ورقة حقائق حول واقع الحقوق الرقمية الفلسطينية للمنظمات الأهلية الفلسطينية وما صاحبها عقب حرب الإبادة

ضمن إطار عمل المبادرة الفلسطينية لتعميق الحوار العالمي والديمقراطية "مفتاح" في مجال الدبلوماسية الرقمية والعامة، ولدواعي توسيع نطاق التواصل العالمي لدعم القضية الفلسطينية، نفذت "مفتاح" مسحاً تقييمياً يرصد القدرات المعرفية لدى مؤسسات المجتمع المدني في الضفة الغربية (بما فيها القدس) وقطاع غزة حول الحقوق الرقمية، ومدى الممارسة بهذه المعارف. يعكس هذا المسح الواقع المعقد للحقوق الرقمية في فلسطين المحتلة، حيث أُجري المسح لتقييم مدى جاهزية مؤسسات المجتمع المدني للتعامل مع التحديات الرقمية المتزايدة، خاصة بعد حرب الإبادة أكتوبر 2023. يسلط هذا المسح الضوء على الفجوات في المعرفة الرقمية والبنية التحتية للأمان الرقمي، التي تُعد تحديًا بارزًا يعوق المؤسسات عن حماية بياناتها وأداء دورها بفعالية.

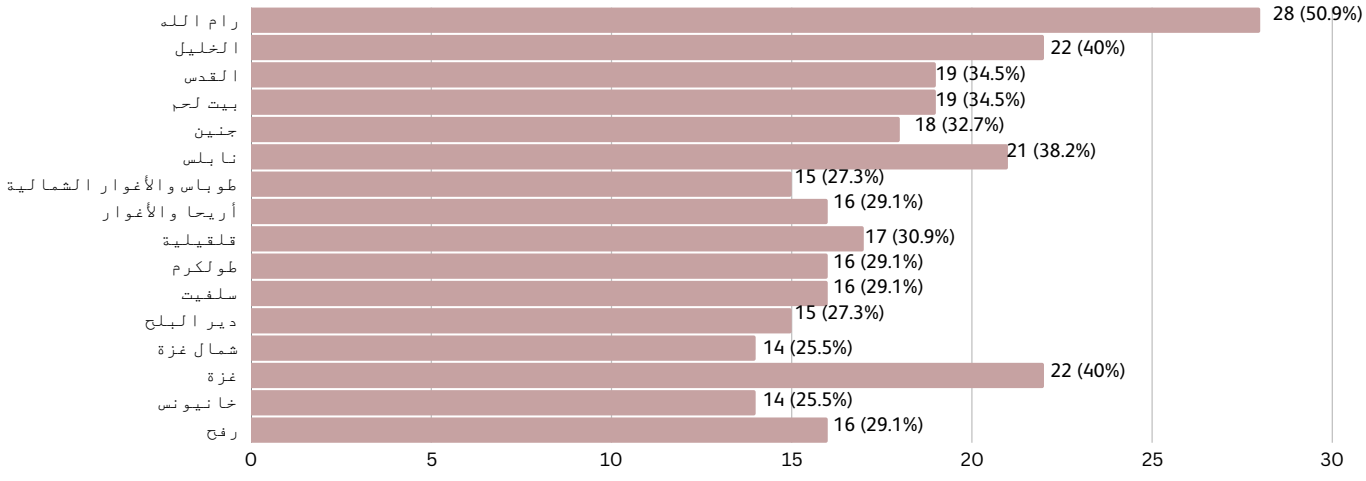
اعتمد المسح على المنهج الوصفي، شمل استبيانات من 55 مؤسسة موزعة بين الضفة الغربية (بما فيها القدس) وقطاع غزة. بالإضافة إلى مقابلات معمقة مع ست مؤسسات مختصة بالحقوق الرقمية، ومؤسسات نسوية، وأخرى عاملة في قطاع غزة. وتم تحليل البيانات الكمية باستخدام أدوات متقدمة مثل SPSS وNVivo.

الوصف العام

وفقًا لنتائج الاستبيان، تستهدف منظمات المجتمع المدني فئات متنوعة ضمن عملها، وتُعتبر النساء الفئة الأكثر استهدافًا بنسبة 43.6%، تليها فئة الأطفال بنسبة 16.4%، ثم كبار السن بنسبة 12.7%. كما تمثل فئة الشباب 10.9% من المستهدفين، بينما تبلغ نسبة الأشخاص ذوي الاحتياجات الخاصة 9.1%. أما الإعلاميون، فيشكلون نسبة 7.3% من الفئات المستهدفة. إضافة إلى ذلك، تشير النتائج إلى أن 34.5% من هذه المنظمات تستهدف جميع الفئات دون تمييز، مما يعكس شمولية العينة.
ويتوزع نطاق عمل المؤسسات الفلسطينية عبر المحافظات كالتالي: رام الله يأتي في المقدمة بنسبة 50.9% من المؤسسات، يليه الخليل بنسبة 40%، والقدس بنسبة 34.5%، ثم نابلس بنسبة 38.2%. كما يمتد نطاق عمل المؤسسات إلى محافظات بيت لحم وجنين وطولكرم وسلفيت بنسبة 29.1% لكل منها، وطوباس والأغوار الشمالية بنسبة 32.7%، وأريحا والأغوار بنسبة 27.3%، وقلقيلية بنسبة 25.5%

أما في قطاع غزة، فيشمل نطاق عمل المؤسسات شمال غزة بنسبة 40%، وخان يونس بنسبة 29.1%، وغزة بنسبة 40%، بينما يغطي رفح بنسبة 25.5%، ودير البلح بنسبة 27.3%.

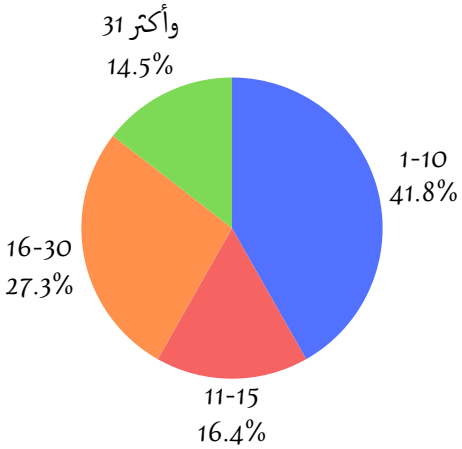
الشكل رقم (1): توزيع المؤسسات في المحافظات الفلسطينية المختلفة



توزعت مواقع مؤسسات المجتمع المدني الفلسطينية المشاركة في المسح بين المدن والمخيمات والقرى، حيث تتمركز غالبية المؤسسات في المدن بنسبة 74.5%، أما القرى، فتحتضن 16.4% من مقارّ هذه المؤسسات في المقابل، فإن 9.1% فقط من المؤسسات تتخذ من المخيمات مقرًا أساسيًا لها، هذا التوزيع يعكس التركز الحضري للمؤسسات ويبرز الحاجة إلى زيادة التواجد في المناطق الريفية والمخيمات لتعزيز الشمولية والوصول إلى الفئات المهمشة والمحتاجة.

وتتفاوت أحجام مؤسسات المجتمع المدني الفلسطينية المشاركة في المسح، من حيث عدد الموظفين، حيث أظهر المسح أن 27.3% من المؤسسات تضم من 1 إلى 10 موظفين، بينما تضم 16.4% منها بين 11 و15 موظفًا. يشكل العدد الأكبر من المؤسسات 41.8% والتي يتراوح عدد موظفيها بين 16 و30 موظفًا، في حين أن 14.5% فقط من المؤسسات تضم أكثر من 31 موظفًا. يعكس هذا التوزيع تنوعًا في حجم المؤسسات، حيث تظل غالبية المؤسسات صغيرة إلى متوسطة الحجم، وهو ما يتناسب مع العينة التي يسعى المسح للتركيز عليها.

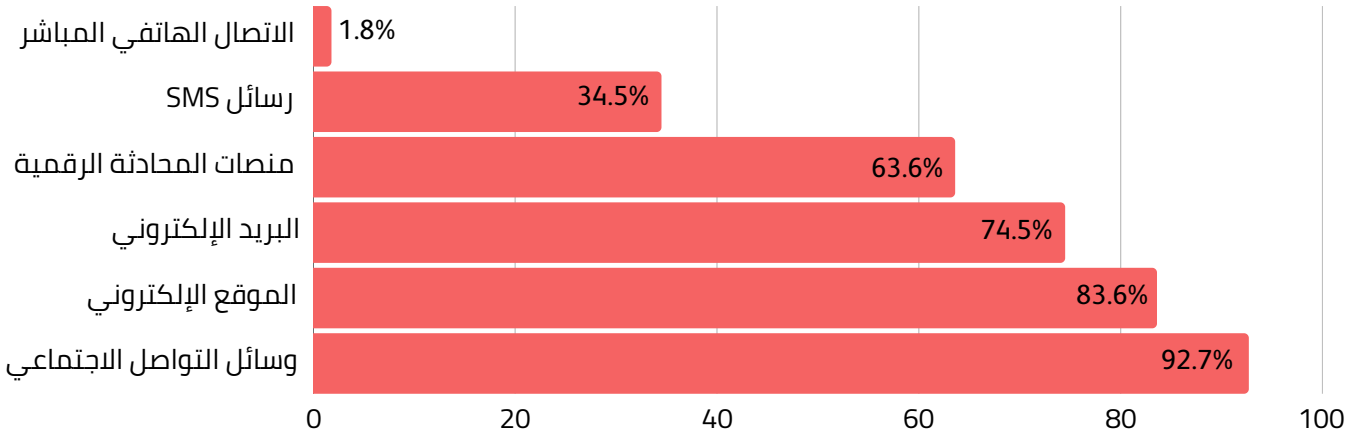
الشكل رقم (2): حجم مؤسسات المجتمع المدني وفقاً لعدد العاملين فيها



وسائل التواصل لدى المؤسسات

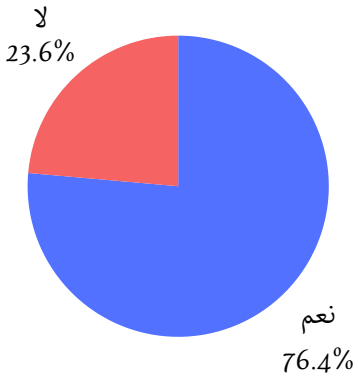
تعتمد مؤسسات المجتمع المدني الفلسطينية المشاركة بالمسح على مجموعة متنوعة من الوسائل الرقمية للتواصل مع الجمهور والمستفيدين، حيث تُعد وسائل التواصل الاجتماعي الخيار الأكثر شيوعًا، إذ تستخدمها 92.7% من المؤسسات، مما يشير إلى أهمية هذه المنصات كقنوات رئيسية للتواصل والنشر. تليها المواقع الإلكترونية التي تستخدمها 83.6% من المؤسسات، كما تعتمد 74.5% من المؤسسات على البريد الإلكتروني كوسيلة للتواصل، ويستخدم 63.6% منها منصات المحادثة الرقمية مثل واتساب، وعلى الرغم من تطور وسائل الاتصال، إلا أن 34.5% من المؤسسات لا تزال تستخدم الرسائل النصية (SMS)، في حين أن 1.8% فقط تعتمد على الاتصال الهاتفي المباشر.

شكل رقم (3): الوسائل الرقمية التي تستخدمها المؤسسات للتواصل مع الجمهور والمستفيدين



أظهر المسح أن 76.4% من المؤسسات لديها معرفة حول الحقوق الرقمية، بينما 23.6% منها تفتقر إلى هذه المعرفة، وهذه النسبة تشير إلى أن هناك شريحة مهمة من المؤسسات بحاجة إلى رفع مستوى معرفتها وفهمها لهذه الحقوق بشكل شامل.

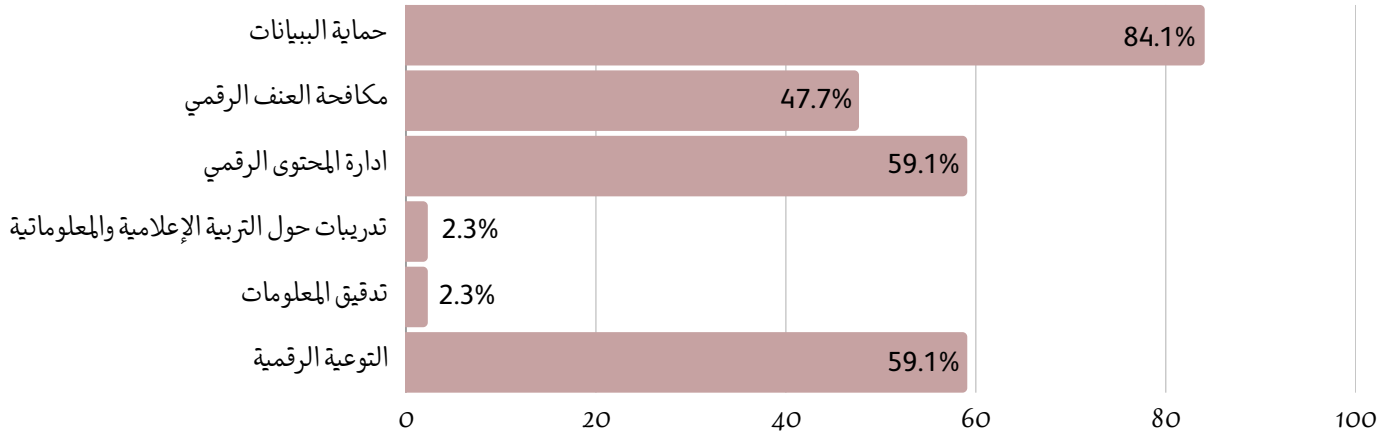
الشكل رقم (4): الموقف حول المعرفة بالحقوق الرقمية وفقاً للمؤسسات



وتظهر النتائج علاقة واضحة بين مقرّ المؤسسة الأساسي وفهمها للحقوق الرقمية، وفقًا للاستبيان: ففي المدن، 86.0% من المؤسسات لديها فهم واضح للحقوق الرقمية، بينما 14.0% منها تفتقر لهذا الفهم. أما في القرى، تبلغ نسبة المؤسسات التي لديها فهم واضح للحقوق الرقمية 66.7%، مقارنةً بـ 33.3% تفتقر لهذا الفهم. بينما في المخيمات، فإن 16.7% فقط من المؤسسات المشاركة لديها فهم واضح للحقوق الرقمية، بينما 83.3% تفتقر إلى هذا الفهم.

وتُظهر المؤسسات التي أفادت بأن لديها فهمًا واضحًا للحقوق الرقمية وكيفية تطبيقها في العمل اليومي تركيزًا على عدة مواضيع رئيسية لتعزيز هذه المعرفة. تأتي حماية البيانات الشخصية في الصدارة، حيث تشكل أولوية لدى 84.1% من هذه المؤسسات، بينما يعتبر مكافحة العنف الرقمي ضروريًا بنسبة 47.7%. كما تُولي المؤسسات اهتمامًا كبيرًا بإدارة المحتوى الرقمي والتوعية الرقمية بنسبة 59.1%، في حين تشير بعض المؤسسات أيضًا إلى أهمية تدقيق المعلومات والتربية الإعلامية وإن كان ذلك بنسب أقل. يعكس هذا التركيز إدراكًا متزايدًا للحاجة إلى بناء قدرات متكاملة في مجالات الحماية وإدارة المحتوى، بما يضمن تعزيز الحقوق الرقمية بشكل فعّال ومستدام.

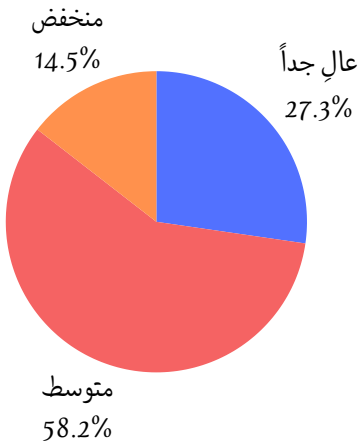
الشكل رقم (5): الحقوق الرقمية التي تركز عليها مؤسسات المجتمع المدني



أما على صعيد المعرفة فيما يتعلق بالتهديدات الرقمية والانتهاكات، كشف المسح أن 58.2%من المؤسسات تصنف معرفتها بالمخاطر الرقمية على أنها "متوسطة"، بينما 27.3% تعتبر معرفتها "منخفضة"، في حين 14.5% فقط تعتقد أن لديها معرفة "عالية جدًا، ويوضح هذا تفاوتًا في مستوى الوعي بين المؤسسات، ما يشير إلى ضرورة تعزيز المعرفة حول التهديدات الرقمية.

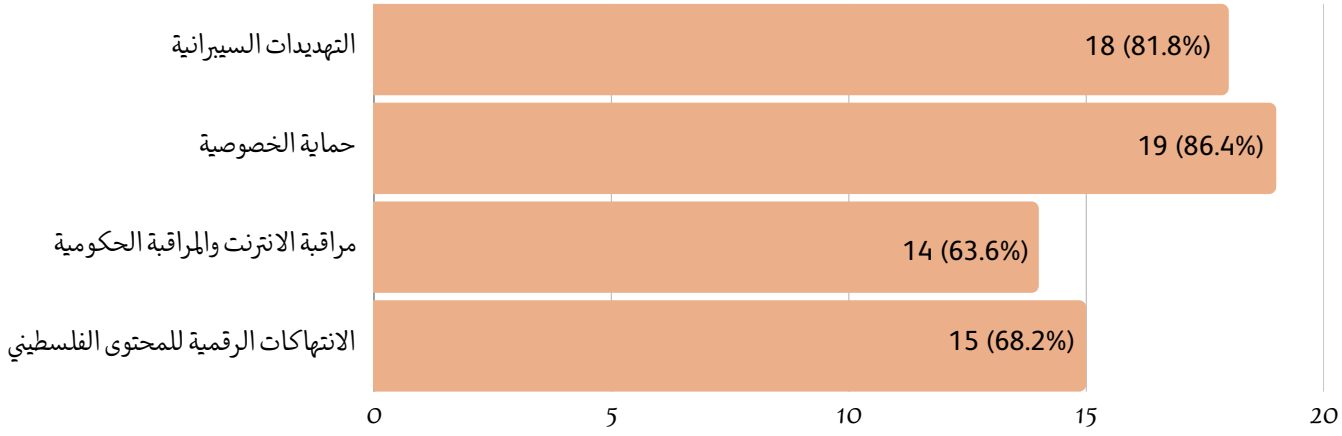
أما على صعيد المعرفة فيما يتعلق بالتهديدات الرقمية والانتهاكات، كشف المسح أن 58.2%من المؤسسات تصنف معرفتها بالمخاطر الرقمية على أنها "متوسطة"، بينما 27.3% تعتبر معرفتها "منخفضة"، في حين 14.5% فقط تعتقد أن لديها معرفة "عالية جدًا، ويوضح هذا تفاوتًا في مستوى الوعي بين المؤسسات، ما يشير إلى ضرورة تعزيز المعرفة حول التهديدات الرقمية.

الشكل رقم (6): الحقوق الرقمية التي تركز عليها مؤسسات المجتمع المدني



وبالنسبة للمؤسسات التي صنفت فهمها للحقوق الرقمية بأنه "منخفض"، أظهرت النتائج أن هناك حاجة لتعزيز عدة مجالات: جاءت حماية الخصوصية الأكثر من حيث الحاجة للتعزيز، حيث أبدت 86.4% من المؤسسات رغبتها في تحسين قدراتها في هذا الجانب. تلتها التهديدات السيبرانية بنسبة 81.8%، مما يشير إلى القلق المتزايد حول الأمان الرقمي. كما أظهرت 68.2% من المؤسسات حاجتها إلى تعزيز المعرفة بخصوص الانتهاكات الرقمية للمحتوى الفلسطيني، في حين أن 63.6% من المؤسسات ترى أن مراقبة الإنترنت والمراقبة الحكومية تحتاج إلى اهتمام أكبر.

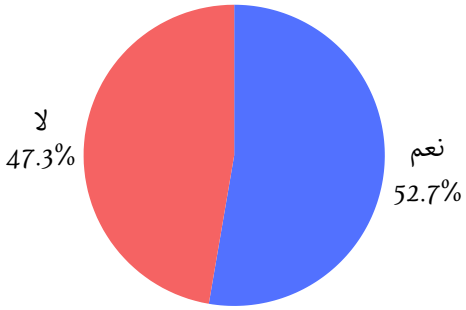
الشكل رقم (7): الاحتياجات التمكينية لتحسين الفهم حول الحقوق الرقمية وفقاً للمؤسسات



سياسات حماية الحقوق الرقمية

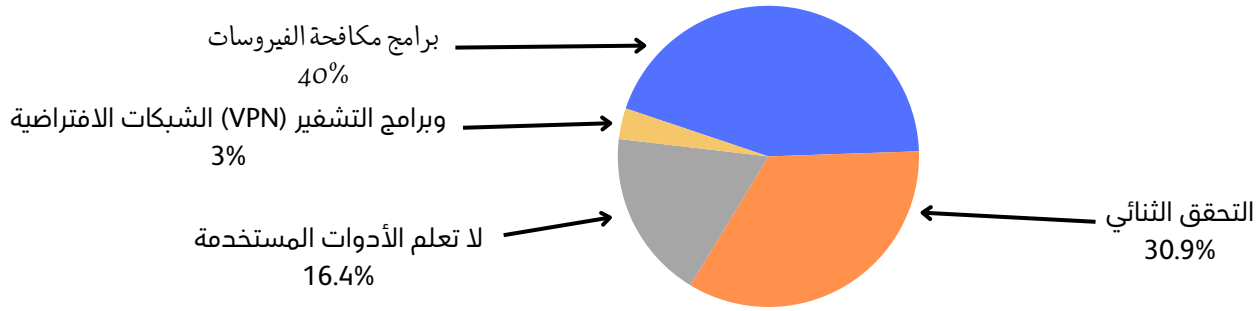
أبرزت نتائج المسح أن 52.7% من المؤسسات لا تمتلك سياسات محددة لحماية الحقوق الرقمية، بينما 47.3% طبقت سياسات مثل سياسات الخصوصية

الشكل رقم (8): نسبة المؤسسات التي تمتلك سياسات للحقوق الرقمية



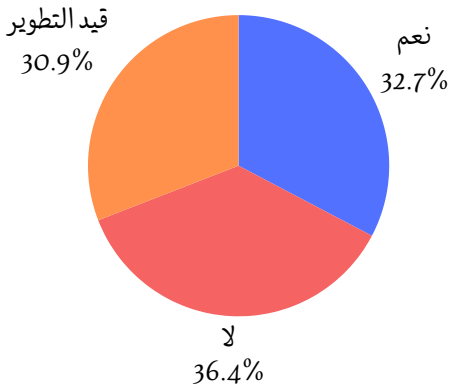
وأظهرت البيانات المتعلقة بالأدوات الرقمية التي تعتمد عليها المؤسسات لتأمين البيانات والمعلومات أن 40% من المؤسسات تستخدم برامج مكافحة الفيروسات كوسيلة أساسية للحماية. كما أن 30.9% تعتمد على التحقق الثنائي لتعزيز الأمان الرقمي. بالإضافة إلى ذلك، 16.4% من المؤسسات أشارت إلى أنها لا تعلم الأدوات المستخدمة لحماية البيانات، مما قد يعكس نقصًا في المعرفة التقنية في بعض المؤسسات، وهناك أيضًا نسبة صغيرة من المؤسسات تعتمد على الشبكات الافتراضية الخاصة (VPN)، وبرامج التشفير، وأدوات أخرى، إلا أن هذه النسب كانت أقل من الخيارات الأخرى الواضحة.

شكل رقم (9): الأدوات الرقمية المستخدمة لتأمين البيانات والمعلومات في المؤسسات



وحول اتباع المؤسسات لسياسة واضحة للتعامل مع البيانات الشخصية الرقمية للنساء والفتيات تنوعاً في الآراء بين المستجيبين، فقد أشار 32.7% من المؤسسات إلى اتباعهم سياسة واضحة للتعامل مع البيانات، ما يعني أن حوالي ثلث المؤسسات تتبع بالفعل سياسة حماية البيانات الشخصية، وفي المقابل، عبّرت 36.4% من المؤسسات أنها لا تتبع سياسة واضحة للتعامل مع البيانات، في حين أشار 30.9% من المؤسسات أن سياستها قيد التطوير حاليًا، ولكنها لم تُنفذ بعد بشكل كامل.

شكل رقم (10): مدى تبني سياسات واضحة لحماية البيانات الشخصية للنساء والفتيات

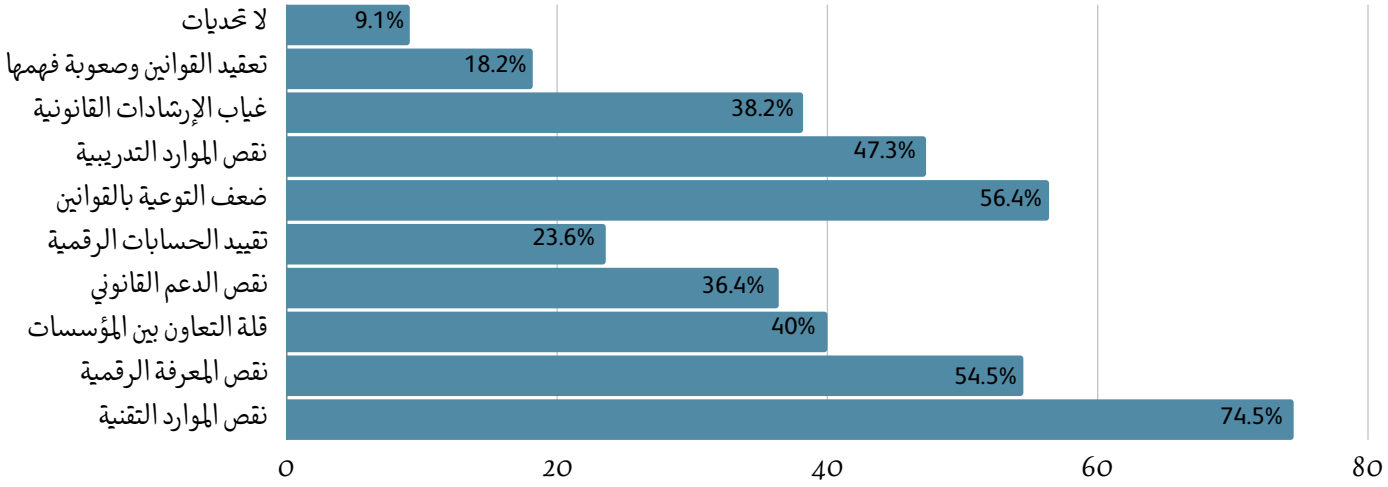


التحديات في حماية الحقوق الرقمية

عبرت 74.5% من المؤسسات أنها تعاني من نقص في الموارد التقنية، و54.5% من نقص حول المعرفة الرقمية، و40% من المؤسسات ترى أن قلة التعاون بين المؤسسات تمثل تحديًا كبيرًا، و36.4% تفتقر إلى الدعم القانوني، و23.6% من المؤسسات تواجه تقييدًا في الحسابات الرقمية، ما يشير إلى تحديات متعددة في الحماية الرقمية.

وتعتبر 56.4% من المؤسسات أن ضعف التوعية بالقوانين يمثل تحديًا رئيسيًا، بينما 47.3% تعاني من نقص الموارد التدريبية، و38.2% ترى أن غياب الإرشادات القانونية يزيد من الصعوبات، و18.2%فقط من المؤسسات تعاني من تعقيد القوانين وصعوبة فهمها، بينما 9.1% لم تواجه تحديات تُذكر.

شكل رقم (11): التحديات الرئيسية التي تواجه المؤسسات بما يتعلق بالحماية الرقمية

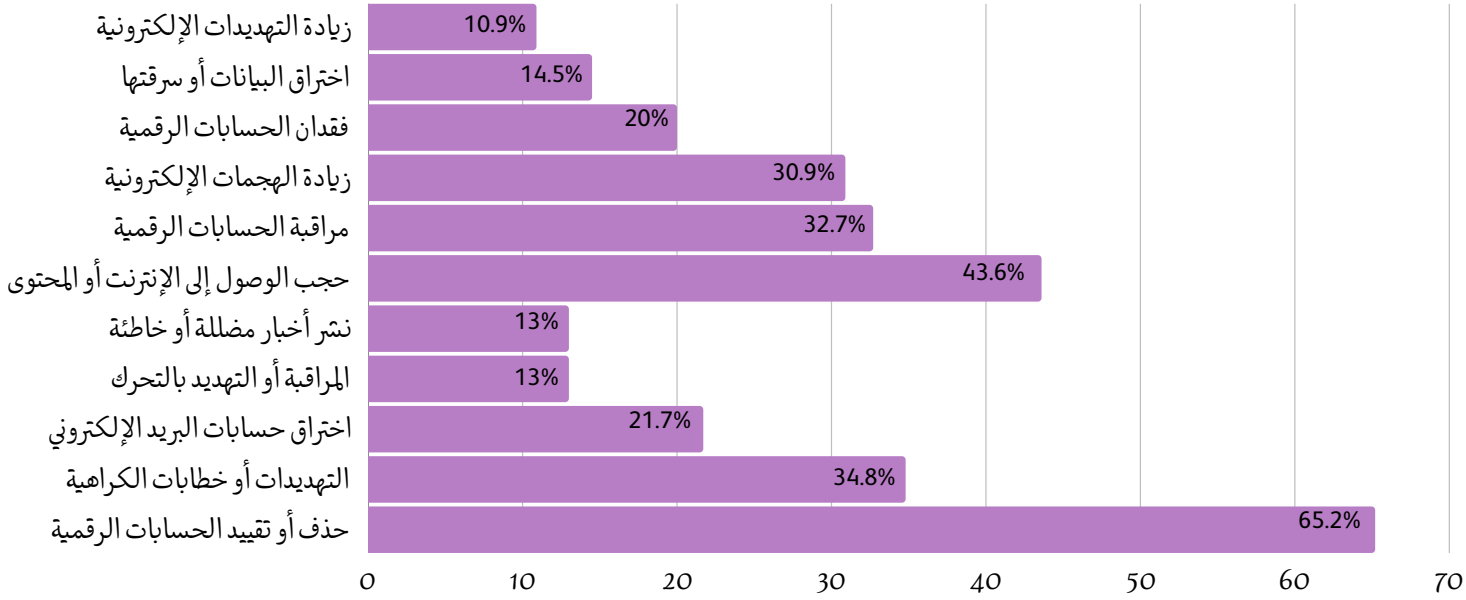


الحقوق الرقمية إبان حرب الإبادة

أظهر المسح أنه وعقب السابع من أكتوبر 2023، أشارت 60% من المؤسسات إلى أنها لم تتعرض لأي انتهاكات رقمية مباشرة، بينما أكدت 40% منها تعرضها لانتهاكات بشكل مباشر. وبالنسبة للمؤسسات التي تعرضت لانتهاكات، كانت أبرز أنواع الانتهاكات هي حذف أو تقييد الحسابات الرقمية بنسبة 65.2%، تليها التهديدات أو خطابات الكراهية عبر الإنترنت بنسبة 34.8%، ثم اختراق حسابات البريد الإلكتروني بنسبة 21.7%. وشملت الانتهاكات الأخرى المراقبة أو التهديد بالتحرك ضد العمل الرقمي ونشر أخبار مضللة أو معلومات خاطئة، حيث مثلت كل منها نسبة 13% من الحالات.

من ناحية أخرى، واجهت المؤسسات تحديات رقمية رئيسية شملت حجب الوصول إلى الإنترنت أو المحتوى الرقمي بنسبة 43.6%، ومراقبة الحسابات الرقمية بنسبة 32.7%، وزيادة الهجمات الإلكترونية بنسبة 30.9%، بينما أفادت 20% من المؤسسات بفقدان الحسابات الرقمية، و14.5% بحدوث اختراق للبيانات أو سرقتها، و10.9% بزيادة التهديدات الإلكترونية ضد المؤسسات.

شكل رقم (12): أبرز الانتهاكات الرقمية التي واجهت المؤسسات بعد السابع من أكتوبر 2023

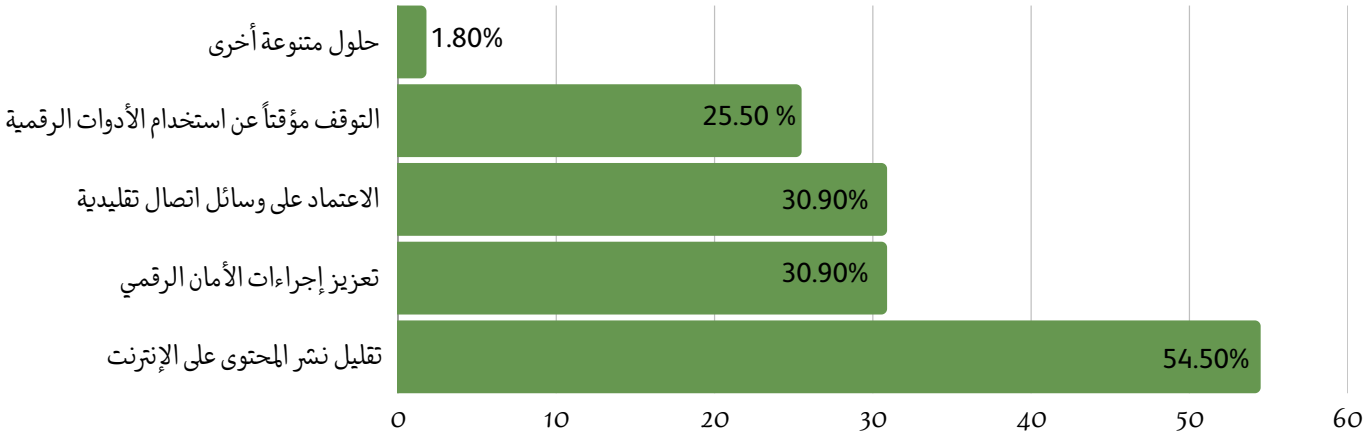


وحول كيفية تعامل المؤسسات مع هذه التهديدات والانتهاكات الرقمية بعد 7 أكتوبر 2023، أشارت المؤسسات، بنسبة 41.8%، أنها تطبق سياسات داخلية للحماية كإجراء للتعامل مع هذه التهديدات، فيما أفادت 32.7% من المؤسسات بتقديم بلاغات للجهات المختصة كإجراء رئيسي. بينما اختارت 25.5% من المؤسسات التعاون مع جهات قانونية للتصدي لهذه التحديات، وقدمت 16.4% منها دعمًا نفسيًا وتقنيًا للضحايا المتأثرين. أما 20% من المؤسسات فأشارت إلى أنها لا تتعامل مع هذه التهديدات والانتهاكات بشكل مباشر.

وحول تأثير التصعيد على استخدام التكنولوجيا أو توثيق الانتهاكات والتواصل مع المستفيدين، اضطرت 54.5% من المؤسسات إلى تقليل نشر المحتوى على الإنترنت كإجراء احترازي. كما أفادت 30.9% من المؤسسات بأنها لجأت إلى تعزيز إجراءات الأمان الرقمي، بينما اعتمدت 30.9% أخرى على وسائل اتصال تقليدية بدلاً من الوسائل الرقمية.

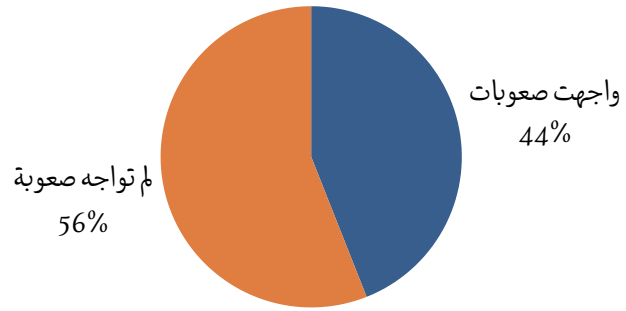
من جهة أخرى، توقفت 25.5% من المؤسسات مؤقتًا عن استخدام الأدوات الرقمية كليًا، وهناك مجموعة صغيرة من المؤسسات (1.8% لكل منها) لجأت إلى حلول متنوعة أخرى، مثل محاولة تجاوز خوارزميات مواقع التواصل، بسبب تقليل التفاعل مع المنشورات.

شكل رقم (13): أبرز المتغيرات على صعيد استخدام التكنولوجيا والتواصل الالكتروني بعد 7 أكتوبر 2023



أظهرت نتائج المسح أن 56.4% من المؤسسات لم تواجه صعوبة في الوصول إلى الإنترنت أو وسائل الاتصال الأخرى خلال الأحداث، في حين أفادت 43.6% بوجود صعوبات كبيرة أثرت على أدائها. شملت هذه الصعوبات انقطاعات متكررة في خدمة الإنترنت ونقصًا في توافر الكهرباء، مما أدى إلى توقف مؤقت عن العمل أو تأخير في التواصل مع المستفيدين والزملاء، خصوصًا في المناطق الأكثر تأثرًا مثل قطاع غزة وجنين. وأوضح المشاركون أن هذه الانقطاعات أثرت بشكل كبير على قدرة المؤسسات على توثيق الأحداث والتحقق من المعلومات، حيث أدى تدمير البنية التحتية للاتصالات إلى صعوبة التنقل والتواصل بين الموظفين.

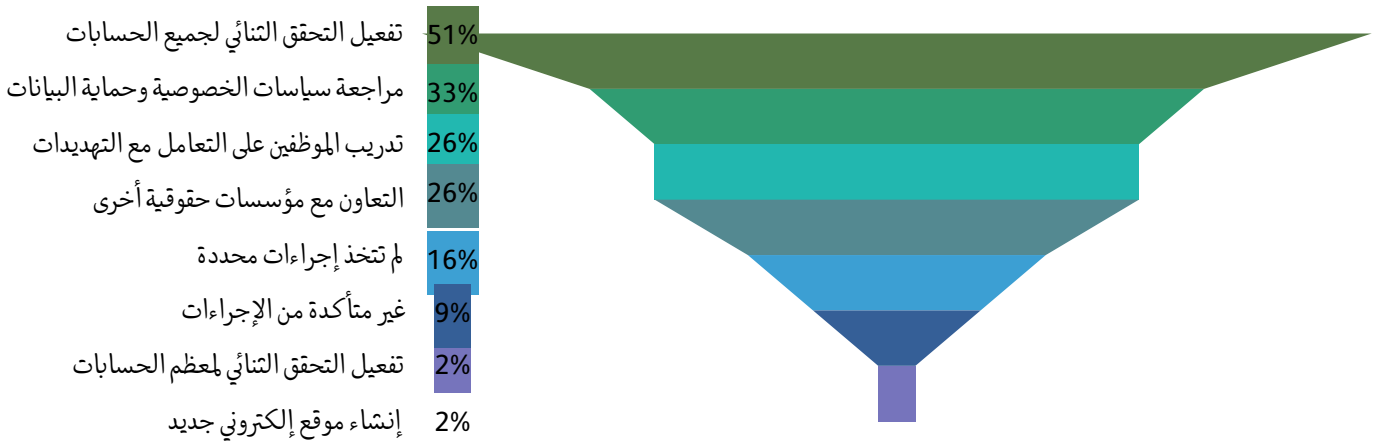
شكل رقم (14): حجم المؤسسات التي واجهت صعوبة في الوصول إلى الإنترنت



وبالإضافة إلى الصعوبات اللوجستية، أفادت بعض المؤسسات بتعرض مواقعها الرسمية لمحاولات اختراق وضغوط متزايدة على مستوى مراقبة المحتوى وتقييد النشر، مما زاد من التحديات التي تواجهها في أداء مهامها بفعالية. كما أن انقطاع الإنترنت لفترات طويلة نتيجة القصف والنزوح المتكرر حال دون إقامة بدائل مؤقتة للاتصال، وأدى إلى عزلة بعض الفرق الميدانية ومنعهم من الوصول إلى خطوط اتصال بديلة. في ظل هذه الظروف، اضطرت بعض المؤسسات إلى التنقل سيرًا على الأقدام للوصول إلى الفئات المستفيدة، ما يعكس التحديات الجسيمة التي تواجهها المؤسسات في استمرارية العمل الميداني وتقديم خدماتها بفعالية في بيئة شديدة التعقيد والتوتر.

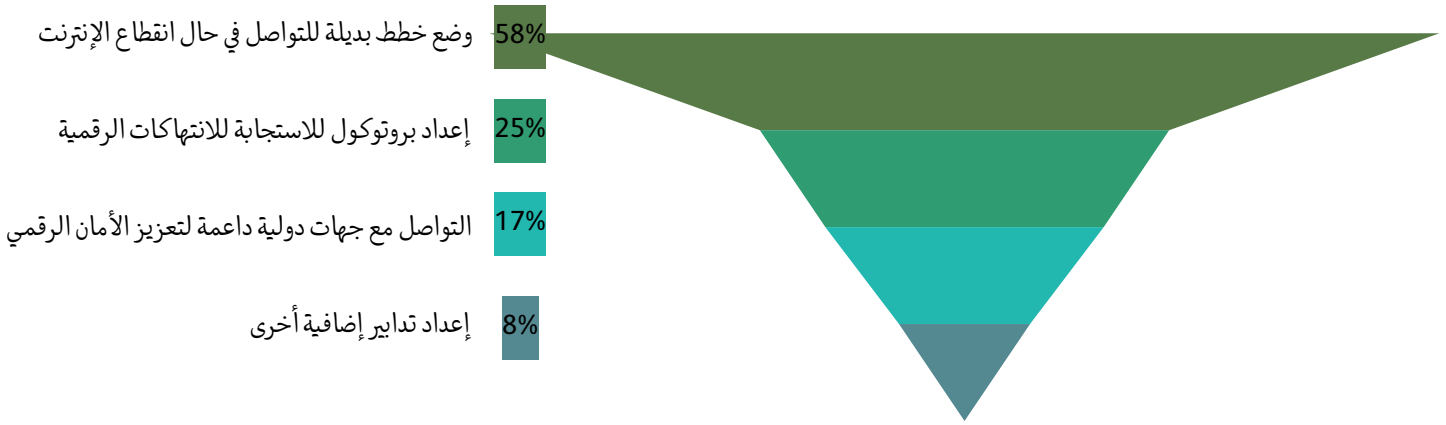
وبحسب النتائج، اتخذت المؤسسات عدة إجراءات لتعزيز الأمان الرقمي بعد 7 أكتوبر 2023، وكان الإجراء الأكثر شيوعًا هو تفعيل التحقق الثنائي لجميع الحسابات، حيث اعتمدته 50.9% من المؤسسات. تلاه مراجعة سياسات الخصوصية وحماية البيانات بنسبة حوالي 33%، مما يعكس أهمية حماية المعلومات الحساسة. كما اتخذت حوالي 26% من المؤسسات إجراءات تدريب الموظفين على كيفية التعامل مع التهديدات الرقمية والتعاون مع مؤسسات حقوقية أخرى لتعزيز الحماية. وأشارت نسبة 16.4% من المؤسسات إلى أنها لم تتخذ إجراءات محددة، بينما 9.1% منها أفادت بأنها لا تعلم بالإجراءات المتخذة. من بين التدابير الأقل شيوعًا، أبلغت 1.8% من المؤسسات عن تفعيل التحقق الثنائي لمعظم الحسابات أو العمل على إنشاء موقع إلكتروني جديد كإجراءات إضافية. تعكس هذه النتائج وعي المؤسسات بأهمية الأمان الرقمي والتوجه نحو تعزيز الحماية لمواجهة التهديدات المتزايدة.

الشكل رقم (15): الإجراءات التي اتخذتها المؤسسات التي عملت على تعزيز الأمان الرقمي إبان أكتوبر 2023



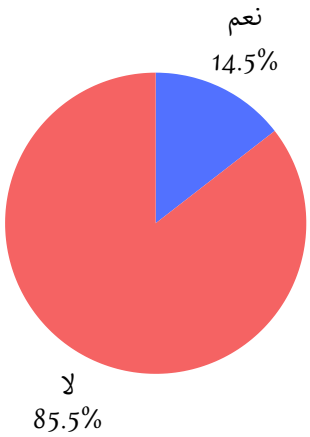
أظهرت نتائج المسح أن 80% من المؤسسات لم تطور خطة استجابة للطوارئ الرقمية بعد التصعيد الأخير، بينما 20% فقط قامت بتطوير خطة استجابة. وبالنسبة للمؤسسات التي أجابت بـ "نعم" حول تطوير خطة الاستجابة، فقد تنوعت الإجراءات المتبعة ضمن خطط الاستجابة. أشارت 58.3% من هذه المؤسسات إلى أنها قامت بوضع خطط بديلة للتواصل في حال انقطاع الإنترنت. كما ذكرت 25% من المؤسسات أنها قامت بإعداد بروتوكول للاستجابة للانتهاكات الرقمية، بينما تواصلت 16.7% من المؤسسات مع جهات دولية داعمة لتعزيز الأمان الرقمي. وأخيرًا، أفادت 8.3% من المؤسسات أنها قامت بإعداد تدابير إضافية أخرى كجزء من خطة الاستجابة. تعكس هذه الخطوات الوعي بأهمية وضع خطط طوارئ رقمية، رغم أن الغالبية العظمى لم تتخذ هذه الخطوة بعد.

الشكل رقم (16): أبرز الإجراءات التي اتبعتها المؤسسات التي طورت خطة استجابة رقمية



وأظهرت النتائج، أن الغالبية العظمى من المؤسسات، بنسبة 85.5%، لم تتلقَ أي دعم تقني أو قانوني لمواجهة التهديدات الرقمية بعد 7 أكتوبر2023، في المقابل، أفادت 14.5% من المؤسسات بأنها تلقت دعماً لمواجهة هذه التحديات. تشير هذه النتيجة إلى وجود فجوة كبيرة في الدعم المتاح للمؤسسات لمواجهة التهديدات الرقمية، مما قد يزيد من أهمية تطوير شبكات دعم فعّالة لتعزيز الأمن الرقمي للمؤسسات.

الشكل رقم (17): حجم المؤسسات التي تلقت دعماً تقنياً أو قانونياً لمواجهة التهديدات الرقمية بعد 7 أكتوبر



وعبرت 58.2% من المؤسسات أنها لاحظت زيادة في التضامن الرقمي من جهات دولية ومحلية بعد الانتهاكات، حيث تنوع هذا التضامن بين الدعم التقني (36%)، والدعم المالي لتطوير البنية التحتية الرقمية (16%)، وحملات إعلامية لنشر الوعي (80%).

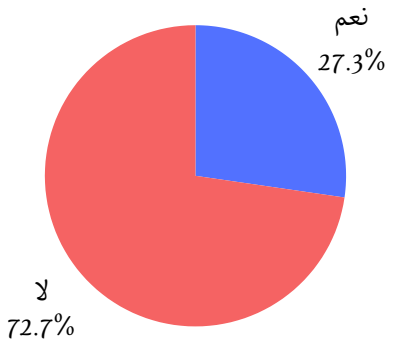
توثيق الانتهاكات الرقمية

74.5% من المؤسسات لم توثق الانتهاكات الرقمية، بينما 25.5% قامت بتوثيق الانتهاكات الرقمية، ومن بين المؤسسات التي وثقت الانتهاكات، 68.8% قامت بتوثيق داخلي فقط، و31.3% تعاونت مع منظمات حقوقية أخرى. وواجهت 56%من المؤسسات قيودًا أو صعوبات في توثيق الانتهاكات، حيث تشمل هذه القيود الرقابة على النشر (65.2%) والتهديدات المباشرة للناشطين (65.2%).

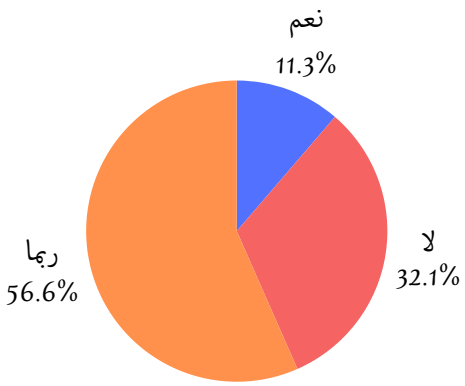
التشريعات الفلسطينية لحماية الحقوق الرقمية

تشير النتائج إلى أن غالبية مؤسسات المجتمع المدني المشاركة في المسح، بنسبة 72.7%، لا تعرف التشريعات أو السياسات المحلية المتعلقة بحماية الحقوق الرقمية في الفضاء الرقمي، في حين أن 27.3% فقط منها على علم بهذه التشريعات. أما بالنسبة لفعالية قانون الجرائم الإلكترونية في حماية مؤسسات المجتمع المدني من الانتهاكات الرقمية، فقد كان رأي المؤسسات متباينًا؛ إذ اعتبرت 56.6% من المؤسسات أنه ربما يكون فعالاً، بينما ترى 32.1% أنه غير فعال، و11.3% فقط تعتبره فعالاً.

الشكل رقم (18): الموقف حول المعرفة بالتشريعات أو السياسات المحلية المتعلقة بحماية الحقوق الرقمية في الفضاء الرقمي



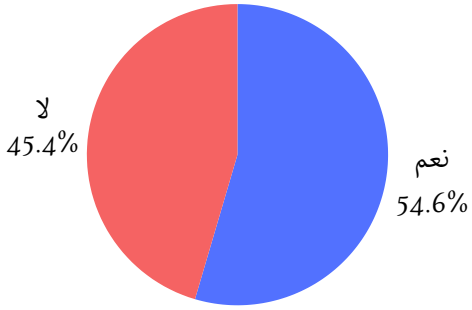
الشكل رقم (19): الموقف حول قانون الجرائم الالكتروني وحمايته لمؤسسات المجتمع المدني من الانتهاكات



وفيما يخص بجهود الحكومة الفلسطينية لحماية الفلسطينيين من الانتهاكات الرقمية، تعتقد 61.8% من المؤسسات أن الحكومة لا تبذل جهودًا كافية، في حين ترى 7.3% فقط أن هذه الجهود كافية، و30.9% لا تعلم بمدى فعالية تلك الجهود. أما عن معرفة آليات تقديم الشكاوى المحلية في حال انتهاك الحقوق الرقمية، فقد كانت النتائج متقاربة؛ حيث أفادت 50.9% من المؤسسات بأنها تعرف آليات تقديم الشكاوى، في حين أن 49.1% لا تعرف هذه الآليات.

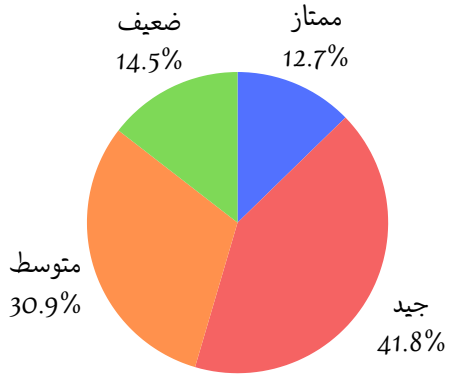
وحول التشريعات الدولية، فإن 54.5% من المؤسسات مطلعة على بعض الاتفاقيات أو القوانين الدولية التي تعزز الحقوق الرقمية وتدعم حرية الوصول إلى الإنترنت، في حين أن 45.5% منها لا تعرف هذه القوانين.

الشكل رقم (20): حجم المؤسسات ذات المعرفة فيما يتعلق بالتشريعات الدولية



وعند تقييم مستوى المعرفة بفهم "حرية الوصول إلى الإنترنت" في القوانين الدولية، اعتبرت 41.8% من المؤسسات أن معرفتها ضعيفة، بينما 30.9% وصفتها بالمتوسطة، و14.5% بالجيّدة، و12.7% فقط بالمتفوقة.

الشكل رقم (21): مستوى معرفة المؤسسات حول حرية الوصول إلى الانترنت في القوانين الدولية



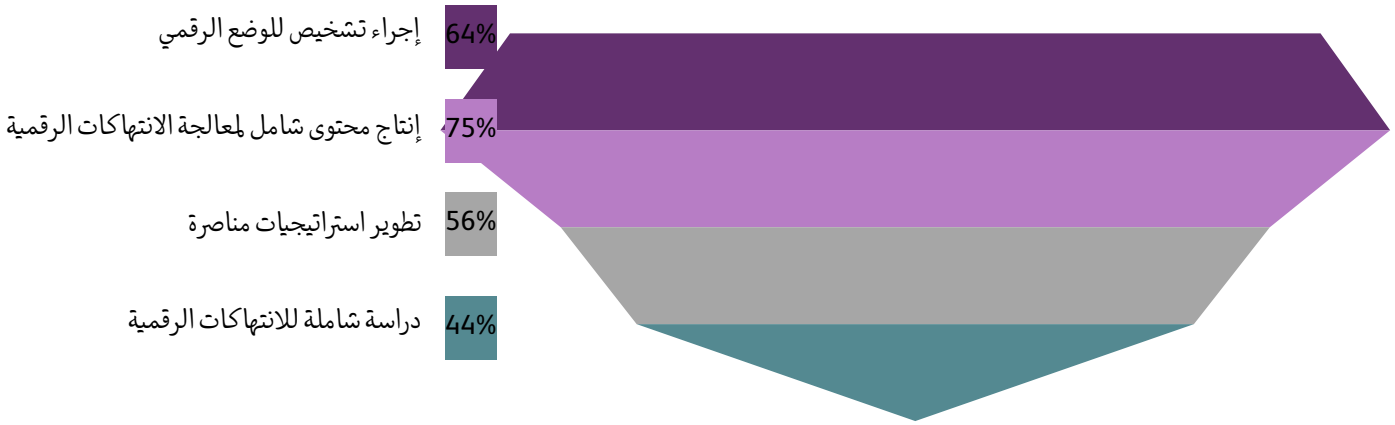
أما بالنسبة لأهم القوانين والمواثيق الدولية التي يجب على الحكومات المحلية الالتزام بها لضمان الحقوق الرقمية للفلسطينيين، فقد اعتبرت 88% من المؤسسات أن قوانين حرية الرأي والتعبير هي الأهم، تلتها قوانين حماية البيانات بنسبة 76%، ثم قوانين مكافحة التمييز الرقمي بنسبة 52%، وأخيرًا قوانين ضمان حرية الوصول إلى الإنترنت بنسبة 68%.

احتياج المؤسسات فيما يتعلق بحماية الحقوق الرقمية

67.3% من المؤسسات ترغب في تدريبات حول أساسيات الحقوق الرقمية، و63.6% من المؤسسات تطلب تدريبًا حول القوانين المحلية، في حين تحتاج 60% إلى التدريب حول القوانين الدولية، كما أن 63.6% من المؤسسات تحتاج أيضًا لتدريب حول آليات تقديم الشكاوى.

وفيما يتعلق بالأمن الرقمي، تحتاج 76.4% من المؤسسات لتدريب متخصص في الأمان الرقمي، و72.7% بحاجة إلى أدوات حماية مثل برامج مكافحة الفيروسات والتشفير، و63.6% من المؤسسات تسعى لتعزيز التعاون مع مؤسسات دولية، و49.1% ترغب في بناء شبكات دعم مشترك مع مؤسسات أخرى. وفقط 16.4% من المؤسسات أفادت بعدم الحاجة لمزيد من التدريب.
تقترح 63.6% من المؤسسات إجراء تشخيص للوضع الرقمي، بينما 74.5% توصي بإنتاج محتوى شامل لمعالجة الانتهاكات الرقمية، و56.4% من المؤسسات تقترح تطوير استراتيجيات مناصرة، و43.6% توصي بدراسة شاملة للانتهاكات الرقمية، مما يعكس حرصًا على تحليل الوضع بشكل أفضل.

الشكل رقم (22): توصيات المؤسسات لتعزيز حماية الحقوق الرقمية



أبرز الفجوات التي رصدها المسح

الجانب	نقاط الضعف/الفجوات	التأثير
البنية التحتية الرقمية	ضعف الوصول إلى التقنيات المتقدمة مثل الجيل الخامس؛ الاعتماد على البنية التحتية القديمة مثل خطوط الـ *ADSL*.	يقلل من الكفاءة ويعيق تبادل المعلومات بسرعة.
الوعي الرقمي	انخفاض الوعي بالحقوق الرقمية لدى 23.6% من المؤسسات؛ نقص كبير في برامج التدريب.	يساهم في زيادة الهشاشة أمام التهديدات الرقمية ويحد من الإجراءات الاستباقية.
تطبيق السياسات	غياب سياسات شاملة لحماية الحقوق الرقمية في 52.7% من المؤسسات.	يعرض المؤسسات لخطر الاختراقات وسوء استخدام البيانات.
توفر الموارد	قص في الموارد التقنية (74.5%) والدعم القانوني (36.4%)	يضعف قدرة المؤسسات على الاستجابة للتحديات الرقمية بفعالية.
الأمان الرقمي	اعتماد غير كافٍ على أدوات التشفير والأمان المتقدمة؛ وعي محدود بالتهديدات السيبرانية.	يزيد من خطر انتهاكات البيانات ويحد من الحماية ضد الهجمات السيبرانية المتقدمة.
التوثيق والإبلاغ	74.5% من المؤسسات لا توثق الانتهاكات الرقمية؛ قدرة محدودة على التعاون في مجال الإبلاغ.	يعيق الجهود المبذولة لمحاسبة المنتهكين والدفاع عن الحقوق الرقمية.
الدعم الدولي	اعتماد على تمويل دولي قصير الأمد؛ صعوبات في إقامة شراكات مستدامة.	يحد من التخطيط الاستراتيجي طويل الأمد والقدرة على الصمود الرقمي.
المراقبة الرقمية	المراقبة الرقمية المتكررة واستهداف المحتوى والاتصالات من قبل السلطات والمنصات.	يخلق مناخًا من الخوف والرقابة الذاتية بين المؤسسات والأفراد.
الإطار القانوني	ضعف الإطار التشريعي؛ غياب قانون شامل لحماية البيانات في فلسطين.	لا يوفر آلية موثوقة لحماية المؤسسات والأفراد.