بالتعاون مع مجتمع الإنترنت - ليبيا

مشروع اصلاح السياسات الرقمية في ليبيا

مارس 2026

وثيقة عمل للمشاورة العامة ـــ غير رسمية

ديباجة

انطلاقاً من حرص دولة ليبيا على صون الأمن الرقمي الوطني وحماية مواطنيها في الفضاء الإلكتروني، وإيماناً بأن أي تشريع في مجال الجرائم الإلكترونية لا ينبغي أن يتعارض مع حقوق الإنسان الأساسية كحرية التعبير وحق الخصوصية وسرية الاتصالات، وإدراكاً للثغرات التي رصدتها التحليلات المستقلة في قانون رقم (5) لسنة 2022م من غموض في التعريفات وتوسع في صلاحيات المراقبة وقيود على التشفير وغياب الإشراف القضائي الكافي، واستناداً إلى اتفاقية بودابست لمكافحة الجرائم الإلكترونية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتوصيات هيئات حقوق الإنسان الأممية،

صدر القانون الآتي:

الباب الأول

التعريفات والأحكام العامة

المادة (1): نطاق التطبيق

يسري هذا القانون على الجرائم المرتكبة بوسائل إلكترونية أو الواقعة على الأنظمة المعلوماتية أو الشبكات أو البيانات الرقمية، متى ارتُكبت على الأراضي الليبية أو كان أثرها فيها أو كان مرتكبها مواطناً ليبياً. ولا يُطبَّق هذا القانون خارج نطاقه الإقليمي إلا وفق اتفاقيات التعاون القضائي الدولي النافذة.

المادة (2): التعريفات

في تطبيق أحكام هذا القانون، تُعنى العبارات الآتية المعاني المبيّنة قرين كل منها:

النظام المعلوماتي: أي جهاز أو مجموعة أجهزة مترابطة قادرة على تنفيذ معالجة آلية للبيانات، بما في ذلك الحواسيب والهواتف الذكية والشبكات والأنظمة المدمجة.

البيانات الرقمية: أي تمثيل لوقائع أو معلومات أو مفاهيم في صيغة قابلة للمعالجة بواسطة نظام معلوماتي، بما في ذلك برامج تشغيل الأنظمة.

الوصول غير المصرح به: الدخول إلى نظام معلوماتي أو بيانات رقمية دون تصريح من صاحب الحق أو بتجاوز التصريح الممنوح.

الاعتراض: الرصد التقني لمحتوى الاتصالات الإلكترونية أو بياناتها أثناء الإرسال.

التشفير: تقنية تحويل البيانات إلى صيغة غير مقروءة لحمايتها من الوصول غير المصرح به.

البرمجيات الخبيثة: كل برنامج أو كود مصمم للتسلل إلى نظام معلوماتي أو إتلافه أو اختراقه أو تعطيله دون إذن.

الجريمة الإلكترونية: كل فعل يُرتكب بوسيلة إلكترونية أو يستهدف نظاماً معلوماتياً أو بيانات رقمية ويُعدّ مخالفاً لأحكام هذا القانون.

مزود الخدمة: كل شخص طبيعي أو اعتباري يوفر للمستخدمين إمكانية الاتصال بالشبكات الإلكترونية أو المعالجة أو التخزين أو الخدمات ذات الصلة.

البيانات الوصفية: البيانات الدالة على مصدر الاتصال ووجهته ومساره وتوقيته وحجمه دون أن تتضمن مضمونه.

الإشراف القضائي: الرقابة التي يمارسها قاضٍ مختص على إجراءات التحقيق والمراقبة الإلكترونية وإصداره الأوامر اللازمة لها.

الباب الثاني

الجرائم الإلكترونية

الفصل الأول: جرائم الاعتداء على الأنظمة والبيانات

المادة (3): الوصول غير المصرح به

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من دخل عمداً إلى نظام معلوماتي أو جزء منه أو إلى بيانات مخزنة فيه دون أن يكون مخوّلاً بذلك أو بتجاوز التخويل الممنوح له.

العقوبة: الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من خمسة آلاف إلى خمسين ألف دينار ليبي أو إحدى هاتين العقوبتين.

تشدَّد العقوبة لتبلغ الحبس من سنة إلى خمس سنوات والغرامة المضاعفة في الأحوال الآتية:

1. إذا كان النظام المُخترَق متعلقاً بالبنية التحتية الحيوية أو الخدمات العامة.
2. إذا أسفر الاختراق عن تسريب بيانات أو إتلافها.
3. إذا ارتُكبت الجريمة من قِبل شخص مُخوَّل بالوصول وتجاوز حدود صلاحياته بصورة جسيمة.

المادة (4): اعتراض الاتصالات بغير إذن

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من اعترض عمداً، بأي وسيلة تقنية، محتوى اتصال إلكتروني أو بياناته الوصفية دون أن يكون له حق قانوني أو إذن قضائي بذلك.

العقوبة: الحبس من سنة إلى أربع سنوات والغرامة من عشرة آلاف إلى مئة ألف دينار ليبي.

لا تسري أحكام هذه المادة على ما يأتي:

1. تدابير الأمن المعلوماتي التي يتخذها مزود الخدمة لحماية شبكته وفق بروتوكولات مهنية معتمدة.
2. الاعتراض المرخص قضائياً وفق أحكام الباب السادس من هذا القانون.
3. الاتصالات التي وافق على اعتراضها جميع أطرافها.

المادة (5): الإخلال بسلامة البيانات

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من أتلف أو عدّل أو حذف أو أتاح بيانات رقمية دون مسوّغ قانوني أو موافقة صاحب الحق.

العقوبة: الحبس من سنة إلى خمس سنوات والغرامة من عشرين ألفاً إلى مئتي ألف دينار.

تُضاعف العقوبة إذا كانت البيانات المستهدفة ذات صلة بالبنية التحتية الحيوية أو الخدمات الحكومية أو الصحة أو النظام المالي.

المادة (6): الاعتداء على سلامة الأنظمة

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من أدخل أو نقل أو أتاح بيانات رقمية أو برمجيات خبيثة أو مشوّشات إلكترونية بقصد التدخل في سير نظام معلوماتي أو تعطيله أو إعاقته.

العقوبة: الحبس من سنتين إلى سبع سنوات والغرامة من خمسين ألفاً إلى خمسمئة ألف دينار.

تُشدَّد العقوبة إلى الحبس من خمس سنوات إلى خمس عشرة سنة إذا استهدف الفعل:

1. أنظمة الطاقة أو المياه أو الاتصالات أو النقل.
2. أنظمة القطاع المالي والمصرفي.
3. أنظمة الرعاية الصحية.
4. أنظمة الأمن الوطني.

الفصل الثاني: جرائم الاحتيال الإلكتروني والجرائم المالية

المادة (7): الاحتيال الإلكتروني

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من توصّل دون حق إلى منفعة مالية أو غير مالية لنفسه أو لغيره عبر التلاعب في نظام معلوماتي أو إدخال بيانات كاذبة أو تعديل بيانات قائمة.

العقوبة: الحبس من سنتين إلى سبع سنوات والغرامة بما يعادل ثلاثة أمثال قيمة المنفعة المكتسبة أو مئة ألف دينار أيهما أكبر.

المادة (8): التزوير الإلكتروني

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من أنشأ أو عدّل أو أتاح بيانات رقمية بقصد الاستخدامها في الإيقاع بالغير كأنها أصيلة.

العقوبة: الحبس من سنة إلى خمس سنوات والغرامة من عشرين ألفاً إلى مئتي ألف دينار.

المادة (9): سرقة الهوية الرقمية

يُعدّ مرتكباً جريمة يعاقب عليها القانون كل من انتحل هوية شخص آخر عبر وسائل إلكترونية بقصد الإضرار به أو اكتساب منفعة على حسابه، بما في ذلك استخدام بياناته الشخصية أو بيانات حساباته دون إذنه.

العقوبة: الحبس من سنة إلى أربع سنوات والغرامة من عشرة آلاف إلى مئة ألف دينار.

الفصل الثالث: جرائم المحتوى الرقمي

المادة (10): المحتوى المحظور المتعلق بالأطفال

يُعدّ جريمة يعاقب عليها القانون بأشد العقوبات كل إنتاج أو توزيع أو حيازة أو تصفح متعمد لمحتوى يصوّر الأطفال دون الثامنة عشرة بصورة جنسية أو يستغلهم بأي شكل.

العقوبة: الحبس من خمس سنوات إلى خمس عشرة سنة والغرامة من مئة ألف إلى مليون دينار، وتُضاعف في حالة الإنتاج والتوزيع.

المادة (11): التحريض على العنف والكراهية عبر الفضاء الرقمي

يُعدّ جريمة يعاقب عليها القانون كل نشر متعمد عبر وسائل إلكترونية لمحتوى يحرّض صراحةً وبشكل مباشر على ارتكاب عنف ضد أفراد أو جماعات محددة أو يروّج للتمييز على أساس العرق أو الدين أو الجنس أو الأصل.

العقوبة: الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من عشرة آلاف إلى مئة ألف دينار.

لا تسري هذه المادة على التعبير النقدي أو الساخر أو الفني أو الأكاديمي أو الصحفي الذي لا يتضمن تحريضاً مباشراً وصريحاً على العنف. ويُفسَّر أي غموض في نطاق هذه المادة لصالح حرية التعبير.

المادة (12): التحرش والابتزاز الإلكتروني

يُعدّ جريمة يعاقب عليها القانون:

1. التحرش الإلكتروني: كل سلوك متعمد ومتكرر عبر وسائل إلكترونية يتضمن تهديداً أو إيذاءً نفسياً أو ملاحقة أو إزعاجاً متكرراً لشخص ما.
2. الابتزاز الإلكتروني: كل تهديد بنشر بيانات أو صور أو معلومات شخصية بقصد انتزاع منفعة أو إجبار الضحية على فعل أو ترك فعل.

العقوبة: الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من خمسة آلاف إلى خمسين ألف دينار، وتُشدَّد العقوبة إذا كانت الضحية قاصراً أو امرأة.

المادة (13): القرصنة الإلكترونية وانتهاك الملكية الفكرية

يُعدّ جريمة يعاقب عليها القانون كل نسخ أو توزيع أو إتاحة غير مشروع للبرمجيات أو الأعمال الرقمية المحمية بحقوق الملكية الفكرية بنطاق تجاري.

العقوبة: الغرامة من خمسة آلاف إلى خمسين ألف دينار أو الحبس لمدة لا تتجاوز سنة في حالات الاستغلال التجاري الجسيم.

الباب الثالث

ضمانات حقوق الإنسان والحريات الرقمية

المادة (14): حظر التجريم المفرط لحرية التعبير

لا يُجرَّم أي محتوى رقمي بسبب التعبير عن الرأي أو النقد أو المعارضة السياسية أو الصحافة أو الفن أو البحث الأكاديمي ما لم يتضمن تهديداً مباشراً أو حثاً صريحاً على ارتكاب جريمة أو انتهاكاً لحق محدد نص عليه هذا القانون. وكل تفسير لأحكام هذا القانون يجب أن يتوافق مع ضمانات حرية التعبير الواردة في المواثيق الدولية لحقوق الإنسان.

المادة (15): حظر الملاحقة على الهوية الرقمية

لا يُعدّ استخدام أسماء مستعارة أو حسابات غير موثقة عبر الإنترنت جريمةً في ذاتها. ولا يجوز استخدام هذه الهوية دليلاً وحيداً على القصد الجرمي أو إخضاعها للتحقيق إلا في إطار تحقيق في جريمة محددة وبإذن قضائي.

المادة (16): حماية التشفير

يحق لكل شخص استخدام وسائل التشفير بحرية لحماية اتصالاته وبياناته. ويُحظر ما يأتي:

1. إلزام أي شخص بالكشف عن مفاتيح التشفير الخاصة به إلا بأمر قضائي في إطار تحقيق جنائي محدد وبعد استنفاد الوسائل التقنية البديلة.
2. حظر استخدام أدوات التشفير المشروعة أو تقييده لأسباب أمنية مبهمة.
3. إلزام مزودي الخدمات بتضمين ثغرات أمنية مقصودة أو بوابات خلفية في أدوات التشفير.

يُعدّ استخدام التشفير قرينة على الشفافية لا على الجريمة، ولا يجوز استخدامه وحده دليلاً على الاشتباه.

المادة (17): مبدأ الضرورة والتناسب

تُطبَّق أحكام هذا القانون وفق مبدأ الضرورة والتناسب. ولا تُتخذ أي تدابير قسرية إلا إذا كانت:

1. ضرورية لتحقيق غرض مشروع محدد.
2. متناسبة مع جسامة الجريمة المشتبه بها.
3. الأقل تدخلاً في الحقوق والحريات من بين الوسائل المتاحة.
4. خاضعة للإشراف القضائي.

الباب الرابع

إجراءات التحقيق الجنائي الرقمي

الفصل الأول: ضبط الأدلة الرقمية

المادة (18): ضبط البيانات الرقمية وتحفظها

تلتزم النيابة العامة والجهات المختصة بالتحقيق وفق الضوابط الآتية عند ضبط البيانات الرقمية:

1. الحصول على أمر قضائي مسبق يحدد نطاق الضبط وطبيعة البيانات المطلوبة والجريمة موضوع التحقيق.
2. الاقتصار على البيانات ذات الصلة المباشرة بالجريمة المحققة فيها.
3. إخطار صاحب البيانات بالضبط في أقرب وقت ممكن ما لم يصدر أمر قضائي بتأجيل الإخطار لمدة لا تتجاوز تسعين يوماً.
4. إعادة أو إتلاف البيانات التي لا صلة لها بالتحقيق فور إغلاقه.
5. الاحتفاظ بسجل دقيق لكل عمليات الضبط والتحفظ.

المادة (19): الحصول على بيانات المرور والبيانات الوصفية

يُشترط للحصول على بيانات المرور والبيانات الوصفية المحفوظة لدى مزودي الخدمة:

1. أمر قضائي مسبق يحدد الغرض والمدة الزمنية ونطاق البيانات المطلوبة.
2. أن تكون البيانات المطلوبة ضرورية للتحقيق في جريمة إلكترونية محددة.
3. ألا تشمل الطلبات مجموعات بيانات واسعة النطاق غير محددة بشكل كافٍ.

يلتزم مزود الخدمة بتقديم البيانات المطلوبة بموجب الأمر القضائي ويحق له الاعتراض عليه قضائياً.

المادة (20): المراقبة الإلكترونية في التحقيقات

لا تجوز المراقبة الإلكترونية للاتصالات في الزمن الحقيقي إلا وفق الشروط المتراكمة الآتية:

1. وجود اشتباه جدي ومعقول موثق بأدلة مادية في ارتكاب جريمة جسيمة.
2. صدور أمر قضائي مسبق يصادق على المراقبة ويحدد هدفها ومدتها ونطاقها.
3. عجز وسائل التحقيق البديلة الأقل تدخلاً عن تحقيق الغرض ذاته.
4. ألا تتجاوز مدة المراقبة ستين يوماً قابلة للتجديد بأمر قضائي جديد مع تقديم تبرير جديد.
5. تحرير تقرير قضائي دوري كل ثلاثين يوماً عن مآلات المراقبة ومدى ضرورة الاستمرار فيها.

يُحظر استخدام أدوات التجسس التجارية والبرامج الهجومية إلا بترخيص قضائي مشدد في الجرائم الجسيمة فحسب.

المادة (21): التعاون مع مزودي الخدمة

يلتزم مزودو الخدمة بما يأتي:

1. الاستجابة للطلبات المصحوبة بأوامر قضائية في المدد المحددة.
2. الاحتفاظ ببيانات المرور لمدة لا تتجاوز اثني عشر شهراً لأغراض التحقيق الجنائي حصراً مع اتخاذ تدابير الأمان اللازمة.
3. تقديم تقرير سنوي شفاف يكشف عدد الطلبات الرسمية التي تلقّوها ونطاقها دون الإخلال بالسرية.

يحق لمزود الخدمة الاعتراض على الطلبات التي يرى أنها مبهمة أو متجاوزة للنطاق المشروع.

الباب الخامس

الإشراف القضائي والرقابة

المادة (22): محكمة الجرائم الإلكترونية

تُنشأ دوائر قضائية متخصصة في الجرائم الإلكترونية ضمن هيكل القضاء العادي، تختص بـ:

1. النظر في طلبات إصدار أوامر المراقبة والضبط الرقمي.
2. الفصل في الطعون المتعلقة بانتهاك الحقوق الرقمية خلال التحقيق.
3. محاكمة المتهمين في جرائم هذا القانون.

يشترط في القضاة المعيّنين في هذه الدوائر التدريب المتخصص في القانون الرقمي وعلوم الحاسوب.

المادة (23): الرقابة البرلمانية على المراقبة الإلكترونية

تُقدَّم إلى لجنة برلمانية مختصة تقارير سرية دورية كل ستة أشهر تتضمن:

1. الإجمالي الكلي لأوامر المراقبة الإلكترونية الصادرة ونسبة الموافقة عليها.
2. فئات الجرائم التي صدرت بشأنها أوامر المراقبة.
3. متوسط مدة المراقبة.
4. عدد القضايا التي أسفرت عن ملاحقة قضائية ناجحة.

تنشر اللجنة ملخصاً غير سري سنوياً لهذه المعطيات.

المادة (24): الرقيب المستقل على عمليات المراقبة

يُعيَّن رقيب مستقل بمرسوم يُختار من ذوي الكفاءة القانونية والتقنية لمدة أربع سنوات غير قابلة للتجديد، يختص بـ:

1. مراجعة سجلات عمليات المراقبة الإلكترونية والتحقق من مشروعيتها.
2. تلقي الشكاوى المتعلقة بالمراقبة غير المشروعة والفصل فيها.
3. رفع تقارير سنوية علنية حول أوضاع المراقبة الإلكترونية في ليبيا.

الباب السادس

المراقبة الإلكترونية المرخصة

المادة (25): شروط المراقبة القانونية

لا تُعدّ جريمة بموجب هذا القانون المراقبة الإلكترونية المستوفية للشروط الآتية مجتمعةً:

1. صدور أمر قضائي مسبق وفق أحكام المادة (20).
2. اقتصارها على نطاق الأمر القضائي الصادر.
3. إخطار الشخص المراقَب في أقرب وقت ممكن بعد انتهاء التحقيق.
4. توثيق جميع إجراءات المراقبة وحفظها لمدة خمس سنوات للمراجعة القضائية.

المادة (26): حظر المراقبة الجماعية

يُحظر تحت أي ظرف:

1. مراقبة الاتصالات الإلكترونية على نطاق جماعي واسع دون استهداف فردي محدد.
2. إلزام مزودي الخدمة بتوفير إمكانية الوصول الدائم لجهات الأمن إلى شبكاتهم أو بيانات مستخدميهم.
3. استخدام برامج التجسس الهجومية لمراقبة الصحفيين والناشطين والمحامين ومنظمات المجتمع المدني بسبب نشاطهم المشروع.
4. الاحتفاظ بقواعد بيانات شاملة عن الاتصالات والتنقلات الخاصة بالمواطنين لأغراض وقائية غير مبنية على اشتباه محدد.

الباب السابع

مسؤولية الأشخاص الاعتبارية

المادة (27): المسؤولية الجنائية للشركات

تسأل الأشخاص الاعتبارية جنائياً عن الجرائم الإلكترونية المنصوص عليها في هذا القانون متى ارتُكبت لحسابها أو باسمها أو بتساهل من أجهزة إدارتها، وذلك مع عدم الإخلال بالمسؤولية الجنائية الشخصية لمرتكبي الجريمة.

العقوبة: الغرامة من خمسة أضعاف إلى عشرة أضعاف الغرامة المقررة للشخص الطبيعي، وجواز سحب الترخيص أو الإغلاق المؤقت.

المادة (28): التزامات مزودي الخدمة

يلتزم مزودو الخدمة بما يأتي:

1. عدم حجب أي موقع أو خدمة أو محتوى رقمي إلا بناءً على أمر قضائي محدد وموثق.
2. إخطار المستخدمين المتضررين من قرارات الحجب بصفة شفافة متى أمكن ذلك.
3. توفير آليات للطعن في قرارات تقييد المحتوى.
4. نشر تقارير شفافية سنوية تكشف عدد الطلبات الحكومية الواردة إليهم ونطاقها وما امتثلوا له منها.

يُعدّ الحجب الذي يتم خارج هذه الشروط انتهاكاً إدارياً يُعرّض مزود الخدمة للمساءلة.

الباب الثامن

العقوبات التكميلية والأحكام العامة

المادة (29): العقوبات التكميلية

يجوز للمحكمة إضافة إلى العقوبات الأصلية الحكم بواحدة أو أكثر من العقوبات التكميلية الآتية:

1. مصادرة الأجهزة والمعدات والبرمجيات المستخدمة في ارتكاب الجريمة.
2. الحرمان من ممارسة الأنشطة المهنية المرتبطة بالفضاء الرقمي لمدة محددة.
3. نشر الحكم في وسائل الإعلام على نفقة المحكوم عليه في الجرائم الجسيمة.
4. إلزام المحكوم عليه بإعادة الحال إلى ما كانت عليه أو بالتعويض.

المادة (30): الظروف المخففة والتدابير البديلة

تأخذ المحكمة بالظروف المخففة في الأحوال الآتية:

1. تبليغ الجاني الجهات المختصة عن ثغرات أمنية قبل استغلالها من قِبل آخرين (الكشف المسؤول).
2. البكارة في ارتكاب الجريمة وصغر السن وانعدام السابقة الجنائية.
3. التعاون الكامل مع التحقيق وإعادة الحال إلى ما كانت عليه.

يُلجأ إلى العقوبات البديلة وعدم السجن في جرائم ذات طابع تقني بحت ارتكبها أفراد دون سابقة وكانت الأضرار محدودة.

المادة (31): حماية باحثي الأمن المعلوماتي

لا تسري أحكام المواد (3) و(4) و(5) على الأنشطة الآتية إذا توافرت شروطها:

1. اختبار الاختراق المرخص: الذي يُجرى بموافقة صريحة وكتابية من صاحب النظام لأغراض الكشف عن الثغرات.
2. الكشف المسؤول: إبلاغ الجهة المعنية بثغرة أمنية مكتشفة بنية حسنة وإتاحة مهلة معقولة لمعالجتها.
3. البحث الأمني الأكاديمي: الذي يُجرى في بيئة معزولة بغرض تحسين الأمن المعلوماتي ووفق معايير أخلاقيات البحث.

يقع عبء إثبات تجاوز هذه الشروط على النيابة العامة.

الباب التاسع

التعاون القضائي الدولي

المادة (32): أسس التعاون الدولي

يستند التعاون القضائي الدولي في مجال الجرائم الإلكترونية إلى:

1. الاتفاقيات الدولية والإقليمية النافذة في ليبيا.

2. مبدأ المعاملة بالمثل في غياب الاتفاقيات.
3. اشتراط ازدواجية التجريم بين الدولتين كأصل عام.

المادة (33): تسليم المجرمين والمساعدة القضائية

تُوجَّه طلبات التسليم والمساعدة القضائية القضائية عبر القنوات الرسمية وفق المعاهدات النافذة. ويُرفض أي طلب تعاون دولي إذا:

1. كان من شأن تنفيذه انتهاك حقوق الإنسان الأساسية للشخص المعني.
2. كان الفعل لا يُعدّ جريمة بموجب القانون الليبي.
3. كانت الملاحقة ذات طابع سياسي أو تمييزي.

المادة (34): حماية البيانات في الإطار الدولي

لا تُنقل بيانات شخصية لمواطنين ليبيين إلى دول أجنبية بموجب طلبات تعاون قضائي إلا وفق الضمانات المنصوص عليها في قانون حماية البيانات الشخصية النافذ.

الباب العاشر

الأحكام الختامية والانتقالية

المادة (35): الإلغاء

يُلغى قانون رقم (5) لسنة 2022م بشأن الجرائم الإلكترونية بجميع أحكامه اعتباراً من تاريخ نفاذ هذا القانون. وتُحال القضايا المنظورة أمام المحاكم إلى هذا القانون إذا كان أصلح للمتهم.

المادة (36): اللوائح التنفيذية

تُصدر الجهات المختصة اللوائح التنفيذية لهذا القانون في غضون تسعة أشهر من تاريخ نشره، وتشمل:

1. الإجراءات التفصيلية لطلبات الضبط والمراقبة الإلكترونية.
2. معايير الأدلة الرقمية وإجراءات حفظها وتقديمها أمام القضاء.
3. ضوابط تعاون مزودي الخدمة مع التحقيقات.
4. الإجراءات التفصيلية لآلية الكشف المسؤول وحماية باحثي الأمن.

المادة (37): المراجعة الدورية

تُعيد الجهة التشريعية النظر في أحكام هذا القانون دورياً كل ثلاث سنوات بالتشاور مع خبراء القانون والتقنية والمجتمع المدني، بهدف مواكبة التطورات التقنية وضمان الامتثال المستمر لمعايير حقوق الإنسان.

المادة (38): النفاذ

يُعمل بهذا القانون اعتباراً من تاريخ نشره في الجريدة الرسمية.

ملاحظات ختامية

هذه المسودة وثيقة عمل أعدّتها مجموعة العمل المتخصصة في إطار النشاط 1.3 استناداً إلى: (1) نتائج تحليل تأثير الإنترنت على قانون رقم 5 لسنة 2022 من النشاط 1.1؛ (2) توصيات مجموعة العمل متعددة أصحاب المصلحة من النشاط 1.2 لا سيما موجز سياسة الحيز الرقمي من منظور حقوق الإنسان؛ (3) اتفاقية بودابست لمكافحة الجرائم الإلكترونية؛ (4) مبادئ الأمم المتحدة التوجيهية بشأن حقوق الإنسان والأعمال التجارية وتوصيات المقرر الخاص للأمم المتحدة المعني بحرية التعبير.

تُفتح هذه المسودة للمشاورة العامة عبر المنصة الرقمية للمشروع وورش العمل التشاركية. الملاحظات والاقتراحات مرحّب بها على: salam@annir.ly