



ورقة بحثية حول:

القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته وأثره على الفضاء المدني في فلسطين

سلسلة تقارير رقم 337





ورقة بحثية حول:

**القرار بقانون رقم (10) لسنة 2018
بشأن الجرائم الإلكترونية وتعديلاته وأثره
على الفضاء المدني في فلسطين**

AMAN
Transparency Palestine



يتقدم ائتلاف أمان بالشكر الجزيل للباحثة عنان جبعيتي لإعدادها هذه الورقة، وللدكتور عزمي الشعبي
مستشار مجلس إدارة ائتلاف أمان، ولغريق ائتلاف أمان لإشرافهم على الورقة ومراجعتهم لها.

جميع الحقوق محفوظة للائتلاف من أجل النزاهة والمساءلة (أمان).

في حالة الاقتباس، يرجى الإشارة إلى المطبوعة كالتالي: القرار بقانون رقم (10) لسنة 2018 بشأن
الجرائم الإلكترونية وتعديلاته وأثره على الفضاء المدني في فلسطين. ائتلاف أمان. 2026. رام الله-
فلسطين.

إنّ الائتلاف من أجل النزاهة والمساءلة (أمان) قد بذل جهوداً في التحقّق من المعلومات الواردة في
هذه الورقة، ولا يتحمّل أيّ مسؤولية تترتب على استخدام المعلومات لأغراض خارج سياق أهداف
الورقة بعد نشرها.

تم إعداد هذه الورقة بتمويل من الاتحاد الأوروبي، والآراء الواردة فيها لا تعبّر بالضرورة عن رأي الاتحاد
الأوروبي ولا يتحمّل مسؤوليتها.

هذا المشروع بدعم من



EUROPEAN UNION

الاتحاد الأوروبي

فهرس المحتويات

4	مقدمة
5	أولاً. السياق القانوني والسياسي لصدور القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته
6	ثانياً. تقييم القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته
12	النتائج والتوصيات
16	قائمة المصادر والمراجع

شهدت البيئة العالمية والمحلية في السنوات الأخيرة طفرة تكنولوجية غير مسبوقة في قطاع تكنولوجيا المعلومات والاتصالات، ما أحدث تحولاً جذرياً في بنية التواصل الإنساني والتنظيمي. لقد أسهم هذا التوسع الرقمي المتسارع في خلق فضاء تفاعلي افتراضي بات يمثل الحاضنة الأساسية للمشاركة المدنية، والتعبير عن الرأي، والممارسات الرقابية للمجتمع المدني والأفراد على حد سواء.

وعُرف الفضاء المدني بأنه «البيئة التي تمكّن الأفراد والجماعات من المشاركة المجدية، عبر الإنترنت، وفي الحياة الواقعية، في أمور مجتمعاتهم السياسية والاقتصادية والاجتماعية والثقافية، حيث يعبر الناس عن آرائهم بحرية ودون خوف، ويتجمعون بسلام، ويشاركون في عمليات صنع القرارات المتعلقة بالقضايا التي تؤثر في حياتهم»¹.

إلا أن هذا التحول لم يخلُ من التحديات؛ حيث ترافقت الطفرة الرقمية مع نشوء أنماط مستحدثة ومعقدة من الجرائم المرتبطة باستخدام الشبكة العنكبوتية وتقنيات الاتصال، الأمر الذي وضع الدول أمام مسؤولية مباشرة لتطوير أطر تشريعية قادرة على مكافحة هذه الجرائم، وضمان الأمن الرقمي وحماية الخصوصية وحماية حرية الرأي والتعبير. فوفقاً للمعايير الدولية، فإن الفضاء المدني الحر يتميز بوجود بيئة تشريعية ومؤسسية داعمة تضمن حماية حقوق التعبير والتجمع وتكوين الجمعيات دون تدخلات إدارية أو أمنية تعسفية، وإمكانية الوصول إلى العدالة والمساءلة عند حدوث انتهاكات.

وفي السياق الفلسطيني، تأرجحت هذه الحاجة التشريعية بين متطلبات الحفاظ على الأمن الإلكتروني ومكافحة الجريمة من جهة، وبين التزامات فلسطين الدولية وحماية الحريات العامة ومساحات الفضاء المدني من جهة أخرى. وبات من الواضح أن القوانين المصممة لمكافحة الجرائم الإلكترونية، بما فيها القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، عندما تتضمن نصوصاً فضفاضة منحت السلطة التنفيذية وأجهزة إنفاذ القانون صلاحيات واسعة النطاق، أثارت تساؤلات جوهرية حول مدى قدرة هذه التشريعات على تحقيق التوازن المطلوب بين موجبات الأمن ومقتضيات احترام الحريات والحقوق الأساسية، وبما يشمل حرية التعبير وحقوق الإنسان.

تهدف هذه الورقة إلى مراجعة القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته؛ من أجل اقتراح تعديلات عليه تحد من تقييده للفضاء المدني، وذلك من خلال:

1. تسليط الضوء على المواد ذات العلاقة التي أتاحت المجال للسلطات التنفيذية بالتوسع في صلاحياتها وفرض المزيد من القيود على الفضاء المدني.
2. اقتراح التوصيات التي تسهم في تعزيز وإنفاذ البيئة القانونية والمؤسسية الفلسطينية لحماية الفضاء المدني، وتقوية قدرات فاعلي الفضاء المدني لمساءلة السلطات الحاكمة، والمساهمة في حماية فاعلي الفضاء المدني من القيود التي تفرض عليه.

1 الائتلاف من أجل النزاهة والمساءلة (أمان). 2024. تقييم المساحة المتاحة أمام الفضاء المدني الفلسطيني للمشاركة في صنع السياسات العامة والمساءلة على تنفيذها. رام الله-فلسطين. ص 5.

أولاً. السياق القانوني والسياسي لصدور القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته

برزت الحاجة الفلسطينية لإقرار تشريع خاص بالجرائم الإلكترونية لسد الفراغ القانوني الناجم عن تقادم القوانين العقابية السارية (مثل قانون العقوبات الأردني رقم (16) لسنة 1960 الساري في الضفة الغربية، وقانون العقوبات الانتدابي رقم (74) لسنة 1936 الساري في قطاع غزة)، التي لم تكن مؤهلة بطبيعتها للتعامل مع الجرائم الافتراضية والبيانات الرقمية. استجابةً لذلك، أصدر الرئيس في العام 2017 القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية، وتم العمل بموجبه، حيث اتضح من خلال الممارسة أن بعض أحكامه تم استخدامها لتقييد حرية الرأي والتعبير وتقليص الفضاء المدني، الأمر الذي أدى إلى موجة من الانتقادات والرفض من قبل مؤسسات المجتمع المدني الفلسطيني، والمدافعين عن حقوق الإنسان، إضافة إلى الأطراف الدولية والمنظمات الأممية. تركزت هذه الانتقادات حول احتواء القانون على نصوص عقابية شديدة القسوة، وعبارات فضفاضة وتفسيرات مطاطة منحت السلطات التنفيذية والأمنية تفويضاً واسعاً لملاحقة النشطاء، وحجب المواقع الإعلامية، وتقويض حرية التعبير الرقمي. وتحت وطأة هذا الضغط المجتمعي والحقوقى والدولي الواسع²، ومطالبات المواءمة مع الاتفاقيات الدولية التي انضمت إليها دولة فلسطين (وفي مقدمتها العهد الدولي الخاص بالحقوق المدنية والسياسية) اضطرت الحكومة الفلسطينية إلى التراجع النسبي، ما أفضى إلى إلغاء قرار بقانون رقم (16) لسنة 2017، وإصدار القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته بدلاً منه.

على الرغم من أن القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته جاء ليعالج بعض الاختلالات الصارخة التي شابت سلفه، فإنه حافظ على جوهر المقاربة الأمنية التقييدية في العديد من بنوده، وظل محتفظاً بنصوص فضفاضة تسهم في خلق بيئة تعسفية وإساءة استخدام السلطة من قبل المكلفين بإنفاذ القانون. وقد شهدت الأروقة الحكومية اللاحقة لصدور القانون حراكاً مستمراً بفعل تداخل الضغوط المحلية والدولية؛ حيث استجاب مجلس الوزراء لضغوط خارجية وداخلية بضرورة إجراء تعديلات جوهرية على الأحكام القانونية، بما يضمن عدم استخدام التشريع كأداة لتضييق الخناق على مؤسسات المجتمع المدني وحرية الرأي والتعبير. وشكلت هذه الضغوط والالتزامات الدولية المترتبة على انضمام فلسطين للمعاهدات الدولية، الدافع المباشر للحكومة لإصدار قرار من مجلس الوزراء في جلسته المنعقدة بتاريخ 2025/4/30، لتشكيل لجنة من وزارة العدل (مقرراً)، ووزارة الاتصالات والاقتصاد الرقمي، ووزارة الداخلية، والنيابة العامة، والأمانة العامة لمجلس الوزراء، وممثل عن مؤسسات المجتمع المدني، لدراسة القرار بقانون للجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم 10 لسنة 2018 وتعديلاته، ليتواءم مع الاتفاقيات والمعايير الدولية.

قامت اللجنة المشكلة من مجلس الوزراء برئاسة وزارة العدل بدراسة القرار بقانون، وتم الأخذ في بعض الملاحظات المقدمة من مؤسسات المجتمع المدني³. وعليه، قامت وزارة العدل بصياغة مسودة لمشروع قرار بقانون معدل للقرار بقانون الجرائم الإلكترونية لسنة 2018 وتعديلاته، وحالياً مطروح للمشاورات العامة وعلى موقع منصة التشريع الإلكترونية التابعة لوزارة العدل⁴. وتهدف الحكومة بهذه الخطوات إلى إيجاد مظهر من التشاركية المجتمعية، والحد من الانتقادات الدولية الموجهة لمنظومة العدالة وصناعة القرار في فلسطين.

2 <https://www.aman-palestine.org/activities/6677.html>

تم الدخول للموقع بتاريخ 2026/8/7.

3 مقابلة أجرتها الباحثة مع أ. أشرف أبو حية، مستشار قانوني، مؤسسة الحق، بتاريخ 2026/8/12

4 <https://econsultation.moj.pna.ps/consultation-details/114>

ثانياً. تقييم القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته

أ- الأهمية والآثار الإيجابية

على الرغم من الجدل الواسع حول أثر القرار بقانون الجرائم الإلكترونية على الفضاء المدني، فإن القانون ينطوي على ركائز تنظيمية بالغة الأهمية، تستهدف سد الفجوات القانونية ومواجهة التحديات الأمنية والتقنية المستجدة. ويمكن حصر أهمية هذا القرار بقانون وآثاره الإيجابية في الأبعاد الرئيسية الآتية:

1. سد الفراغ التشريعي وتحديث المنظومة العقابية: شكل صدور القرار بقانون نقلة نوعية في سد فراغ قانوني مزمن عانت منه المنظومة القضائية الفلسطينية لعقود طويلة. فقد كانت المحاكم الفلسطينية تستند في تكييف القضايا المرتبطة بالتكنولوجيا إلى نصوص تقليدية جامدة تعود إلى قانون العقوبات الأردني رقم (16) لسنة 1960 الساري في الضفة الغربية، وقانون العقوبات الانتدابي رقم (74) لسنة 1936 الساري في قطاع غزة. هذه القوانين القديمة لم تكن تتضمن أي إشارة لمفاهيم مثل «البيانات الرقمية»، و«الشبكات اللاسلكية»، و«البريد الإلكتروني»، أو «التوقيع الرقمي». ومن خلال القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، أصبح للقضاء الفلسطيني إطار تشريعي حديث يُمكنهم من توصيف وتكييف الأفعال الجرمية الرقمية بصورة دقيقة دون اللجوء إلى التفسيرات والقياسات القانونية المجحفة والمثيرة للجدل.

2. توفير الحماية الجنائية للمؤسسات والقطاع المصرفي والمالي: يُعد حماية الأمن الاقتصادي الرقمي واحداً من أبرز الآثار الإيجابية للقرار بقانون؛ إذ تضمن القانون نصوصاً صارمة تجرم عمليات اختراق الأنظمة المعلوماتية للمؤسسات والوزارات، والعيب ببياناتها أو سرقتها. وساهمت هذه النصوص في تعزيز الثقة بالقطاع المالي والمصرفي الفلسطيني وجهازيته الرقمية لتقديم الخدمات المصرفية والإلكترونية بأمان.

3. مكافحة الجرائم المستحدثة وحماية السلم الأهلي والنسيج الاجتماعي: حيث قدم القرار بقانون إجابات رادعة لمجموعة من الجرائم الأخلاقية والاجتماعية المستحدثة التي اتسعت رقعتها بفعل الانتشار السريع لمنصات التواصل الاجتماعي، ومن أبرزها: الابتزاز الإلكتروني والتهديد، حيث وفر القانون حماية جنائية خاصة لضحايا الابتزاز (وبخاصة النساء والفئات المستضعفة)، وشدد العقوبات على الجناة الذين يستغلون الصور أو البيانات الشخصية لتهديد الضحايا ومقايضتهم مالياً أو جسدياً.

4. حماية البيانات الشخصية والخصوصية الرقمية على الرغم من الملاحظات على بعض البنود الإجرائية.

ب. سلبات القرار بقانون بشأن الجرائم الإلكترونية رقم (10) لسنة 2018 وتعديلاته وأثره على الفضاء المدني في فلسطين

على الرغم من الدوافع التي رافقت صدور القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، فإن التطبيق الفعلي والممارسات العملية لجهات إنفاذ القانون، بالاستناد إلى بعض النصوص الواردة فيه، قد أفضت إلى تراجع ملموس وغير مسبوق في مؤشرات الفضاء المدني وحرية الرأي والتعبير في فلسطين. ونتناول في هذا المحور تحليلاً نقدياً تفصيلياً للمواد الأكثر إثارة للجدل، وأثرها على واقع الفضاء المدني في فلسطين، ومقارنتها بأهم المعايير والمواثيق الدولية التي انضمت إليها دولة فلسطين، على النحو الآتي:

أولاً. تقييد حرية الرأي والتعبير عند استخدامها الوسائط الإلكترونية

يكفل القانون الأساسي لسنة 2003، ولاسيما المادة (19) منه، حرية الرأي والتعبير، حيث نصت على أنه لا مساس بحرية الرأي، ولكل إنسان الحق في التعبير عن رأيه ونشره بالقول أو الكتابة أو غير ذلك من وسائل التعبير أو الفن مع مراعاة أحكام القانون. كما تكفل هذا الحق المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة (19) من الإعلان العالمي لحقوق الإنسان، اللتان نصتا على أن لكل فرد الحق في اعتناق الآراء دون مضايقة، والحق في حرية التعبير، بما يشمل حرية البحث عن المعلومات والأفكار وتلقيها ونقلها عبر مختلف الوسائل، بما فيها الوسائط الإلكترونية.

وعلى الرغم من أن الفقرة (3) من المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية التي تنص على بعض القيود التي من الممكن فرضها على حرية التعبير، فإنها اشترطت أن تكون محددة بنص القانون وأن تكون ضرورية⁵:

أ. لاحترام حقوق الآخرين أو سمعتهم؛
ب. لحماية الأمن القومي، أو النظام العام، أو الصحة العامة، أو الآداب العامة.

كما يحظر التعليق العام رقم (34) للجنة حقوق الإنسان التابعة للأمم المتحدة استخدام المصطلحات المبهمة لقمع الآراء، أو حظر انتقاد السياسات العامة والشؤون الحكومية⁶.

ويعد القرار التفسيري رقم (2017/04) الصادر عن المحكمة الدستورية العليا⁷ أداة قانونية رئيسية لحماية حرية التعبير عبر ترسيخ سمو الاتفاقيات الدولية على التشريعات الداخلية، بحيث تكتسب قواعد هذه الاتفاقيات قوة أعلى من التشريعات الداخلية، بما يتواءم مع الهوية الوطنية والدينية والثقافية للشعب العربي الفلسطيني. إن هذا القرار التفسيري يجعل القضاء العادي ملزماً بتقديم المادة (19) من العهد الدولي للحقوق المدنية والسياسية على قوانين العقوبات والجرائم الإلكترونية عند التعارض. وعلى الرغم من غياب إلغاء صريح للمواد المقيدة، فإن هذا المبدأ يُفعل معايير دولية صارمة ضد القيود الفضفاضة.

وبتطبيق هذه المعايير على القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، يلاحظ أن بعض النصوص تحد من ممارسة حرية الرأي والتعبير، ولا تتلاءم مع المعايير الدولية، ومن أبرز هذه المواد الآتي⁸:

1. المادة (3) من القرار بقانون التي تنص على إنشاء وحدة للجرائم الإلكترونية في جهاز الشرطة وفي قوى الأمن، الأمر الذي يؤدي إلى تعدد الجهات وتداخل في الاختصاصات وتوسيع لعمل أجهزة الأمن وصلاحياتها، فالأصل أن تتم ملاحظة هذا النوع من الجرائم لدى جهاز الشرطة صاحب الصلاحية الأصلية في تتبع الجرائم، وتعد الجهات من شأنه أن ينعكس سلباً، ويقيّد حرية الرأي والتعبير ونشر وتواصل نشاطات مؤسسات المجتمع في وسائط التواصل الإلكتروني.

2. المادة (59) التي منحت جهات التحري والضبط والنيابة العامة صلاحيات واسعة لطلب حجب المواقع والمنصات التي «تهدد الأمن القومي أو النظام العام أو الآداب العامة»، حيث تضمنت هذه المادة مصطلحات عامة فضفاضة «الأمن القومي والنظام العام والآداب العامة»، التي لا تصلح أن تكون نصوصاً جنائية، بحسب مبدأ الشرعية، الذي يقضي بأن تكون نصوص التجريم والعقاب، واضحة لا تحتمل التفسير ولا التأويل، وألا تكون خاضعة للقائمين على تطبيق القانون. كما أن هذه المادة تنطوي على مساس بحق الأفراد بالعلم في القاعدة القانونية، فكيف للمواطن أن يحدد ما يعتبر جريمة وما لا يعتبر جريمة في ظل عدم وضوح النص الجنائي. إضافة إلى ذلك، فإن أي قيود على حرية التعبير والإعلام، يشترط أن تكون واضحة ومحددة في القانون، ومصطلح النظام العام والأمن القومي والآداب العامة كأحد هذه القيود غير واضحة تماماً⁹.

5 <https://www.ohchr.org/ar/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

6 <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedom-opinion-and>

7 حكم المحكمة الدستورية رقم 4/2017 جلسة 19/11/2017 المنشور في الجريدة الرسمية بتاريخ 29/11/2017، العدد (138). ص 84

8 تم الاستناد في إعداد هذه الورقة إلى القرار بقانون رقم 10 لسنة 2018 الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات والمنشور على المرجع الإلكتروني للجريدة الرسمية: <https://mjrb.gov.ps/MergedLegislations/ViewText/41>

9 الائتلاف من أجل النزاهة والمساءلة (أمان). 2024. تقييم المساحة المتاحة أمام القضاء المدني ... مصدر سابق، ص 12.

من جهته يُشير الباحث القانوني في الهيئة المستقلة لحقوق الإنسان، عمار جاموس، إلى ضرورة أن يكون التجريم واضحاً تماماً، وألا يتترك مجالاً للشك والتفسير من قبل المحاكم والأجهزة الأمنية، بما لا يتعارض مع القانون الأساسي الفلسطيني وتعديلاته سارية المفعول للعام 2003.

وبشأن حجب المواقع الإلكترونية، يقول إن حجب المواقع الإلكترونية يجب أن يكون بناءً على جريمة واضحة، لا أن يكون الحجب على أساس المحتوى الذي يخالف الاتجاه العام للسلطة، أو أن يكون محتوى ناقداً للسلطة، وأن يُسمح للمعنيين بتقديم الدفاع، على عكس المعمول به وفقاً لمواد القرار بقانون بشأن الجرائم الإلكترونية.

* تم الأخذ بالملاحظة جزئياً، إذ أبقى المشرع على المصطلحات الفضفاضة دون أي تعريف أو تحديد، ولكنه أضاف شرط أن يراعى مبدأ الضرورة والتناسب، وحق الطعن والاستئناف للجهة المتضررة، وبالتالي اقتصرَت الإضافة الإيجابية على إضافة الضمانات الإجرائية فيما لو تم الحجب، ولكن جوهر المشكلة في المادة، والمتمثلة في المصطلحات الفضفاضة، بقيت كما هي دون أي حل.

كما أن الصياغة الحالية للمادة تتعامل معه بوصفه جزءاً ذا طبيعة عقابية وليس مجرد إجراء احتياطي، ومن المؤكد ووفقاً إلى ما تمت ممارسته من قبل الأجهزة الأمنية والنيابة العامة، مثل قضية احتجاز هواتف الصحافيات، وإغلاق مواقع ومنصات، واعتقالات لنشطاء في المجتمع المدني، الأمر الذي يقتضي، تبعاً لذلك، كفالة الضمانات القانونية المقررة للمتهم، وفي مقدمتها إتاحة حق الدفاع، وتمكينه من الاعتراض والطعن في القرار أمام جهة قضائية مختصة.

3. المادة (65) من القرار بقانون: «إن ما ورد من نص فضفاض في هذه المادة، باعتبار أن مرتكب أي جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية، أو بإحدى وسائل تكنولوجيا المعلومات، أو تدخل فيها أو حرّض على ارتكابها، ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع». إن هذا النص، الواسع، من شأنه أن يُدخل عشرات «المصطلحات الفضفاضة» الواردة في التشريعات الفلسطينية، وبخاصة القوانين العقابية، إلى قرار بقانون بشأن الجرائم الإلكترونية؛ من قبيل ذلك مثلاً الجرائم الواقعة على أمن الدولة الداخلي والخارجي الواردة في قانون العقوبات للعام 1960 النافذ، ومن بينها الجرائم التي تنال من «هيبة الدولة»، والجرائم التي تهدف إلى «إضعاف الشعور القومي»، والجرائم التي «توهن نفسية الأمة»، ... وغيرها من عشرات المصطلحات الفضفاضة التي تنتهك المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية والمعايير الدولية ذات الصلة بشأن الحق في حرية الرأي والإعلام والحقوق الرقمية¹⁰.

وتكمن الإشكالية في أن اتّسع السلطة التقديرية لا يرتبط فقط بالعقوبة التي يمكن أن تترتب على الفعل، وإنما يبدأ منذ مرحلة تحديد ما إذا كان السلوك محل الفحص يدخل أصلاً ضمن نطاق التجريم أو يستدعي اتخاذ إجراء يتعلق بالمحتوى أو البيانات أو الأجهزة الإلكترونية. وكلما اتسعت العبارات المستخدمة في النص، زادت احتمالات اختلاف تفسيرها وتطبيقها من حالة إلى أخرى، ومن منظور حماية الفضاء المدني، يمكن أن تؤدي هذه الحالة إلى زيادة عدم اليقين لدى الصحافيين والنشطاء ومؤسسات المجتمع المدني بشأن الحدود التي تفصل بين التعبير المشروع والسلوك الذي قد يُعرّض صاحبه لإجراء قانوني، وهو ما قد يعزز الميل إلى تجنب بعض أشكال التعبير أو النشاط الرقمي، حتى في الحالات التي لا يترتب عليها، بالضرورة، اتخاذ إجراء فعلي.

4. المغالاة في فرض العقوبات على الجرائم الواردة: تمثل المادة 29 من القرار بقانون تجسيداً لتوجه تشريعي متشدد يوسع نطاق المسؤولية الجنائية ليشمل الأشخاص المعنوية (كمؤسسات المجتمع المدني والمؤسسات الإعلامية)، حيث تُفرض غرامات مالية باهظة وعقوبات قاسية تصل إلى الحرمان من ممارسة النشاط لمدة تصل إلى خمس سنوات أو حتى الحل النهائي. إن ربط عقوبة الحل والإغلاق بوجود جريمة معاقب عليها بالحبس لمدة لا تقل عن سنة، يمنح القضاء صلاحيات ذات أثر مباشر على الوجود القانوني والفعلي لتلك المؤسسات، ما يشكل «إعداماً مؤسسياً واقتصادياً» يتجاوز الفاعل الأصلي ليطال الموظفين والمستفيدين من خدمات تلك المؤسسات¹¹.

5. المغالاة بفرض العقوبات دون الاستناد إلى حكم قضائي: فالأصل حتى يتم إنفاذ الحكم أن يصدر حكم قضائي باتٌ ومنهي من المحكمة، وليس أمراً قضائياً يصدر من القاضي، حيث اعتبرت بعض نصوص القانون الإجراءات الأولى المتعلقة بتقييد الحريات والتفتيش والإغلاق والحجب مبنية على أمر قضائي، في حين أن نص المادة (70) من القانون ذاته، أعطى المحكمة صلاحية «إصدار قرار يتضمن مدة إغلاق المحل وحجب الموقع الإلكتروني ومصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجرائم المنصوص عليها في هذا القرار ... وأبرز مثال إغلاق مكتب الجزيرة الإعلامي».

6. المادة (66)¹² تعتبر أن كل الإجراءات المنصوص عليها في القرار بقانون سرية، وهذا يخالف المبدأ العام الذي ينص على أن الأصل بالمعلومات أن تكون عامة ما لم تقيد بنص (الأصل بالمعلومات الإتاحة). وهذا يفتح الباب أمام تفسيرات تعسفية قد تشمل معلومات لا تضر بالمصلحة العامة في حال نشرها، ما يشكل تهديداً مباشراً لحرية الرأي والتعبير والعمل الصحافي والحقوق وصعوبة الحصول على المعلومة.

10 مقابلة هاتفية أجرتها الباحثة مع المحامي عمار جاموس، الهيئة المستقلة لحقوق الإنسان، 2026/8/4.

11 وهذا ما أكدت عليه مؤسسة الحق في ورقة موقف صادرة عنها بشأن قرار بقانون الجرائم الإلكترونية وحجب مواقع إلكترونية المنشورة على الموقع الإلكتروني: <https://www.alhaq.org/ar/advocacy/16110.html>، تم الدخول إلى الموقع بتاريخ 2026/7/23.

12 تنص المادة (66) على أنه «كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون، في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلا العقوبتين».

شرعن مواد القرار بقانون الجرائم الإلكترونية المشار إليها أعلاه حجب عشرات المواقع الإخبارية والمنصات الحقوقية بقرارات قضائية مستندة إلى طلبات النيابة العامة، دون المرور بإجراءات المحاكمة العادلة ومنح المتهمين ضمانات المحاكمة، حيث أصدرت محكمة صلح رام الله في أكتوبر/تشرين الأول 2019، قراراً بحجب 59 موقعاً إلكترونياً وصفحات على مواقع التواصل الاجتماعي، بناءً على طلب من النائب العام الفلسطيني. وأوضحت النيابة العامة أن هذه المواقع تمارس التهجم والإساءة إلى رموز في السلطة الوطنية، وتنتشر محتوى من شأنه تهديد الأمن القومي والسلام الأهلي، والإخلال بالنظام العام والآداب العامة، وإثارة الرأي العام الفلسطيني. كما أصدرت محكمة صلح رام الله، في الخامس من شباط 2025، قراراً بحجب عدد من المواقع الإلكترونية التابعة لشبكة الجزيرة الإعلامية لمدة أربعة أشهر، بناءً على طلب تقدم به النائب العام¹³.

كما وثق الائتلاف من أجل النزاهة والمساءلة (أمان) في تقاريره الرقابية تزايد حالات استدعاء مواطنين ونشطاء المجتمع المدني وتوقيفهم قضائياً على خلفية منشورات رقمية انتقدوا فيها السياسات العامة، أو أثاروا قضايا تحوم حولها شبهات فساد في إدارة الشأن العام، بالاعتماد على قانون الجرائم الإلكترونية رقم (10) لسنة 2018 وتعديلاته؛ إذ استمرت محاكمة كل من المدير التنفيذي ومستشار مجلس إدارة ائتلاف (أمان)، وذلك على خلفية نشر تقرير ائتلاف (أمان) السنوي الذي أشار إلى وجود أشخاص في مكتب الرئيس يستغلون وظيفتهم للحصول على مكاسب ومصالح خاصة¹⁴. كما وثقت مؤسسات حقوقية أخرى اعتقال عدد من النشطاء والصحافيين ومنتقدي الشأن العام وملاحقتهم استناداً إلى هذا القرار بقانون، فمثلاً تم اعتقال الصحافي يوسف الفقيه في كانون الثاني/يناير 2019، وصودرت أجهزة إلكترونية من منزله. فوفق لجنة حماية الصحفيين، أخبر محاميه اللجنة بأن التحقيق انصب على مقالات ومنشورات كتبها الفقيه على فيسبوك، وأنه اتهم بـ«التحريض على إثارة النعرات الطائفية» بموجب قانون الجرائم الإلكترونية. كما أشارت اللجنة إلى مقال نشره الفقيه في كانون الأول/ديسمبر 2018، دعا فيه السلطة الفلسطينية إلى قطع العلاقات مع إسرائيل والسماح باحتجاجات للعصيان المدني¹⁵.

نلاحظ أن هذه القرارات تأتي في إطار سياسة توظيف المنظومة التشريعية، لتضييق مساحات الحريات في المجتمع الفلسطيني؛ سيما حرية الرأي والتعبير¹⁶، وتقويض الحق في الوصول إلى المعلومات وحصار التعددية الإعلامية. كما أن استخدام أدوات الملاحقة الرقمية بموجب قانون الجرائم الإلكترونية يمثل شكلاً ممنهجاً من تقويض بيئة المساءلة المجتمعية ومكافحة الفساد، حيث يدفع مؤسسات المجتمع المدني والمؤسسات الإعلامية والناشطين إلى فرض رقابة ذاتية صارمة ومفرطة تجنباً لأي خطأ قد يعرض المؤسسة بأسرها لخطر الحل، الأمر الذي يتقاطع سلباً مع مبادئ حرية التعبير والعمل الأهلي والمساءلة المجتمعية المكفولة قانوناً ودولياً.

ثانياً. انتهاك الحق في الخصوصية وحماية البيانات

تنص المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية على عدم جواز تعريض أي شخص لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو مراسلاته¹⁷.

وفي هذا الإطار، تثير الأحكام المتعلقة بحفظ بيانات المستخدمين، وتمكين الجهات المختصة من الوصول إليها، تساؤلات بشأن مدى كفاية الضمانات القانونية والقضائية المقررة لحماية الخصوصية، ولا سيما في ضوء المبادئ التي أرستها لجنة حقوق الإنسان بالأمم المتحدة، والتي تؤكد ضرورة أن يكون أي تدخل في الحق في الخصوصية¹⁸:

1. منصوصاً عليه في القانون (Legality).
2. يحقق هدفاً مشروعاً.
3. ضرورياً لتحقيق ذلك الهدف.
4. متناسباً بحيث لا يتجاوز القدر اللازم لتحقيق الغاية.
5. خاضعاً لرقابة قضائية فعالة وضمنيات ضد التعسف.

13 https://www.alaraby.co.uk/entertainment_media

14 الائتلاف من أجل النزاهة والمساءلة (أمان)، التقرير السنوي الثامن عشر (واقع النزاهة ومكافحة الفساد في فلسطين 2025)، ص 27.

15 <https://cpj.org/201901/palestinian-security-forces-arrest-journalist-yous/>

16 الهيئة الدولية لدعم حقوق الشعب الفلسطيني (حشد)، ورقة موقف بشأن قرار بقانون الجرائم الإلكترونية وسياسة حجب المواقع في الأراضي الفلسطينية، رامي معين محسن وأحمد نسيب موسى، 2019، ص 1.

المركز الفلسطيني لاستقلال المحاماة والقضاء «مساواة»، ورقة موقف بعنوان يُلغى على الفور قرار بقانون الجرائم الإلكترونية، ولإبعاد بناء منظومة العدالة بإرادة مجتمعية، 2019، المنشورة على الموقع:

<https://musawa.ps/post/the-decree-law-on-cyber-crimes-shall-be-abolished-immediately.html>

17 <https://www.ohchr.org/ar/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

18 <https://www.ohchr.org/ar/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data>

وبمراجعة القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، نجد نصوصاً تنتهك الحق في الخصوصية، وتتعارض مع القانون الأساسي الفلسطيني لسنة 2003، وبخاصة المادة (32) التي تكفل الحق في الخصوصية، كما تتعارض مع المعايير الدولية لحقوق الإنسان من خلال التوسع المفرط في التدخل بالحق في الخصوصية وسرية الاتصالات؛ ومن أبرز هذه المواد الآتي:

1. النص الوارد في المادة (51)¹⁹ من القرار بقانون، لا سيما في بندها الثالث، الذي يلزم مزودي الخدمة بالاحتفاظ بمعلومات المشتركين لمدة لا تقل عن ثلاث سنوات، ما يشكل أداة لجمع وتخزين جماعي للبيانات يخلق بيئة مراقبة مستمرة تطال الأفراد كافة، بمعزل عن أي شبهة جنائية محددة. وفي حين تطلبت بعض البنود أوامر قضائية صارمة (مثل قرار قاضي المحكمة في البند الرابع أو أوامر الجهات القضائية في البند الثاني)، فإن منح النيابة العامة صلاحيات مباشرة في طلب معلومات المشتركين (البند الأول) يضعف من ضمانات الإشراف القضائي المسبق. هذا التوسع في فرض الالتزامات الرقمية الطويلة، وتسهيل النفاذ إلى بيانات الأفراد، وبخاصة النشطاء والمعارضين، يمس الحق في الخصوصية وحرمة الحياة الخاصة. كما أن هذا الخلل في الإجراءات يفتقر إلى مبدأ الضرورة والتناسب، ويغيب عنه الإشراف القضائي المسبق، كما أنه يقوض الثقة في الفضاء الرقمي، ما ينعكس سلباً وبشكل مباشر على الفضاء المدني من خلال دفع الصحفيين والنشطاء والمؤسسات الحقوقية نحو الرقابة الذاتية خوفاً من تعقب بياناتهم ومراسلاتهم، ويقوض تماماً قدرتهم على حماية مصادرهم وأداء أدوارهم الرقابية في المسائلة وشفافية الشأن العام.

2. تُكرس المادة (52)²⁰ من القرار بقانون بشأن الجرائم الإلكترونية وتعديلاته إشكاليات عبر منح النيابة العامة، أو من تتدبه من مأموري الضبط القضائي، صلاحيات واسعة لتفتيش الأشخاص والأماكن والوسائل التكنولوجية، مع إجازة تجديد أمر التفتيش بلا سقف زمني محدد طالما بقيت مبرراته قائمة، فضلاً عن خطورة البند الرابع الذي يجيز لوكيل النيابة الإذن بـ «النفاذ المباشر» إلى الأجهزة والبيانات دون توفير إشراف قضائي مسبق. هذا التوسع في إجراءات التفتيش الرقمي، وغياب الضمانات الصارمة، ينتهك، بشكل صارخ، مبدأ الضرورة والتناسب في المساس بالحق في الخصوصية وحرمة المراسلات، ما ينعكس بآثار مدمرة على الفضاء المدني من خلال تقويض أمان الصحفيين والمدافعين عن حقوق الإنسان، وتهديد سرية مصادرهم، ودفعهم نحو الرقابة الذاتية خشية التعرض للتعسف والتفتيش الرقمي غير المبرر.

3. تضمنت المادة (53)²¹ من القرار بقانون بشأن الجرائم الإلكترونية إشكاليات قانونية تتمثل في منح النيابة العامة صلاحيات واسعة للضبط والتحفيز على كامل نظام المعلومات أو الأجهزة والبيانات دون إحاطتها بضمانات قضائية مسبقة، فضلاً عن تجاوز مبدأ «تخصيص الأدلة»، من خلال إمكانية حجز أنظمة كاملة قد تتضمن مراسلات وبيانات لا علاقة لها بالجريمة محل التحقيق. كما تعطي فرصة لأن يكون هناك تصيد بحيث يكون الهدف البحث عن جريمة، ولذلك فإن النصوص الموجودة حالياً المتعلقة بالتفتيش تنتهك ضمانات الحق في الخصوصية. إن هذا النوع من تقييد الخصوصية والحريات الشخصية، يؤدي عملياً إلى تعطيل أعمال المؤسسات الحقوقية والإعلامية، ما يشكل عبئاً تعسفياً يعمق حالة انعدام الثقة الرقمية، ويدفع الفاعلين في الفضاء المدني نحو مزيد من الرقابة الذاتية خشية فقدان

19 المادة (51) يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي:

1. تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.
2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية، مع مراعاة الإجراءات الواردة في المادة (39) من هذا القرار بقانون.
3. الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة (1) من هذه المادة.
4. التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها.
- 20 تنص المادة (52) على أنه:
1. للنيابة العامة أو من تتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.
2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة.
3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.
4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.
5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية ولجرائم الاتصالات وتكنولوجيا المعلومات.
- 21 تنص المادة (53) على أنه:

1. للنيابة العامة الحصول على الأجهزة، أو الأدوات، أو الوسائل، أو البيانات، أو المعلومات الإلكترونية، أو بيانات المرور، أو البيانات المتعلقة بحركة الاتصالات، أو بمستعملها، أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية.
2. للنيابة العامة الإذن بالضبط والتحفيز على كامل نظام المعلومات، أو جزء منه، أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.
3. إذا لم يكن الضبط والتحفيز على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات.
4. إذا استحال إجراء الضبط والتحفيز بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال الوسائل المناسبة كافة، لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.
5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفز عليه، بما في ذلك الوسائل الفنية لحماية محتواها.
6. تحرر قدر الإمكان قائمة بالمضبوط المتحفز عليه بحضور المتهم أو من وجد لديه المضبوط المتحفز عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفز عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ، وساعته، وعدد المحاضر، والقضية.

السيطرة على أنظمتهم ومحتوَاهم المهني. فلذلك، يجب أن تكون هناك جريمة أو اشتراك في وقوع جريمة، وأن يكون هناك قرار من القاضي المختص يجيز التفتيش أو النفاذ إلى محتويات الوسائل الإلكترونية، وأن يكون القرار القضائي مُسبباً بما ينسجم مع نص القانون الأساسي²².

4. تعكس المادة (54)²³ من القرار بقانون بشأن الجرائم الإلكترونية وتعديلاته ذروة التدخل في سرية الاتصالات والحق في الخصوصية، نظراً لمنحها صلاحيات بالغة الخطورة تخوّل قاضي الصلح بمنح إذن للنائب العام بمراقبة وتسجيل الاتصالات الإلكترونية في جرائم قد لا تقتصر على الجنايات الخطيرة، بل تمتد لتشمل جناحاً ثقل عقوبتها عن سنة (أو تعادلها)، فضلاً عن الخطورة البالغة للفقرة الثانية التي تمنح النائب العام أو مساعديه صلاحية إصدار أمر بالجمع والتزويد الفوري لبيانات الاتصالات والمرور، ومعلومات المشتركين بشكل مباشر، ودون الحاجة لإذن قضائي مسبق. هذا التوسع في التنصت الرقمي وجمع البيانات الفورية، المتقاطع مع التزامات مزودي الخدمة الواردة في المادة (51) بالاحتفاظ بالبيانات لسنوات طويلة، يهدم المعايير الدولية للضرورة والتناسب، ويقوض تماماً الثقة الرقمية، ما يُلقي بآثار سلبية على الفضاء المدني، ويجبر الصحفيين والمدافعين عن حقوق الإنسان على العمل في بيئة ملوّهة الرقابة الذاتية وخطر التعسف الأمني.

من أبرز الوقائع التي كشفت عن المخاطر العملية التي يمكن أن يتعرض لها الحق في الخصوصية في البيئة الرقمية الفلسطينية، ما رافق الاحتجاجات التي اندلعت عقب وفاة الناشط السياسي نزار بنات في حزيران/يونيو 2021. فقد وثقت مؤسسات حقوقية شكاوى وتقارير تفيد بقيام أشخاص يُشتبه بارتباطهم بالأجهزة الأمنية، وبعضهم بلباس مدني، بالاستيلاء على هواتف عدد من المشاركين والمشاركات في الاحتجاجات، ولا سيما النساء والصحفيات. كما صودرت هواتف عدد من الناشطين والناشطات والصحفيين/ات، وأفادت التقارير باستخراج صور شخصية من بعض هذه الهواتف ونشرها عبر وسائل التواصل الاجتماعي²⁴.

تكتسب هذه الواقعة أهمية من منظور الفضاء المدني، بالنظر إلى أن الهاتف المحمول يحتوي عادةً على قدر واسع من المراسلات والصور والملفات وجهات الاتصال والمعلومات الشخصية والمهنية، بحيث يمكن أن يؤدي الوصول إليه إلى كشف معلومات تتجاوز نطاق الواقعة أو النشاط محل الاهتمام. وفي سياق الاحتجاجات، فإن الوصول إلى هذه البيانات أو نشر بعضها قد لا يقتصر أثره على الأشخاص الذين طالبتهم الإجراءات، بل يمكن أن يمتد إلى أشخاص آخرين يرتبطون بهم اجتماعياً أو مهنيًا، وأن يثير مخاوف لدى الصحفيين والنشطاء والمدافعين عن حقوق الإنسان بشأن سلامة بياناتهم واتصالاتهم.

وتشير هذه الآثار إلى أن المساس بالخصوصية الرقمية يمكن أن يتجاوز نطاق الحق الفردي إلى التأثير في البيئة التي يعمل فيها المجتمع المدني. فضعف الشعور بالأمان الرقمي قد يدفع بعض الفاعلين إلى الحد من اتصالاتهم أو مشاركتهم في الأنشطة المدنية، أو إلى تجنب تداول معلومات حساسة أو التواصل مع المصادر والمؤسسات الحقوقية والإعلامية، بما قد يحد من قدرة هذه الجهات على التنظيم والتعبير وتوثيق القضايا العامة وممارسة أدوارها الرقابية.

ومن هذا المنظور، فإن حماية الخصوصية الرقمية لا تمثل حماية لحق فردي فحسب، وإنما ترتبط أيضاً بتوفير بيئة تمكن الصحفيين والمدافعين عن حقوق الإنسان ومؤسسات المجتمع المدني من أداء وظائفهم بحرية واستقلالية. فكلما زادت مخاطر النفاذ المباشر غير المنضبط إلى البيانات والاتصالات والمصادر المهنية، زادت احتمالات الرقابة الذاتية، وتراجع استخدام الوسائل الرقمية في العمل المدني، وهو ما قد ينعكس بصورة غير مباشرة على قدرة المجتمع المدني والإعلام على كشف المخالفات والقضايا العامة ومساءلة المؤسسات العامة، بما في ذلك في مجال مكافحة الفساد وتعزيز النزاهة.

وبالتالي، تكشف هذه الواقعة عن أن ضمانات الخصوصية الرقمية لا ينبغي النظر إليها باعتبارها حماية تقنية أو فردية فحسب، بل باعتبارها أحد المكونات الضرورية لوجود فضاء مدني آمن وفاعل، ولا سيما عندما يتعلق الأمر بالصحفيين والنشطاء والمدافعين عن حقوق الإنسان الذين يعتمد عملهم، بصورة أساسية، على سرية الاتصالات وحماية البيانات والمصادر المهنية.

22 وهذا ما أكد عليه الأستاذ عمار جاموس باحث قانوني في الهيئة المستقلة لحقوق الإنسان في مقابلة أجرتها الباحثة بتاريخ 2026/8/4.
23 تنص المادة (54) على أنه: 1. لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد مرة واحدة، بناءً على توافر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة.

24 <https://www.alhaq.org/ar/monitoring-documentation/18746.html>

أولاً. النتائج والاستخلاصات

بعد مراجعة الإطار التشريعي والتحليلي للقرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، وتحليل عدد من نصوصه ذات الصلة بالحقوق والحريات العامة، ومقارنتها بالمعايير الدولية لحقوق الإنسان، ولا سيما ما يتصل بحرية الرأي والتعبير والحق في الخصوصية، وانعكاساتها على الفضاء المدني، يمكن استخلاص النتائج الآتية:

1. اتساع نطاق أثر القرار بقانون بشأن الجرائم الإلكترونية على الفضاء المدني:

خلصت الورقة إلى أن أثر القرار بقانون لا يقتصر على تنظيم مكافحة الجرائم الإلكترونية، وإنما يمتد إلى البيئة التي يمارس فيها الأفراد والصحافيون والنشطاء والمدافعون عن حقوق الإنسان ومؤسسات المجتمع المدني أنشطتهم الرقمية (الفضاء المدني). ويظهر ذلك بصورة خاصة في الأحكام المتعلقة بالاحتفاظ ببيانات المستخدمين، والوصول إلى الأجهزة والأنظمة والبيانات، وتفتيش أنظمة المعلومات وضبطها، ومراقبة الاتصالات، وحجب المواقع والمحتوى الإلكتروني.

ويزداد هذا الأثر في ضوء استخدام سلطات إنفاذ القانون بعض النصوص لمصطلحات واسعة الدلالة وفضفاضة، مثل «النظام العام» و«السلم الأهلي»، إلى جانب محدودية بعض الضمانات القضائية والرقابية، ما قد يؤدي إلى عدم وضوح الحدود الفاصلة بين النشاط المشروع والنشاط الذي قد يكون عرضة للمساءلة، الأمر الذي قد يدفع الأفراد والمؤسسات إلى توخي الحذر في ممارسة حقوقهم. وبالتالي، فإن أثر هذه الأحكام قد لا يظهر، فقط، عند اتخاذ إجراءات قانونية بحق أشخاص أو مؤسسات، وإنما قد يظهر بصورة غير مباشرة من خلال تردد بعض الناشطين والعاملين في مؤسسات المجتمع المدني في التعبير أو نشر المعلومات أو التواصل والمشاركة في الأنشطة الرقمية خشية التعرض للمساءلة.

2. قصور في ضمانات المحاكمة العادلة والخصوصية:

تبين الورقة أن بعض الأحكام المتعلقة بمراقبة الاتصالات، وحفظ البيانات، والوصول إلى المعلومات الرقمية، وحجب المواقع الإلكترونية، لا توفر في جميع الحالات ضمانات قضائية سابقة ومشددة تكفل حصر هذه الإجراءات في الحالات الضرورية والمشروعة، وتحدد نطاقها ومدتها والجهات المخولة باتخاذها. ويثير ذلك إشكالات جدية بشأن حماية الحق في الخصوصية وضمانات المحاكمة العادلة، ولا سيما في ضوء التزامات دولة فلسطين بموجب العهد الدولي الخاص بالحقوق المدنية والسياسية.

3. الفجوة التشريعية في حماية البيانات الشخصية:

تبين الورقة أن بعض أحكام القرار بقانون تلزم مزودي خدمات الاتصالات والجهات ذات الصلة بالاحتفاظ ببيانات المستخدمين وبيانات حركة الاتصالات والسجلات الرقمية، وتوفيرها للجهات المختصة وفقاً للإجراءات المنصوص عليها في القانون. وفي ظل عدم وجود قانون فلسطيني شامل ومتكامل لحماية البيانات الشخصية، ينظم بصورة دقيقة جمع البيانات ومعالجتها والاحتفاظ بها ومشاركتها، ويحدد أغراض استخدامها، والجهات المخولة بالوصول إليها، ومدة الاحتفاظ بها، وآليات الرقابة والمساءلة والطعن والتظلم، تظل هناك فجوة تشريعية قد تزيد من مخاطر الوصول إلى البيانات أو استخدامها على نحو يتجاوز الغرض الذي جُمعت من أجله، بما قد يؤثر في مستوى الحماية المقررة للخصوصية والثقة في البيئة الرقمية.

4. تأثير القرار بقانون الجرائم الإلكترونية على سلوك العاملين في الفضاء المدني وعلى الرقابة والمساءلة الاجتماعية:

خلصت الورقة إلى أن بعض أحكام القرار بقانون بشأن الجرائم الإلكترونية لا توفر ضمانات كافية لحماية الحق في الخصوصية، ولا سيما الأحكام التي تمنح جهات إنفاذ القانون صلاحيات واسعة في تفتيش الأجهزة أو الحصول عليها والوصول إلى البيانات والاتصالات. وقد لا يقتصر أثر هذه الصلاحيات على الإجراءات القانونية، بل قد يمتد إلى سلوك الصحافيين والمدافعين عن حقوق الإنسان والعاملين في مؤسسات المجتمع المدني، من خلال زيادة الخشية من الملاحقة واللجوء إلى الرقابة الذاتية وتجنب بعض أشكال التعبير والتواصل. وقد يؤثر ذلك في قدرة الفاعلين المدنيين والإعلاميين على الوصول إلى المعلومات وتبادلها، وتوثيق المخالفات، والتواصل مع المصادر.

وتبرز أهمية ذلك في مجال مكافحة الفساد، حيث تشكل حرية الوصول إلى المعلومات، والإبلاغ عن المخالفات، ومناقشة أداء المؤسسات العامة، عناصر أساسية للرقابة والمساءلة المجتمعية.

ثانياً. التوصيات

في ضوء مجموع النتائج السابقة، نرى أن التحدي لا يتمثل في وجود تشريع يجرم الجرائم الإلكترونية أو ينظم إجراءات التحقيق فيها، وإنما في ضمان أن تتم مكافحة هذه الجرائم ضمن إطار قانوني واضح ومحدد ومتوازن، يضمن عدم تحول الصلاحيات المقررة لمواجهة الجريمة الإلكترونية إلى قيود غير متناسبة على الحقوق والحريات، أو إلى عامل يحد من الفضاء المدني. وعليه، نورد مجموعة من التوصيات التي تساهم في حماية الفضاء المدني، وتمكنه من القيام بدوره في المساءلة المجتمعية ومكافحة الفساد:

1. ضرورة قيام مجلس الوزراء ووزارة العدل بمواءمة قرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018 وتعديلاته بالكامل مع الاتفاقيات والمعايير الدولية والممارسات الفضلى بشأن حرية الرأي والتعبير والحريات الإعلامية والحقوق الرقمية والحق في الخصوصية، ولا سيما المواد التالية، علماً بأنه في مشروع قرار بقانون رقم () لسنة 2026 بتعديل قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته، المنشور على منصة التشريع التابعة لوزارة العدل بتاريخ 2026/8/2، قد أخذ ببعض هذه التوصيات وفقاً لما هو موضح في الهوامش أدناه:

- المادة (3): العمل على توحيد وحدة متخصصة للجرائم الإلكترونية واقتصارها فقط عند الشرطة²⁵.
- المادة (29): بحيث يتم إلغاء عقوبة الحل النهائي للأشخاص المعنوية باعتبارها عقوبة استثنائية لا يجوز اللجوء إليها إلا في حالات محددة جداً، وتحديد تلك الجرائم في القرار بقانون؛ مثل إنشاء الشخص المعنوي بقصد ارتكاب الجرائم، أو اتخاذه نشاطاً إجرامياً رئيسياً²⁶.
- استبدال الحل النهائي بعقوبات متدرجة، مثل:
 - الإنذار.
 - إزالة المحتوى المخالف.
 - الغرامة المتناسبة.
 - وقف النشاط المرتبط بالمخالفة لمدة محددة.
 - إلزام المؤسسة بتبني برامج امتثال وتدابير تصحيحية.
 - إلزام المحكمة بمراعاة مبدأ التناسب قبل توقيع أي عقوبة، مع الأخذ في الاعتبار:
 - جسامة الجريمة.
 - حجم الضرر.
 - مدى استفادة الشخص المعنوي من الجريمة.
 - أثر العقوبة على العاملين والمستفيدين والجمهور.
- النص صراحة على حماية المؤسسات الإعلامية ومؤسسات المجتمع المدني من الحل أو الإغلاق بسبب أفعال فردية لا تعبر عن سياسة المؤسسة أو لم تكن بعلم إدارتها.

- المادة (51):²⁷ يتم تعديلها بما يضمن إعادة ضبط نطاق الالتزامات المفروضة على مزودي الخدمة، من خلال قصر الاحتفاظ ببيانات المشتركين على البيانات الضرورية والمدة اللازمة لتحقيق غرض مشروع ومحدد، وإخضاع أي طلب للحصول على هذه البيانات أو النفاذ إليها لإذن قضائي مسبق ومسبب يحدد نطاق الطلب ومدته والغاية منه، مع وضع ضمانات واضحة لحماية البيانات من الاستخدام غير المشروع أو الإفصاح غير المبرر، وحصر أي صلاحيات استثنائية للنيابة العامة في حالات الضرورة القصوى وبإشراف قضائي لاحق. كما نوصي بإلغاء الاحتفاظ الشامل والطويل الأمد بالبيانات لجميع المستخدمين دون تمييز، واعتماد نظام يقوم على مبادئ الضرورة والتناسب والرقابة القضائية الفعالة، بما يحقق التوازن بين متطلبات مكافحة الجرائم الإلكترونية، وحماية الحق في الخصوصية وحرمة الحياة الخاصة المكفولة بالمعايير الدولية.

25 تم الأخذ بالملاحظة في مشروع القانون المقترح، واقتصار تشكيل الوحدة على جهاز الشرطة، وليس الشرطة وقوى الأمن.
26 تم الأخذ بالملاحظة جزئياً، إذ ميز التعديل بين الحبس والسجن، ورفع الحد الأدنى للعقوبة اللازمة للحكم بحل الشخص المعنوي من الحبس لمدة سنة إلى السجن لمدة لا تقل عن ثلاث سنوات، بما يضيّق نطاق الحالات التي يمكن فيها حل الشخص المعنوي. في المقابل، أبقى النص على عبارة «عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له»، ولم يؤخذ بالملاحظة المتعلقة بحذفها.
27 لم يتم الأخذ بهذه الملاحظة في مشروع القانون المقترح.

- المادة (52):²⁸ استبدال صلاحية وكيل النيابة بالإذن المباشر بالإنفاذ بإذن قضائي مسبق، لأن التفتيش الرقمي يمس نطاقاً واسعاً من الحياة الخاصة.
- إلغاء عبارة «يجوز تجديده أكثر من مرة ما دامت مبرراته قائمة» لأنها لا تضع سقفاً زمنياً واضحاً، واستبدالها برقابة قضائية على كل تجديد.
- تحديد نطاق البيانات لمنع ما يعرف بـ«الصيد في البيانات» (Fishing Expedition): أي البحث غير المحدد عن معلومات قد لا تكون مرتبطة بالجريمة.
- إضافة ضمانات لحماية البيانات غير المتعلقة بالجريمة، وبخاصة بيانات الصحفيين والمدافعين عن حقوق الإنسان.
- إقرار استثناء ضيق لحالات الاستعجال مع رقابة قضائية لاحقة، بدلاً من منح سلطة واسعة غير مقيدة.
- المادة (53): إعادة ضبطها بما يضمن التوازن بين متطلبات التحقيق في الجرائم الإلكترونية، وبين حماية الحق في الخصوصية وسرية البيانات، وذلك من خلال تعزيز الرقابة القضائية، وتحديد نطاق إجراءات التحفظ ومدتها، وقصرها على القدر الضروري والمرتبط مباشرة بالجريمة محل التحقيق، بما ينسجم مع مبادئ الشرعية والضرورة والتناسب المنصوص عليها في المعايير الدولية لحقوق الإنسان.²⁹
- المادة (54) نقترح أن تعدل بحيث:³⁰
 - تقتصر المراقبة على الجرائم الخطيرة (تحدد بالقانون) بدلاً من جميع الجناح المعاقب عليها بالحبس سنة أو أكثر.
 - اشتراط الإذن القضائي ليس لمراقبة المحتوى فحسب، وإنما، أيضاً، للحصول على بيانات المرور وبيانات المشتركين، باعتبار أن هذه البيانات محمية بموجب المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية.
 - إلزام المحكمة بتطبيق مبدأ الوسيلة الأقل تقييداً، بحيث لا تلجأ المراقبة إلا إذا تعذر الحصول على الدليل بوسيلة أخرى أقل مساساً بالخصوصية.
 - منع أوامر المراقبة العامة أو الشاملة، من خلال إلزام القاضي بتحديد الأشخاص، والبيانات، والمدة، والغرض.
 - إلزام السلطات بإتلاف البيانات غير المرتبطة بالتحقيق وعدم الاحتفاظ بها دون مبرر.
 - إقرار حق الطعن والرقابة القضائية اللاحقة لتعزيز ضمانات المشروعية والمساءلة.
- المادة (59): نقترح أن يتم تحديد الحالات التي تهدد الأمن القومي، أو النظام العام، أو الآداب العامة. وحصر صلاحيات حجب المواقع بموجب أحكام قضائية مسبقة ومسببة خاضعة للاستئناف والطعن.³¹
- المادة (65): بشأن التجريم والمعاقبة بالتشريع ذاته للجريمة المرتكبة باستخدام الشبكة الإلكترونية، نوصي بحذف هذه المادة من القرار بقانون والخاصة بإحالة لقانون العقوبات، كونها متزيدة، ولا حاجة إليها في ظل سريان القواعد العامة في قانون العقوبات على المسائل التي لم يرد بشأنها نص خاص، تطبيقاً للقاعدة العامة «الخاص يقيد العام»³².
- المادة (66): نقترح حصر تجريم إفشاء السرية بحالات محددة ينص عليها في القانون، والتي يترتب عليها فعلياً الإضرار بسير العدالة، أو تعريض حياة الأشخاص للخطر، أو المساس بسلامة التحقيقات الجنائية الجارية حصراً.³³
- إلغاء الحبس على قضايا النشر، واستبدالها بالتعويض المدني، إن كان له مقتضى، انسجاماً مع الاتفاقيات والمعايير الدولية وبخاصة المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي انضمت إليه دولة فلسطين والتعليق العام رقم (34) على المادة (19) الصادر عن اللجنة المعنية بحقوق الإنسان في الأمم المتحدة.³⁴

2. توصيات إلى القضاء والنيابة العامة:

- التوقف عن إصدار قرارات حجب المواقع والمنصات الحقوقية والإعلامية بشكل جماعي وتلقائي بناءً على طلبات الجهات الأمنية والتنفيذية.
- توفير بيئة حامية للمدافعين عن حقوق الإنسان ومكافحي الفساد عبر التفسير الضيق والمقيد للنصوص العقابية لمصلحة صيانة الحريات العامة والدستورية.

28 تم الأخذ جزئياً بالملاحظة، حيث نصت المادة المقترحة على أن يراعى عند تفتيش الأشخاص والأماكن الوارد في الفقرة (1) من هذه المادة الأحكام الواردة في قانون الإجراءات الجزائية النافذ.

29 تم الأخذ بالملاحظة جزئياً في مشروع القانون المقترح، حيث تم تعديل المادة بإزالة العبارات النفضاضة «قدر الإمكان»، التي تعطي لمأمور الضبط القضائي صلاحية واسعة، وأصبحت ملزمة أكثر.

30 لم يؤخذ بالملاحظة عليها بالمطلق في مشروع القانون المقترح.

31 لم يتم الأخذ بالملاحظة بالمطلق.

32 لم يتم الأخذ بالملاحظة بالمطلق في مشروع القانون المقترح.

33 تم الأخذ بالملاحظة، حيث تم تضيق نطاق السرية ليصبح النص «كل من أفشى سرية إجراءات سير الدعوى الجزائية»: بمعنى أن النص أصبح مقتصر على إجراءات التقاضي، ما أتاح إباحة المعلومات، وهو يُعتبر تقدماً ملحوظاً نوعاً ما.

34 لم يتم الأخذ بهذه الملاحظة في مشروع القانون المقترح.

3. توصيات إلى مؤسسات المجتمع المدني:

- مواصلة بناء قدرات الفاعلين في الفضاء المدني على مهارات الأمان الرقمي والمقاومة القانونية والملاحقة القضائية للانتهاكات.
- مؤسسة الرصد والتوثيق والتبليغ الممنهج عن قضايا التوقيف والاستدعاء المرتبطة بالتعبير الرقمي.

ثالثاً. آليات الضغط والمناصرة لتبني التوصيات وتنفيذها:

لضمان عدم بقاء هذه التوصيات حبيسة الأدراج، ولتفعيل الضغط المجتمعي على مراكز صنع القرار، تقترح الورقة تبني الآليات والأدوات الآتية:

- التحالفات: تشكيل تحالف وطني واسع يضم ائتلاف (أمان)، والهيئة المستقلة لحقوق الإنسان، ومؤسسة الحق، ونقابة المحامين، ونقابة الصحفيين، وممثلي كليات الحقوق بالجامعات، والمنظمات الأهلية، لتوحيد الصوت المطالب لإصدار قانون جديد يتواءم مع المعايير والاتفاقيات الدولية.
- حملات المناصرة الرقمية الشاملة: إطلاق حملات توعية عبر منصات التواصل الاجتماعي لتثقيف الجمهور بحقوقهم الرقمية، وعرض قصص واقعية لضحايا تكميم الأفواه الرقمي، واستخدام وسوم موحدة للضغط من أجل تعديل التشريعات.
- التقاضي: رفع قضايا أمام المحكمة الدستورية العليا للطعن في دستورية المواد الفضفاضة بدعوى مخالفتها لأحكام القانون الأساسي الفلسطيني، والاتفاقيات الدولية التي انضمت إليها فلسطين.
- المساءلة وجلسات الاستماع: عقد جلسات استماع ومواجهة علنية وموثقة مع ممثلي الرئاسة ووزارة العدل والأمانة العامة لمجلس الوزراء والنيابة العامة لعرض الفجوات في القانون، وإلزامهم بتقديم توضيحات أمام الرأي العام.
- استثمار قنوات الشركاء الدوليين: الاستمرار في تزويد المقرررين الخاصين للأمم المتحدة والشركاء الدوليين بتقارير دورية تبرز الفجوة بين الالتزامات الدولية لفلسطين وبين ممارساتها التشريعية على الأرض، لتوظيف الضغط الدولي لدعم المطالبة بتعديل القرار بقانون الجرائم الإلكترونية لينسجم مع الاتفاقيات الدولية.

أولاً. المصادر:

1. القانون الأساسي لسنة 2003 وتعديلاته.
2. قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات (المدمج)، المنشور على المرجع الإلكتروني للجريدة الرسمية:
[/https://mjr.ogb.gov.ps/MergedLegislations/ViewText/41](https://mjr.ogb.gov.ps/MergedLegislations/ViewText/41)
3. العهد الدولي الخاص بالحقوق المدنية والسياسية 1966.
4. الإعلان العالمي لحقوق الإنسان 1948.

ثانياً. المراجع:

1. التقارير:
 - الائتلاف من أجل النزاهة والمساءلة (أمان). التقرير السنوي الثامن عشر (واقع النزاهة ومكافحة الفساد في فلسطين 2025)، 2025.
 - الائتلاف من أجل النزاهة والمساءلة (أمان). تقييم المساحة المتاحة أمام الفضاء المدني الفلسطيني للمشاركة في صنع السياسات العامة والمساءلة على تنفيذها، 2024. رام الله- فلسطين.
 - مؤسسة الحق، ورقة موقف بشأن قرار بقانون الجرائم الإلكترونية وحجب مواقع إلكترونية، 2026.
 - الهيئة الدولية لدعم حقوق الشعب الفلسطيني (حشد)، رامي معين محسن وأحمد نسيب موسى، ورقة موقف بشأن قرار بقانون الجرائم الإلكترونية وسياسة حجب المواقع في الأراضي الفلسطينية، 2019.
 - المركز الفلسطيني لاستقلال المحاماة والقضاء «مساواة»، ورقة موقف بعنوان ليُلغى على الفور قرار بقانون الجرائم الإلكترونية وليعاد بناء منظومة العدالة بإرادة مجتمعية، 2019.
2. البحوث:
 - أحمد عبد المالك سويلم أبو درابي. «حماية القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية للحقوق الدستورية»، مجلة الباحث للدراسات والأبحاث القانونية والقضائية، العدد 48، 2022، ص 40-58.
 - كيara عياد. الأمن الرقمي لمراقبة من؟ قانون الجرائم الإلكترونية في فلسطين، منشورات مبادرة الإصلاح العربي، 2026.
3. المواقع الإلكترونية:
 - <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and>
 - <https://www.wattan.net/ar/video/465588.html>. (تاريخ الدخول: 2026/08/14)
 - https://civicusmonitor.contentfiles.net/media/documents/Arabic_Monitor_Report_PPUA_2025.pdf
 - <https://www.facebook.com/watch/?v=4038683603041710>. (تاريخ الدخول: 2026/08/14)
 - <https://www.alhaq.org/ar/advocacy/16110.html>. (تاريخ الدخول: 2026/07/23)
 - <https://www.arab-reform.net/ar/publication>. (تاريخ الدخول: 2026/08/14)
 - <https://icspr.ps/4712>. (تاريخ الدخول: 2026/08/14)
 - <https://musawa.ps/post/the-decree-law-on-cyber-crimes-shall-be-abolished-immediately.html>. (تاريخ الدخول: 2026/08/14)

ثالثاً. المقابلات:

- عمار جاموس، باحث قانوني في الهيئة المستقلة لحقوق الإنسان، 2026/8/4.
- أشرف أبو حية، مستشار قانوني في مؤسسة الحق، 2026/8/13.



الائتلاف من أجل النزاهة والمساءلة (أمان)

المؤسسة الفلسطينية المعتمدة من قبل منظمة الشفافية الدولية منذ العام 2006، تأسس في العام 2000 من مجموعة من المؤسسات الأهلية الفاعلة في مجال الديمقراطية والحكم الصالح وحقوق الإنسان، سعياً لتحقيق رؤيته نحو «مجتمع فلسطيني خالٍ من الفساد».

يسعى الائتلاف حالياً إلى خلق وقيادة حراك مجتمعي عبر قطاعي مناهض للفساد، والإسهام في إنتاج ونقل وتوطين المعرفة بالفساد ومكافحته على الصعيد الوطني والإقليمي والدولي. يحرص ائتلاف أمان على القيام بدوره الرقابي Watchdog على النظام الوطني للنزاهة بالتركيز على المشاركة المجتمعية وتفعيل دور مؤسسات المجتمع المدني، ووسائل الإعلام في الرقابة والمساءلة وخلق بيئة محصنة ومساهمة في الكشف عن جرائم الفساد والحد من انتشاره.

رام الله: عمارة الريمائي - الطابق الأول - شارع الإرسال ص.ب: رام الله 339 القدس 69647
هاتف: 022989506 - 022974949 فاكس: 022974948
غزة: شارع حبوش، متفرع من شارع الشهداء - عمارة دريم / الطابق الثالث
هاتف: 082884767 تلفاكس: 082884766
الموقع الإلكتروني: www.aman-palestine.org

f @ X v in /AmanCoalition

هذا المشروع بدعم من



EUROPEAN UNION
الاتحاد الأوروبي

