حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

الأمان الرقمي بين الشباب الفلسطيني:

دراسة حول التهديدات والتحديات في ظل الحرب على غزة

(الضفّة الغربيّة والقدس)

آب 2024

حملة – المركز العربي لتطوير الإعلام الاجتماعي

مفهوم الأمان الرّقميّ بين الشّباب الفلسطينيّ في ظل الحرب على غزة
دراسة مَسْحيّة تحليليّة (الضفّة الغربيّة والقدس)

المؤلف: د. سعيد أبو معلا

تحرير: إيناس خطيب

تنسيق مجموعات بؤريّة: سرى أبو الرب

منسّق المشروع: مهدي كرزم

تنفيذ استطلاع: مينا انالیتکس

تصميم: أمل شوفاني

للتواصل معنا:

البريد الإلكترونيّ: info@7amleh.org

الموقع الإلكترونيّ: www.7amleh.org

الهاتف: 774020670 (0) 972+

صفحاتنا على وسائل التواصل الاجتماعيّ: **7amleh**

الفهرس

ملخّص تنفيذي

تسلّط هذه الدراسة الضوء على مشهد الأمان الرقميّ في الضفّة الغربيّة والقدس، من خلال اقتفاء تجارب الشباب الفلسطيني في الفئة العمرية من 15 إلى 30 عامًا، تأتي هذه الدراسة في مرحلة غاية في الحساسيّة والاضطراب والتحوّل، فيما حالت ظروف الحرب على قطاع غزّة من أن تشملها الدراسة. وبغية استخلاص استنتاجات ذات مصداقيّة استخدمت الدراسة طريقتيْن لجمع البيانات وهما: المجموعات البؤريّة (5 مجموعات ضمّت 35 مشاركًا/ةً)، والمسح الميدانيّ (استطلاع رأي شارك فيه 449 مستطلَعًا/ةً)، إلى جانب مراجعة الأدبيّات التي تناولت موضوعي الأمان الرقميّ والحقوق الرقميّة.

احتوت استمارة الاستطلاع على 31 سؤالًا، وُزّعت على ستّة محاور، هي: خصائص المستطلَعين/ات؛ خصائص استخدامات شبكة الإنترنت لدى المستطلَعين/ات؛ مدى معرفة "الأمان الرقميّ" ومدى إدراك المخاطر الرقميّة؛ الهجمات والاعتداءات الرقميّة ومدى التعرّض لها؛ المساءلة والتحقيق من جهات أمنيّة (إسرائيليّة، فلسطينيّة) لأسباب لها علاقة بالنشاط الرقميّ؛ أثر سياسات منصّات التواصل الاجتماعيّ على نشاط الشباب الفلسطينيّ خلال فترة الحرب على قطاع غزّة. بعد تحليل البيانات من الاستطلاع والمقابلات خلصت الدراسة إلى الآتي:

- **86% من المستطلَعين/ات يستخدمون الإنترنت في المنزل.**
- **67% من المستطلَعين/ات يقضون 7 ساعات يوميّة على الأقل باستخدام الإنترنت.**
- **يستخدم المستطلَعون/ات مجموعة كبيرة من التطبيقات والشبكات الاجتماعيّة أبرزها:"واتس اب" 95%،"فيس بوك" 91 %، "انستغرام" 78 % "تيك توك" 71 %،"تلغرام" 66.6 %.**
- **68% من المستطلَعين/ات صرّحوا أنّهم يعرفون أو سمعوا عن برامج تجسّس الأجهزة الإلكترونيّة المرتبطة بالشبكة.**
- **47% مِمَن يعرفون عن برامج التجسّس، مصدر معلوماتهم مُستمدّة من العائلة أو الأصدقاء.**
- **43% من المستطلَعين/ات لم يغيّروا كلمة المرور إطلاقًا.**
- **56% من المستطلَعين/ات يفعّلون إعدادات الأمان.**
- **37% من المستطلَعين/ات لا يصادقون بتاتًا على طلبات صداقة من أشخاص مجهولين، ومن تبقّى يصادقون بوتيرة متفاوتة.**
- **42% من المستطلَعين/ات يشاركون غالبًا أو دائمًا، صورًا وأمورًا شخصيّة عبر الشبكة.**
- **47% من المستطلَعين/ات لا يعرفون ما هي برامج الحماية.**
- **66% من المستطلَعين/ات لا يستخدمون برامج الحماية.**
- **59% من المستطلَعين/ات لا يستخدمون أيّ حماية رقميّة.**
- **43% من المستطلَعين/ات يتجاهلون رسائل من مصادر مجهولة.**
- **30% من المستطلَعين/ات يستخدمون خاصيّة تحديد المواقع.**
- **20% من المستطلَعين/ات تعرّضوا لهجوم أو اعتداء رقميّين.**

- **42%** من المستطلَعين/ات قالوا إنّهم شعروا بالخوف والقلق بعد الهجوم والاعتداء.
- **74%** من المستطلَعين/ات قالوا إنّهم تعرضوا لهجوم أو اعتداء من أفراد (55% غرباء و19% معارف).
- **30%** من المستطلَعين/ات يلجؤون لجهات مختصّة (الشرطة، خبراء رقميّون) عند التعرّض لهجوم أو اعتداء رقميّين.
- **50%** من المستطلَعين/ات تعرّضوا لهجوم او اعتداء من نوع "انتحال الشخصيّة".
- **55%** من المستطلَعين/ات تعرّضوا لهجوم أو اعتداء من نوع "التحرّش" و "الترصّد الإلكترونيّ".
- **50%** من المستطلَعين/ات تعرّضوا شخصيًّا أو يعرفون شخصًا تعرّض للمساءلة والتحقيق من السلطات الإسرائيليّة.
- **38%** من المستطلَعين/ات تعرّضوا شخصيًّا أو يعرفون شخصًا تعرّض للمساءلة والتحقيق من السلطات الأمنيّة الفلسطينيّة.
- **39%** من المستطلَعين/ات تعرّضوا لضغوطات من دوائر اجتماعيّة لحذف منشوراتهم.
- **14%** من المستطلَعين/ات تعرّضوا لضغوطات من مصادر أمنيّة إسرائيلية لحذف منشوراتهم.
- **60%** من المستطلَعين/ات قالوا إنّهم يمارسون رقابة ذاتيّة على نشاطهم الرقميّ.
- **50%** من المستطلَعين/ات قالوا إنّ سياسات التضييق على النشر خفّضت من نشاطهم الرقميّ.

وعكست النقاشات مع المجموعات البؤريّة تراجعًا في ثقة المستخدِمين للشبكة بالجهات الرسميّة (الشرطة)، واعتبار التجربة الشخصيّة في التعرّض لاعتداء أو هجوم هي مصدر التوعية الأساسيّ فيما يتعلق بالمعرفة بقضايا الأمان الرقميّ. جميع المشاركين الشبان ينظرون للشبكة على أنّها مكانٌ غير آمن، على ضوء تجربتهم الشخصيّة والمؤلمة، وهي مسألة تفرض عليهم توعية أنفسهم وعائلاتهم دون أن يعني ذلك الابتعاد عن الشبكة.

الباب الأول

مقدّمة

منذ دخول الإنترنت إلى الأراضي الفلسطينيّة المحتلّة ، فرضت إسرائيل السيطرة والرقابة على الحقوق الرقميّة الفلسطينيّة وحاربتها بشتّى الطرق. هذه الممارسات تؤكّد أنّه لا يمكن الفصل بين احتلال الأرض والاحتلال الرقميّ مثلما بيّن باحثو هذا المجال. يخوض الناشطون الفلسطينيّون في الفضاءات الرقميّة صراعًا متعدّد المستويات، على الصعيدَيْن المحلّيّ والعالميّ، فهم يواجهون ممارسات الاحتلال الإسرائيليّ وما ترتّب عليه من تقسيمات جغرافيّة معقّدة وتشظّيًا للوجود الفلسطينيّ على الأرض. كلّ هذه التحدّيات عبارة عن عمليّات تتبلور بفعل الوقائع على الأرض وفي الفضاء الرقميّ بالتوازي وفي آن واحد. أطلق الباحثون على هذا المشهد اصطلاحًا جديدًا، هو الكولونياليّة السيبرانيّة ("Cyber colonialism")، على اعتبار استحالة الفصل بين مفهومَي الكولونياليّة على الأرض والكولونياليّة في الفضاءات الرقميّة.[1]

كيفما تخضع حياة الفلسطينيّين اليومية لإجراءات الاحتلال العسكريّة والرقابة الدائمة عن طريق أحدث التقنيّات، في نقاط الرقابة العسكريّة والحواجز، فإنّ الفضاء الافتراضيّ يخضع، هو الآخر، لسياسات الرقابة الجماعيّة وباستخدام أحدث التقنيّات. ففي هذا الفضاء، تسيطر إسرائيل وتتعرّف وتراقب أيّ محتوى فلسطينيّ شخصيّ أو عموميّ أو حقوقيّ. هذا فضلًا عن تورّط منصّات التواصل الاجتماعيّ وتواطئها، إلى حدّ بعيد، في ممارسات الانتهاكات للحقوق الفلسطينيّة الرقميّة،[2] وهو الأمر الذي تعاظم بعد السابع من أكتوبر 2023.

يمرّ الشباب الفلسطينيّ منذ بدء الحرب على قطاع غزّة (أكتوبر 2023)، بمرحلة مصيريّة في كلّ ما يخصّ شبكة الإنترنت، فهم عالقون أكثر من أيّ وقت مضى، في مساحة أصبحت خطرة للغاية، بسبب تنامي سياسات القمع الرقميّ وتنامي إحساسهم بفقدان الأمان في ظلّ هذه السياسات التي تنتهك حقوقهم الرقميّة. على سبيل المثال، يتعرّض مستخدمو الشبكة لأنواع متعدّدة من الهجمات والاعتداءات الرقميّة مصدرها متطفّلون أو "هكرز"، تكون على نحو هجمات "انتحال الشخصيّة" و "التحرّش والإساءة على الإنترنت"، و "الترصّد والملاحقة الإلكترونيّة"؛ أو هجمات عبر برامج تجسّس مثل: پچاسوس؛ إلى جانب هجمات "الذباب الإلكترونيّ"، و "التصيّد الاحتياليّ"، و"البورنو الانتقاميّ". تختلف هذه الهجمات فيما بينها من حيث الفاعلين والأهداف والنتائج وإسقاطاتها على الضحايا، وهذا ما يخلق بيئة رقميّة فاقدة لأبسط مقوّمات الأمان.

1. Tawil-Souri, Helga & Aouragh, Miriyam. (2014). Intifada 3.0? Cyber colonialism and Palestinian resistance. **Arab Studies Journal**. Pp. 103-120.
2. Taha, Suhail. (2020). The Cyber Occupation of Palestine; Suppressing Digital Activism and Shrinking the Virtual Sphere. **Global Campus Arab World, Policy Briefs**. Pp. 3-4.

في دراسة أجراها مركز "حملة"[3] منذ سنوات كشفت أنّ أمان الشباب الفلسطينيّ الرقميّ يعاني من "فراغ مؤسّساتيّ مقلق"، ومع إتاحة مواقع التواصل الاجتماعيّ عملية اختراق الخصوصيّات، أدّى كلّ هذا إلى خلق تحدّيات جديدة أمام المستخدمين؛ وما كشفت عنه الدراسات آنذاك أنّ نحو 58% من الشبّان لا يعرفون شيئًا عن حقوقهم الرقميّة، وأكثر من 85% منهم بحاجة لمعرفة طرق حماية خصوصيّتهم وبياناتهم الشخصيّة، وأكثر من 93% من المستطلَعين يحتاجون لمهارات حماية رقميّة لهواتفهم المحمولة.

في المقابل، يتزايد شعور الشباب الفلسطينيّ أنّ علاقتهم مع الشبكة أصبحت راسخة ولا يمكن لها أن تتوقّف، فهي بمثابة حياة رديفة لحياتهم الأصليّة. إذ تُظهر الإحصاءات الرسميّة الفلسطينيّة الصادرة عن الجهاز المركزيّ للإحصاء الفلسطينيّ تناميا سنويًّا مضطردا في استخدام كلّ ما له علاقة ببنية وتكنولوجيا الاتّصال بشبكة الإنترنت، على نحو الخطوط الثابتة والأجهزة المحمولة الذكيّة. وتظهر الإحصاءات أنّ التوسّع في البنى التحتيّة لشبكة الاتّصالات الثابتة جاء متزامنًا مع زيادة استخدام الأُسَر والمؤسّسات لهذه الشبكة والخدمات المرتبطة بها، لا سيّما خدمة الإنترنت،[4] وهو ما يعني زيادة عدد المستخدمين المعرّضين للتهديدات والهجمات الرقميّة.

هذه الثنائية المقلقة، والتي تعمّقت في فترة الحرب على قطاع غزّة، تعزّز الحاجة لمعرفة واقع حالة الأمان الرقميّ، ومعرفة المخاطر الرقميّة على شبكة الإنترنت في تجارب الشباب الفلسطينيّين عند استخدامهم لها، وهي تجارب باتت تجسّد لحظة مقلقة في تاريخ علاقتهم بالشبكة.

ترمي هذه الدراسة إلى استخراج أدوات للعمل على تعزيز حماية الحقوق الرقميّة لدى لشباب من خلال توفير بيانات علميّة حديثة حول طبيعة وخصائص استخدام الشباب الفلسطينيّ لشبكة الإنترنت، والكشف عن طبيعة معرفة الشباب بمفاهيم الأمان الرقميّ والوعي بالمخاطر الرقميّة التي يمكن أن تواجههم، والكشف أيضا عن مدى تعرّض المستطلَعين لهجمات واعتداءات رقميّة. إلى جانب ذلك، ترمي الدراسة إلى تسليط الضوء على واقع المساءلة والتحقيق من قِبل الجهات الأمنيّة لأسباب لها علاقة بالنشاط الرقميّ، وأثر سياسات المنصّات على نشاط الشباب الفلسطينيّ منذ بدء الحرب على قطاع غزّة في أكتوبر 2023.

علاوة على ذلك، تهدف الدراسة إلى التعرّف على التحدّيات والتهديدات والفرص الأساسيّة المتاحة للشباب الفلسطينيّ في الضفّة الغربيّة والقدس الشرقيّة فيما يتعلّق بحماية حقوقهم الرقميّة، تمكينهم والمؤسسات ذات الصلة بالتوعية بشأن الأمان الرقميّ، أملا بالإسهام في تعزيز حماية الحقوق الرقميّة، الانخراط في المناصرة الاستراتيجيّة، ومعالجة الانتهاكات في مجال السلامة والأمن الرقميّ.

3. مركز حملة. (2017، أيّار). **مفهوم الأمان الرقميّ بين الشباب الفلسطينيّين، دراسة مسحيّة**.

4. الجهاز المركزيّ للإحصاء الفلسطينيّ، ووزارة الاتّصالات وتكنولوجيا المعلومات. **بيان معلوماتيّ مشترك**. تاريخ الوصول: 16-3-2024.

الباب الثاني

مسح الأدبيّات

شبكة الإنترنت وولادة الحقوق الرقميّة

منذ بدايات ظهور شبكة الإنترنت وانتشارها واتّساع نطاق استخداماتها، تصاعد الجدل حول مدى وآلية تأثير تمدّد مجتمع المعلوماتيّة، وانبثق جرّاء هذا الجدل آراء متباينة ورؤى مختلفة حول مستقبل الاتّجاهات والنزعات ("Trends") للمجتمع المعلوماتيّ على الشبكات.[5] في هذا الصدد، انقسم الباحثون والخبراء إلى فرق مختلفة، فثمّة المبشّرون بالتغيير الرقميّ، وهم أصحاب النظرة الأكثر تفاؤلاً بشأن إمكانيّات شبكة الإنترنت. و رأى هؤلاء أنّ تطوّر شبكة الإنترنت سيكون له تأثير ملحوظ في تقليص الفجوة المعلوماتيّة بين فئات المجتمع، وسيعمل على الحدّ من الفوارق الطبقيّة التقليديّة في الحقّ بمنالية المعلومات. وعلى الطرف النقيض، ثمّة فريق ينظر بعين تشاؤميّة وسوداويّة إلى واقع تطوّر التكنولوجيا الرقميّة لأنّها تعمل على استنساخ التعقيدات الطبقيّة الاجتماعيّة والسياسيّة القائمة على أرض الواقع، وتعيد توظيفها على الشبكة ممّا يخلق نوعًا جديدًا من أنواع اللامساواة، وهو التمييز الرقميّ والمعلوماتيّ. بحسب الفريق الثاني يفشل النشاط الاجتماعيّ والسياسيّ عبر شبكة الإنترنت في كثير من الأحيان في دمج الفئات المهمّشة في المجتمع، أو تلك الفئات التي ليس لديها ميول سياسيّ أو رغبة في النشاط السياسيّ والاجتماعيّ.[6] ومن وجهة نظر أكثر اعتدالاً وموضوعية، ودون المبالغة في التفاؤل أو التشاؤم على حدّ سواء، فإنّه من الطبيعيّ القول إنّ التكنولوجيا الرقميّة خلقت فضاءً يمكنه التأقلم مع النظم الاجتماعيّة والسياسيّة القائمة والتأثّر بها. بيد أنّها، وبالتوازي، تعمل على تغيير القوالب السياسيّة الاعتيادية والتقليدية، بواسطة إحداث تحوّل في توازن المصادر المعرفيّة في المؤسّسات السياسيّة، فعلى سبيل المثال، عملت على تقليص كلفة الوصول للمعلومات وجمعها. هذا التحوّل كان لصالح التجمّعات السياسيّة الصغيرة أو المهمّشة، والنشطاء الأكثر هشاشة. علاوة على ذلك، عملت التكنولوجيا الرقميّة على استحداث أساليب حياة واهتمامات جديدة وغير تقليديّة في المجتمعات، وأحدثت ثورة تاريخيّة في اقتصاد المعرفة والمعلوماتيّة، حيث عملت على تحويل توازن الموارد من الاستثمار في الأراضي ورأس المال نحو الاستثمار في المهارات والخبرات والمعرفة المعلوماتيّة الرقميّة.[7]

مع انتشار الإنترنت حول العالم، أصبح مفهوم السياسة الرقميّة مجالًا ذا إمكانيّات يمكن استغلالها في تعزيز الديمقراطيّات الوطنيّة التي تكافح بغية تمكين نظمها السياسيّة. وأسهم انتشار الإنترنت في المجتمعات المدنيّة في تعزيز العمليّة الديمقراطيّة من خلال تحسين ميكانيزمات التواصل وتدفّق المعلومات.[8] ومع

5. Norris, Pippa. (2001). "Understanding the Digital Divide." In Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide. Pp., 26, 235-238. Cambridge University Press.

6. Ibid

7. Norris, Pippa. (2001). **Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide**. Pp. 26, 235-238. Cambridge University Press.

8. Ibid, pp. 239-240.

اتّضاح الأثر البالغ للتطوّر الرقميّ في التحوّلات الاجتماعيّة والسياسيّة والاقتصاديّة، كان لا بدّ أن يصاحب هذا التطوّر جدل فكريّ وفلسفيّ حول علاقة المستخدمين بهذا الفضاء المولود حديثًا، والذي رغم ما حمله من تغيير وأثر إيجابيّين، إلّا أنّه كشف عن تحدّيات كثيرة تتّسع بالتوازي مع نموّ المجتمع الرقميّ وتغلغل التكنولوجيا الرقميّة العميق في النشاط الإنتاجيّ والحياة اليوميّة للمستخدِمين. في سياق الحديث عن النشاط السياسيّ والاجتماعيّ في الفضاءات الرقميّة، فإنّه لا بدّ من القول إنّ انتشار التكنولوجيا الرقميّة لم يعمل على استحداث أنماط جديدة للمشاركة والفعل السياسيّ والاجتماعيّ فحسب، إنّما فجّر نقاشًا جديدًا يتعلّق بحقوق المستخدمين السياسيّة والمدنيّة في إطار علاقتهم بهذا الوسيط الجديد. وبدا واضحًا أنّ الثورة التي أحدثتها التكنولوجيا الرقميّة غيّرت كلّ المفاهيم والأنظمة التقليديّة، بما فيها الخطاب التقليديّ لحقوق الإنسان، ممّا أدّى إلى انبثاق تصنيفات ومفاهيم جديدة متعلّقة بحقوق الإنسان وظهور مصطلح الحقوق الرقميّة.[9]

ترى كاي ماثيسين أنّ ثمّة حاجة ماسّة لبحث كيفيّة انعكاس مفاهيم حقوق الإنسان وتحقيق العدالة في البيئات الرقميّة بعد أن غيّرت التكنولوجيا الرقميّة، وإلى الأبد، طُرق ووسائل التعلّم والعمل والتواصل.[10] وترى ماثيسين أنّ ثمّة ضرورة ملحّة لإعلان حقوق الإنسان الرقميّة، على غرار الإعلان العالميّ لحقوق الإنسان. إلى جانب ذلك، ترى ماثيسين أنّه لا بدّ من البناء على المواثيق والمعاهدات المتعلّقة بحقوق الإنسان ومراجعتها ودراستها في ضوء التطوّر التكنولوجيّ لمعرفة آليّة تطبيقها في الفضاءات الرقميّة، لأنّ التطوّر الرقميّ خلق بيئة ذات خصوصيّة تختلف عمّا نعيشه في أرض الواقع.[11]

وفي خضّم التطوّر المتسارع لتكنولوجيا البيئات الرقميّة، بدأت الأمم المتّحدة بالتحرّك لضمان احترام حقوق الإنسان في هذه البيئات، إذ أصدرت تعليقات عامّة متعلّقة بالإعلان العالميّ لحقوق الإنسان من أجل إضافة بنود للتخصيص والتوضيح في سياق حقوق معيّنة. فعلى سبيل المثال، أصدرت لجنة حقوق الإنسان عام 2011 التعليق العامّ رقم (34) حول المادّة (19) من الإعلان العالميّ لحقوق الإنسان والمتعلّقة بالحقّ في حريّة التعبير وحريّة الوصول إلى منالّيّة المعلومات واستقبالها. فجاء التعليق العامّ رقم (34) ليحدّد نوع الوسائل التي من حقّ الناس استخدامها للتعبير والوصول للمعلومات؛ وتشمل اللغة الشفويّة والمكتوبة ولغة الإشارة والتعبير غير اللفظيّ مثل الصور والموادّ الفنيّة. وتشمل وسائل التعبير مثل الكتب والصحف والنشرات والملصقات واللافتات والمذكّرات القانونيّة. كما تشمل جميع أشكال التعبير السمعيّ والبصريّ، ووسائل التعبير الإلكترونيّة والمعتمّدة على الإنترنت كذلك.[12] ويحدّد التعليق العامّ على الحقّ في الخصوصيّة -الإعلان العالميّ لحقوق الإنسان مادّة (17)- أنّ جمع المعلومات والبيانات الخاصّة والاحتفاظ بها على أجهزة الحاسوب، أو في البنوك المعلوماتيّة أو على أيّة أجهزة أخرى، سواء أكان من قبل السلطات العامة أم الأفراد والجهات الخاصّة، لا بد وأن يُنفّذ بموجب القانون.[13] وعلى الرغم من أنّ هذه التعليقات العامّة تعتبر مثالً لمحاولات تأقلم الاتّفاقيّات والمواثيق الدوليّة لضمان تطبيق

9. Borjigin, Namulun. (2023). Systemic Dilemmas and Practical Responses of Digital Human Rights Theory in the Context of Smart Society: A Literature Review. **Advances in Education, Humanities and Social Science Research**, 5(1). P. 461.

10. Mathiesen, Kay. (2014). Human Rights for the Digital Age. **Journal of Mass Media Ethics**, 29(1). Pp. 2–18.

11. Ibid, p. 7.

12. UN Human Rights Committee (UNHRC). (2011, September 12). General comment no. 34, Article 19: **Freedoms of opinion and expression**. **CCPR/C/GC/34**. Retrieved February 2, 2023

13. UN Human Rights Committee (UNHRC). (1988, April 8). **CCPR general comment no. 16: Article 17** (right to privacy). **The right to respect of privacy, family, home and correspondence, and protection of honour and reputation**. Retrieved February 2, 2023

حقوق الإنسان المتعارف عليها في البيئات الرقميّة، غير أنّ تعقيدات التكنولوجيا الرقميّة وخصوصيّة البيئة الرقميّة وسرعة تطوّرها تضع هذه المحاولات موضع القصور في كثير من الأحيان، وتجعلها غير قادرة على مواكبة التقدّم الحثيث والتغيّر المستمرّ الذي أصبح من سمات البيئة الرقميّة.

ما زال سؤال تأثير هذه التغيّرات العميقة والمستمرّة في البيئات الرقميّة والافتراضيّة على الحقوق الأساسيّة من حقوق الإنسان؛ كالحقّ في الخصوصيّة والحقّ في حريّة التعبير، سؤالًا مفتوحًا. ففي حين أنّ شبكة الإنترنت وتكنولوجيا الاتّصال والتواصل المرتبطة بها قد خلقت فرصًا ومجالات تعزّز حقوق الإنسان الأساسية، كالحقّ في التعبير، إلّا أنّها، وبالتوازي، فرضت واقعًا جديدًا من التحدّيات والمخاطر والتهديدات للحقوق الأساسيّة ذاتها، وفرضت واقعًا جديدًا على علاقة هذه الحقوق بقضايا مختلفة مثل مفهوم الشفافيّة. يشير تقرير "الخصوصيّة وحريّة التعبير والشفافيّة" الصادر عن منظّمة اليونيسكو عام 2016، إلى أنّ الحقّ في الخصوصيّة الذي يعرّفه التقرير "حقّ المستخدمين والأفراد في الحفاظ على خصوصيّة معلوماتهم وبياناتهم على الشبكة" يتعرّض إلى انتهاكات مستمرّة من عدّة جهات. فمن ناحية، ثمّة تزايد ملحوظ في توظيف تكنولوجيا اختراق الخصوصيّة ("Privacy-invading technologies") التي تعمل على تقويض الحدود المتعارف عليها،[14] حدود تبلورت في زمان ما قبل العصر الرقميّ بواسطة مفاهيم وأدوات كلاسيكيّة، منها على سبيل المثال، القانون والأعراف الأخلاقيّة والاجتماعيّة والحواجز المادّيّة والتقنيّة والحواجز الجغرافية؛ ممّا أدّى إلى انتهاكات حدود خصوصيّة المستخدمين على نطاق عالميّ. ومن ناحية أخرى فإنه بسبب تصاعد اقتصاد المعلوماتيّة فقد أصبح التحكّم ببيانات المستخدمين وخصوصيّاتهم موضوعا في غاية الحساسيّة، ومن شأنه أن يمسّ بكرامة الأفراد واستقلاليّتهم وحريّتهم.[15]

يسلّط التقرير الضوء على قضيّة أخرى هامّة متعلّقة بالاستثمار في حقّ حريّة التعبير وإساءة استخدام هذا الحقّ. فقد أدّت رغبة منصّات التواصل المختلفة من الاستفادة القصوى من بيانات المستخدمين إلى توظيف تقنيّات تتيح سبلًا كثيرة للتعبير، تمكّن الأفراد من الوصول إلى معلومات أكثر ومشاركتها على مستوى عالميّ. إلّا أنّ إساءة استخدام هذا الحقّ الأساسيّ أدّى ويؤدّي إلى انتهاك حقوق الآخرين، على سبيل المثال؛ حملات التشويه والتنمّر الإلكترونيّ والتحرّش والمضايقات وخطاب الكراهية، إلخ.[16]

ومن الممارسات الخطيرة التي تهدّد الحقّ في الخصوصيّة والحقّ في حريّة التعبير على حدّ سواء؛ هي الرقابة الجماعيّة ("Mass surveillance") التي تمارسها الحكومات والأنظمة على الأفراد. وهنا تتقاطع مصالح شبكات التواصل واقتصاد المعلوماتيّة مع مصالح الحكومات، ففي حين تستثمر الأولى في بيانات المستخدمين واستغلالها بطرق بعيدة عن الشفافيّة والوضوح في كثير من الأحيان، تسعى الأخرى إلى توظيف تطوّر تكنولوجيا الشبكات والمعلوماتيّة لفرض الرقابة على المحتوى المعارض وتقييده.[17]

14. (UNESCO). "Privacy, Free Expression and Transparency: Redefining Their New Boundaries in the Digital Age." *UNESDOC Digital Library*. United Nations Educational, Scientific and Cultural Organization (UNESCO), 2016. **https://unesdoc.unesco.org/ark:/48223/pf0000246610**

15. Cannataci, J. A., Zhao, B., Torres Vives, G., Monteleone, S., Bonnici, J. M., & Moyakine, E. (2016). **Privacy, free expression and transparency: redefining their new boundaries in the digital age**. Unesco Publishing.

16. Ibid, p. 7.

17. Ibid, p. 8.

الجانب المظلم لشبكات التواصل الاجتماعيّ: القمع الرقميّ والمعلومات المضلّلة والتعدّي على الأفراد

إذا كان ظهور شبكة الإنترنت قد أحدث ثورة غير مسبوقة في عالم المعلوماتيّة، فيمكننا القول إنّ ظهور شبكات التواصل الاجتماعيّ وضع علامة فارقة في تاريخ شبكة الإنترنت. إذ أتاح إمكانيات غير مسبوقة في عالم التواصل، لا سيّما لفئات عمريّة لم تحظ سابقًا بفرصة المشاركة السياسيّة أو المدنيّة في إطار النظم التقليديّة، ألا وهي فئة الشباب. لقد خلقت شبكات التواصل الاجتماعيّ فضاءات عموميّة بديلة مثلما اصطلح عليه الباحثون أعادت هذه الفضاءات صياغة أنماط مشاركة الشباب في الفضاءات المدنيّة والسياسيّة اليوميّة. غير أنّ دراسة مجال مشاركة الشباب لا يزال في طور الصيرورة، خاصّة في ظلّ تحدّيات كثيرة متعلّقة بتنوّع المجتمعات على شبكات التواصل الاجتماعيّ واختلاف تجاربها تبعًا للتوزيع الجغرافيّ والثقافيّ والاجتماعيّ.[18] ففي حين أنّ التجارب الوليدة وسط المجتمعات التي تتّسم بالديمقراطية تبدو واعدة، فثمّة تجارب أخرى ناشئة في نظم سياسيّة واجتماعيّة غير ديمقراطيّة أو قمعيّة تحمل في طيّاتها الكثير من الصعوبات والمآزق.

فبينما تتيح الفضاءات الرقميّة إمكانيّات المشاركة للشباب، تُفرض الرقابة على نشاط الأفراد والمحتوى المنشور، إلى جانب ممارسات أخرى من القمع الرقميّ. وبكلمات أخرى، تخلق شبكات التواصل الاجتماعيّ فرصة للحراك الاجتماعيّ والسياسيّ، وبالتوازي، تُقدّم أدوات من شأنها أن تعزّز من قدرة النخبة المسيطرة على رقابة جماعيّة ذات كفاءة عالية.[19] يعتبر مصطلح "القمع الرقميّ" مصطلحًا حديث الظهور، واستخدامه آخذ في ازدياد، رغم الاختلاف حول معناه الدقيق بين الباحثين. على العموم، يشار بهذا المصطلح إلى الممارسات الموجّهة ضدّ الأفراد لتقويض نشاطهم السياسيّ والاجتماعيّ عبر الشبكات. يشمل هذا المصطلح الممارسات القمعيّة التقليديّة ضدّ النشطاء الرقميّين، الاعتقال والملاحقة والمضايقات الشخصيّة وصولًا إلى العنف الجسديّ على سبيل المثال؛ ويشمل الممارسات القمعيّة المستحدثة والمرتبطة بالبيئة الرقميّة، الرقابة الرقميّة على سبيل المثال؛ ويشمل تطوير وتوظيف استراتيجيّات تكنولوجيا المعلومات المصمّمة للحدّ والتقليص من النشاط الرقميّ المعارض.[20]

تكمن أهميّة هذا النقاش وحساسيّته في مكانة شبكات التواصل الاجتماعيّ لدى الشباب، فقد أصبحت ركنًا مركزيا في حياتهم اليوميّة العاديّة. فعلى سبيل المثال، وبحسب دراسة إحصائيّة أجراها مركز الإحصاء الفلسطينيّ في عام 2022، فإنّ غالبيّة الشباب الفلسطينيّ من الفئة العمريّة 18-29، وبنسبة 95% يستخدمون الإنترنت، و89% من الشباب يمتلكون هاتفًا ذكيًّا. عمومًا، يتمحور نشاط المستخدمين على شبكات التواصل الاجتماعيّ حول الخدمات التفاعليّة، والمحتوى المُعدّ من قبل المستخدمين، والمجموعات، إلخ. غير أنّه لا يمكن عزل هذا النشاط عن الجانب المظلم والخفيّ من شبكات التواصل الاجتماعيّ الذي يمكن توصيفه بأنّه مجموعة من الظواهر والسلوكيّات السلبيّة المرتبطة باستخدامات تكنولوجيا المعلومات، منها على سبيل المثال تضاعف خطر التعرّض للمعلومات المضلّلة والشائعات

18. Lee, Ashley. (2018). Invisible Networked Publics and Hidden Contention: Youth Activism and Social Media Tactics under Repression. **New Media & Society**, 20(11). P. 4096.

19. Ibid, p. 4097.

20. Earl, Jennifer, Thomas v. Maher, & Pan, Jennifer. (2022). The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review. **Science Advances**, 8 (10). Pp. 1–15.

والدعاية الكاذبة، والتنمّر الإلكترونيّ وخطاب الكراهية والتحرّش. هذه الاستخدامات والسلوكيات هي انتهاك واضح لرفاهية وحقوق الأفراد والمنظّمات والمجتمعات.[21]

الشباب الفلسطينيّ على الشبكات: الصراع على الوجود الرقميّ

لقد أدخلت شبكة الإنترنت تحوّلات ثقافيّة وسياسيّة واقتصاديّة ذات طابع خاصّ لا سيّما في السياق الفلسطينيّ، نظرًا لتاريخ الاحتلال الطويل والنضال الذي يخوضه الشعب الفلسطينيّ منذ النكبة عام 1948، وتحديدًا فيما يتعلّق بالصراع على الحق في الرواية. كانت بدايات حراك الفلسطينيّين السياسيّ والمدنيّ والاجتماعيّ على شبكة الإنترنت متزامنة مع اندلاع الانتفاضة الثانية (28 سبتمبر/أيلول 2000).[22] وقد استغلّ الفلسطينيّون، آنذاك، الإمكانيّات التي أتاحتها شبكة الإنترنت لإيصال صوتهم للعالم والتواصل فيما بينهم، خاصّة في ظلّ الحصار المفروض من قبل الاحتلال. ومنذ دخول الفلسطينيّين إلى العالم الافتراضيّ، مارس الاحتلال ضغوطًا وتضييقات وانتهاكات لحقوق الفلسطينيّين الرقميّة.[23] ومنذ ذلك الحين تحوّل الفضاء الرقميّ إلى ساحة صراع سياسيّ وفكريّ. شهدت السنوات الأخيرة جهودًا غير مسبوقة تبذلها الحكومات الإسرائيليّة لتعزيز "الهَسْباراة" الإسرائيليّة،[24] فهي تشارك في حملات الدعاية المباشرة بواسطة مساعيها الرسميّة عند مالكي ومديري شبكات التواصل الاجتماعيّ مثل شبكة إكس (تويتر سابقًا) وغيرها. تدأب وتواظب السلطات الإسرائيليّة على تقديم طلبات رسميّة لحذف المحتوى الفلسطينيّ أو حجبه أو تضييق نطاق وصوله. علاوة على ذلك، تمتاز حسابات جيش الاحتلال الإسرائيليّ بنشاطها على مواقع التواصل الاجتماعيّ، حيث ينشر القادة بيانات عسكريّة وإعلانات عن حملات عسكريّة في بعض الأحيان، وهو ما يمكن وصفه أو تسميته بـ"العسكرة الرقميّة".[25]

يرافق الصراع على الحقّ في الوجود في الفضاءات الرقميّة تصاعد خطاب الحقوق الرقميّة، وباتت المطالبة بالحقوق الرقميّة للفلسطينيّين جزءًا من حملات المناصرة والنضال على شبكات التواصل. وبطبيعة الحال، فإنّ هذه الحملات صارت جزءًا من حراك عالميّ يطالب بالاعتراف بالحقوق الرقميّة وحمايتها. يمكن اعتبار خصوصيّة السياق الفلسطينيّ وحساسيّته حالة نادرة تصلُح لدراسة علاقات القوى والسلطة والحريّات السياسيّة وتجلّيّات هذه العلاقات في الفضاء الرقميّ.[26]

21. Norri-Sederholm, Teija, Riikonen, Reetta, Moilanen, Panu & Aki-Mauri, Huhtinen. (2020). Young People and the Dark Side of Social Media: Possible Threats to National Security. In Thaddeus, Eze, Lee, Speakman & Cyril, Onwubiko (Eds.). **Proceedings of the 19th European Conference on Cyber Warfare** (pp. 278-283). ACPI.

22. Yin, J. K.H. (2009). The Electronic Intifa`da: The Palestinian Online Resistance in the 2nd Intifada. **Journal of Information Warfare**, 8(1). P. 1.

23. Khoury-Machool, Makram. (2007). Palestinian Youth and Political Activism: The Emerging Internet Culture and New Modes of Resistance. **Policy Futures in Education**, 5(1). Pp. 17–36.

24. Aouragh, Miriyam. (2016). Hasbara 2.0: Israel's Public Diplomacy in the Digital Age. **Middle East Critique**, 25(3). Pp. 271–72.

"الهَسْباراة" الإسرائيليّة، يشير هذا المصطلح إلى حملات دعائيّة منظّمة وممنهجة تخصّص لها المؤسّسة الإسرائيليّة الرسميّة المصادر والموارد اللازمة لإعداد وتدريب مناصرين ومروّجين للدعاية الإسرائيليّة.

25. Cristiano, Fabio. (2019). **Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory**. In louin-Genest G., Doran M.C., and Paquerot, S. (Eds.). **Human Rights as Battlefields** (pp. 249-269). Ottawa, ON, Canada: Human Rights Interventions.

26. Ibid, p. 257.

لعلّ إحدى أبرز تحدّيات حقوق الفلسطينيّين الرقميّة، هي عدم سيطرة الفلسطينيّين على البنية التحتيّة لشبكات الاتّصالات، حيث لا تزال نُظُم الاتّصالات كافّة خاضعة لسيطرة الاحتلال الإسرائيليّ، وبالتالي فإنّ السلطة الفلسطينيّة لا تتمتّع إلّا بقدر ضئيل من السيادة على الفضاء الرقميّ، رغم ما ورد في اتفاقيّة أوسلو الثانية عام 1995، من تأكيد على حقّ الفلسطينيّين في التمتّع باستقلاليّة قطاع تكنولوجيا الاتّصالات، والتمتّع بحكم ذاتيّ على البنى التحتيّة، بمعنى أنّ من حقّ الفلسطينيّين إنشاء وتشغيل نظم اتّصالات منفصلة ومستقلّة مع بنى تحتيّة تشمل شبكات الاتّصالات وشبكة التلفزيون وشبكة الراديو. إلّا أنّ إسرائيل، وباستمرار، تمارس انتهاكًا صارخًا لبنود هذه الاتّفاقيّة وتفرض سيطرتها على البنى التحتيّة لنظام الاتّصالات في فلسطين. إنّ عجز الفلسطينيّين في التحكّم بالبنى التحتيّة للاتّصالات وعدم تمتّعهم بشبكة اتّصالات مستقلّة ومنفصلة ولّد عقبة كبيرة في تحقيق الأمان الرقميّ للفلسطينيّين.[27]

علاوة على ذلك وبالتوازي، يخضع الناشطون والمحتوى عند الفلسطينيّين لرقابة سلطات الاحتلال الإسرائيليّ ممّا يعرّضهم للمساءلة القانونيّة والملاحقة والاعتقال والعقاب. تستثمر سلطات الاحتلال الإسرائيليّ في تطوير تقنيّات التتبّع والرقابة الآليّة بواسطة تطوير أنظمة خوارزميّات شبكات التواصل الاجتماعيّ التي تعمل على فحص مضامين المحتوى الفلسطينيّ عليها.[28] تركّز هذه الخوارزميّات على تدقيق منشورات الحالة والتعليقات والصور، وذلك بغية تحديد المحتوى الذي يخالف السياسات الإسرائيليّة، أو المحتوى الذي يقع ضمن ما تعتبره السلطات الإسرائيليّة تحريضًا على العنف.[29]

27. Cristiano, Fabio. (2020). **Palestine: Whose Cyber Security without Cyber Sovereignty**? In Romaniuk S. N. and Manjikian M. (Eds.). **Routledge Companion to Global Cyber-Security Strategy, Basingstoke: Palgrave Macmillan** (pp. 418-426).

28. Fatafta, Marwa & Nashif, Nadim. (2017, October 23). Surveillance of Palestinians and the Fight for Digital Rights. **Al-Shabaka Policy Brief**.

29. Cristiano, Fabio. (2019). Ibid, pp. 249-268.

الباب الثالث

منهجيّة الدراسة

أدوات البحث:

تسعى هذه الدراسة إلى الكشف والاستقصاء عن حالة الأمان الرقميّ في تجربة الشباب الفلسطينيّ عبر شبكة الإنترنت، وذلك بغية اعتماد النتائج من أجل تعزيز حماية الحقوق الرقميّة للشباب الفلسطينيّ في الضفّة الغربيّة والقدس الشرقيّة، فيما تعذّر إجراء البحث في قطاع غزّة بسبب ظروف الحرب عليه، وقد استخدم البحث لهذا الغرض آليات البحث الكميّ والكيفيّ من أجل الوصول لنتائج شاملة وفق أهداف البحث.

ارتكز البحث إلى إطار نظريّ يضمن مراجعة للأدبيّات العلميّة، واستخدم أداتين بحثيّتين لجمع البيانات وقياسها لإدراك واقع المخاطر الرقميّة في الضفّة الغربية والقدس. الأداة الأولى عبارة عن استمارة أسئلة/ مسح ميدانيّ؛ أمّا الأداة الثانية فكانت عبارة عن لقاءات مع مجموعات بؤريّة من منطقتيْن جغرافيّتيْن هما الضفّة الغربيّة والقدس.

المسح الميدانيّ:

عبارة عن استطلاع رأي هاتفيّ، نفّذته شركة مينا أناليتكس المتخصّصة بالأبحاث والدراسات المسحيّة مطلع شهر فبراير- شباط 2024. شملت عيّنة المسح (449) مشاركًا من مناطق مختلفة في الضفّة الغربيّة والقدس المحتلّة، نظرًا لظروف الحرب استحال علينا أن نشمل قطاع غزّة في عيّنة المسح. أُستخدمت لأغراض المسح الميدانيّ استمارة بحثيّة، فيها 31 سؤالًا موزّعًا على خمسة محاور:

- **أوّلا: خصائص المستطلَعين وبياناتهم الشخصيّة، مكان السكن والنوع الاجتماعيّ، والتحصيل العلميّ.**
- **ثانيا: طبيعة وخصائص استخدام شبكة الإنترنت، من حيث مكان الاتّصال بالإنترنت وعدد ساعات الاستخدام، وطبيعة الحسابات على المنصّات.**
- **ثالثا: مقدار الوعي والمعرفة بالأمان الرقميّ والمخاطر الرقميّة، طبيعة التهديدات التي تعرّض لها المشاركون، وكيف كان تصرّفهم حيالها.**
- **رابعا: مدى تعرّض المشاركين للمساءلة والتحقيق من قِبل جهات أمنيّة أو اجتماعيّة على خلفيّة ما يُنشَر على المنصّات.**
- **خامسا: أثر سياسات المنصّات على نشاط الشباب الفلسطينيّ الرقميّ منذ بدء الحرب على قطاع غزّة.**

مجموعات التركيز:

لقد استخدمت الدراسة مجموعات التركيز (البؤريّة) كأداة ثانية من أجل تعزيز وتعميق فهم نتائج الدراسة الكمّيّة، ولأجل هذا الغرض عقدت خمسة لقاءات مع المجموعات البؤريّة، وذلك على مدار شهري فبراير/شباط ومارس/آذار 2024. نُظّمت ثلاث مجموعات عبر منصّة زووم، ونُظّم لقاءان وُجاهيّان للطلبة في المراحل الثانوية. عُقد اللقاء الأوّل في مركز تامر للتعليم المجتمعيّ في مدينة رام الله، والثاني في أحد مقاهي مدينة القدس.

الجدول (1): تفاصيل المجموعات البؤريّة

	تعريف المجموعة	المنطقة	عدد المشاركين	النوع الاجتماعيّ		طبيعة إجراء اللقاء
				إناث	ذكور	
1	طلبة جامعات ونشطاء	شمال الضفّة الغربيّة (جنين، نابلس، طولكرم)	6	5 إناث	1 ذكور	زووم
2	طلبة جامعات ونشطاء	وسط وجنوب الضفّة والقدس	7	6 إناث	1 ذكور	زووم
3	طلبة مراحل ثانويّة	الضفّة الغربيّة (رام الله)	11	8 إناث	3 ذكور	وجاهيّ/ رام الله
4	طلبة مراحل ثانويّة	القدس	5	3 إناث	2 ذكور	وجاهيّ/ القدس
5	نشطاء وعاملو مؤسّسات مهتمّة في الحقوق الرقميّة	الضفّة الغربيّة والقدس	6	1 إناث	5 ذكور	زووم
	المجموع		**35**	**23**	**12**	

أُختيرت الأسئلة التي أسّست النقاشات في المجموعات البؤريّة بالاستناد على أبرز النتائج التي عكسها المسح الميدانيّ. تضمّنت محاور النقاش داخل مجموعة "طلبة المراحل الثانويّة" البؤريّة: علاقة الطلبة بالشبكة العنكبوتيّة؛ طبيعة المنصّات التي يستخدمونها وينشطون فيها؛ أهدافهم من استخدام الإنترنت؛ طبيعة التهديدات الرقميّة التي يتعرّضون لها؛ مدى شعورهم بالأمان أثناء نشاطهم في المنصّات الرقميّة؛ مدى توفّر إجراءات الأمان في بيت العائلة؛ طبيعة استخدام الإنترنت منذ العدوان على قطاع غزّة؛ التدريبات التي تلقّوها حول الحقوق الرقميّة والأمان الرقميّ؛ نظرتهم لمستقبل استخدام الشبكة.

تناولت محاور النقاش داخل مجموعة "طلبة الجامعات": طبيعة العلاقة بشبكة الإنترنت ومراحل تطوّرها؛ التجارب التي مرّ بها الطلبة في علاقتهم مع الشبكة؛ المنصّات التي يستخدمونها ودوافعهم من ذلك؛ طبيعة التهديدات التي تعرّضوا ويتعرّضون لها؛ التدريبات التي تلقّوها لرفع مستوى معرفتهم في الأمان الرقميّ؛ رؤيتهم للحلول المرتبطة بتراجع حالة الأمان الرقميّ؛ رؤيتهم لمستقبل استخدام شبكة الإنترنت في ظلّ تنامي المخاطر والتهديدات الرقميّة.

أمّا محاور النقاش التي تناولناها داخل مجموعة "المؤسّسات والنشطاء" فتكوّنت من ثلاثة محاور رئيسيّة: طبيعة التجربة المرتبطة باستخدام المشاركين للبيئة الرقميّة (تعرّضهم لتهديد رقميّ) ومدى تأثير هذه التجربة عليهم؛ مدى معرفة المسؤولين والنشطاء بطبيعة الاعتداءات والهجمات المبنيّة على الجانب الاجتماعيّ (إلى جانب البعد السياسيّ والوطنيّ)، وخطورة الهجمات الرقميّة، لا سيما على الأجيال الناشئة؛ مقاربة الحلّ والتحرّك، ومدى مساحات العمل والنشاط التي يمكن العمل عليها.

جرت الحوارات والنقاشات باللغة العربيّة بين المحكيّة والفصحى، واختلفت بنيتها ومكوّنات الأسئلة فيها تبعا للفئة التي تمثّلها المجموعة، وتبعًا لموقفها وطبيعة عملها وعلاقتها بموضوع البحث. أدار الباحث شخصيًا أربعة نقاشات من بين النقاشات الخمسة، ولم يتمكّن من إدارة اللقاء الوجاهيّ في القدس بسبب القيود الأمنيّة والتضييقات لدخول المدينة.

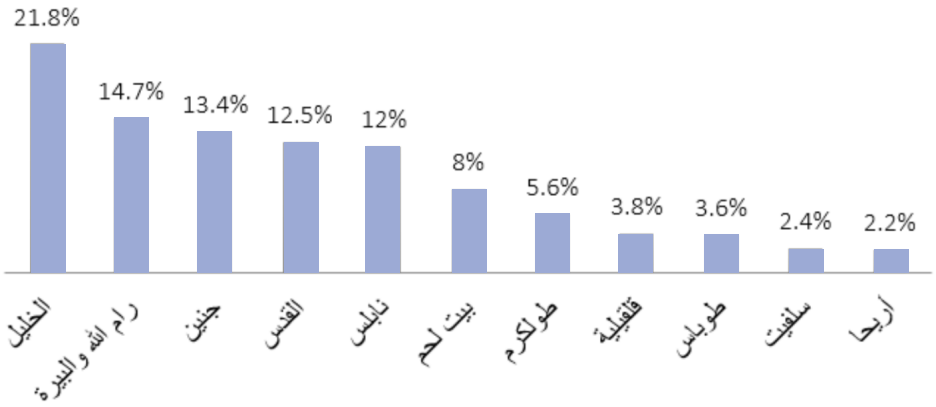
الباب الرابع

نتائج الدراسة التحليليّة: الاستطلاع والمجموعات البؤريّة

1. خصائص المشاركين

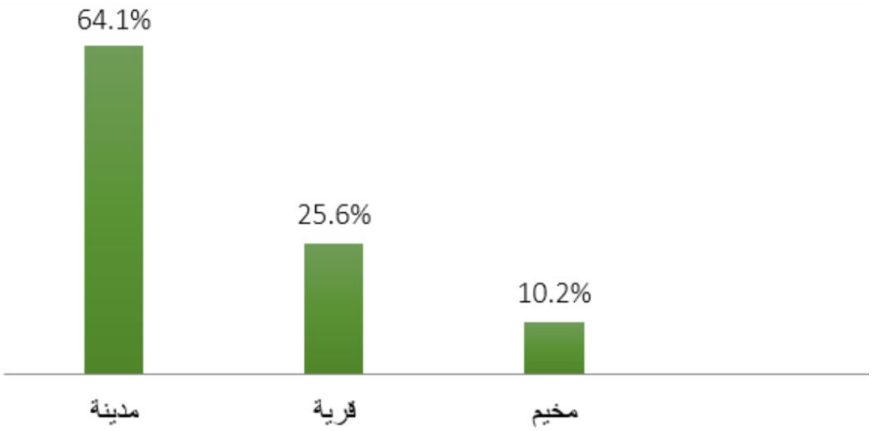
1.1 مكان السكن

الشكل (1): نسب المشاركين بحسب مكان سكناهم



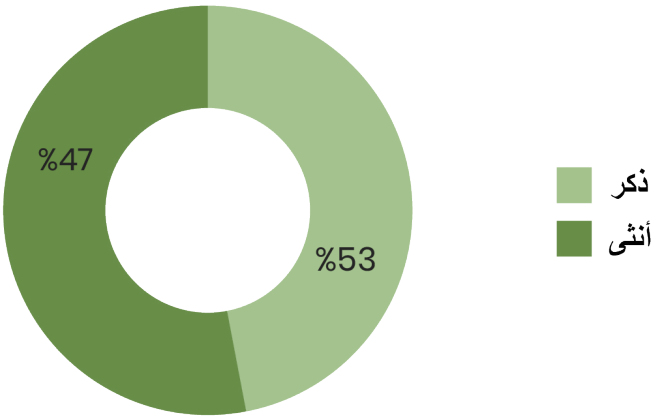
1.2 طبيعة مكان السكن

الشكل (2): طبيعة مكان سكن المشاركين



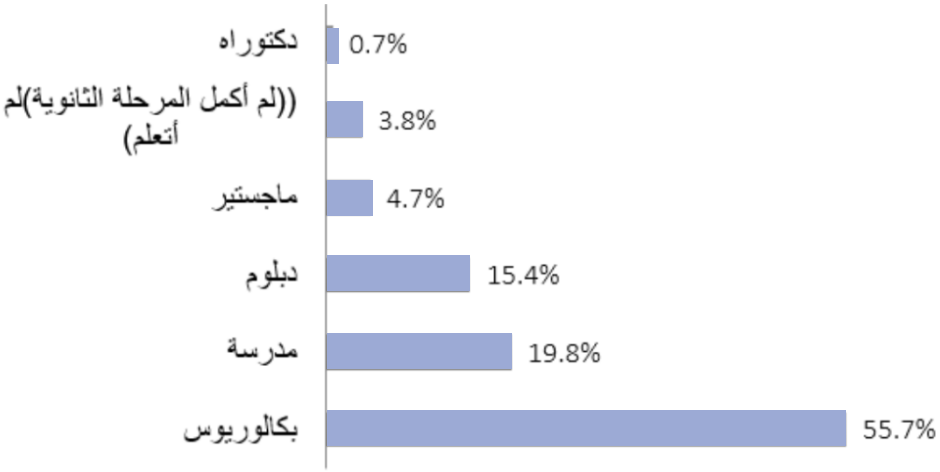
1.3 النوع الاجتماعيّ

الشكل (3): نسبة الذكور والإناث في عيّنة البحث



1.4 التحصيل العلميّ

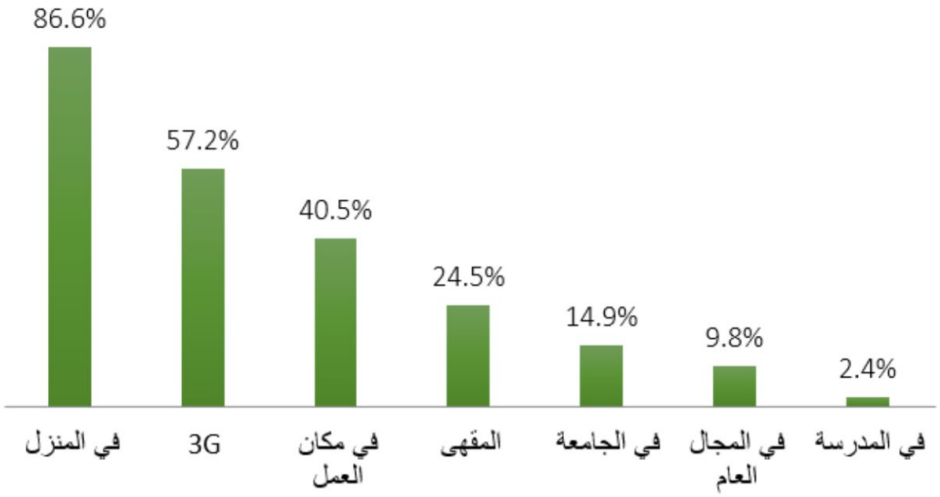
الشكل (4): نسب المشاركين حسب تحصيلهم العلميّ



2. طبيعة وخصائص استخدام شبكة الإنترنت

2.1 مكان الاتّصال بالإنترنت

الشكل (5): نسب المشاركين حسب مكان الاتّصال



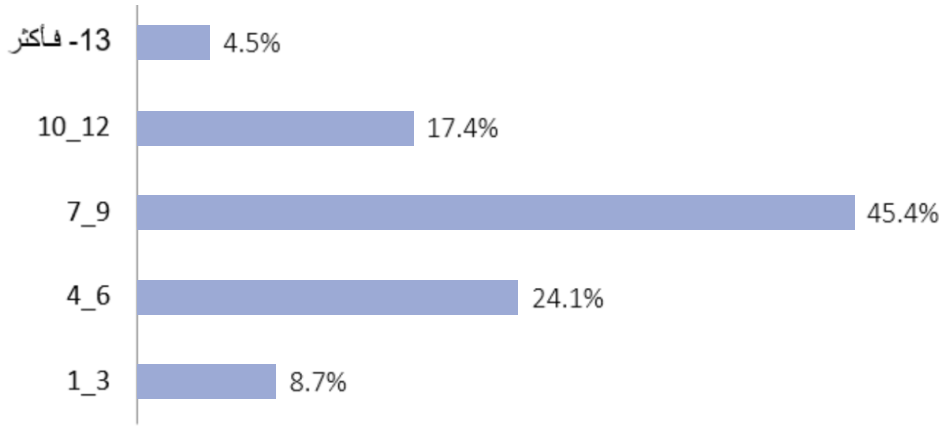
أظهرت النتائج أنّ غالبيّة كبيرة من المشاركين يستخدمون الإنترنت في المنزل وذلك بنسبة 86.6%، تلاها استخدام خدمة "الثري جي" بنسبة 57% (الخدمة تتيح الاتّصال بالشبكة في كلّ مكان)، و40.5% يستخدمون الإنترنت في مكان العمل، و24.5% في المقهى، و15% في الجامعة، ونحو 10% في المجال العامّ بحسب ما يتوفّر من خدمات عامّة في المدن الفلسطينيّة، يُشار إلى أنّ هذا السؤال أتاح إمكانيّة اختيار إجابة واحدة أو أكثر.

تتلاءم هذه النتائج مع نتائج مسح القوى العاملة للعام 2022 التي جاء فيها أنّ 92% من الأُسَر في فلسطين لديها أو لدى أحد أفرادها إمكانيّة النفاذ إلى خدمة الإنترنت في المنزل، 93% في الضفّة الغربيّة؛ وبلغت نسبة الأفراد الذين يمتلكون هاتفًا نقّالًا في فلسطين 79%، 86% في الضفّة الغربيّة. وتشير بيانات وزارة الاتّصالات وتكنولوجيا المعلومات للعام 2022، إلى ارتفاع في عدد الاشتراكات في الاتصالات الخليويّة المتنقّلة في فلسطين مع نهاية العام 2022 فقد بلغت 4.4 مليون مشترك، مقارنة مع 2.6 مليون مشترك في نهاية العام 2010، أي بزيادة نسبتها 69%.[30] تشير هذه الأرقام أنّ تطوّرًا جدّيًّا طرأ على الخدمات الاتّصاليّة في مناطق فلسطين المختلفة، لا سيما في المدن، وبطبيعة الحال هذا مصحوب بتطوّر في البنى التحتيّة. كلّ هذا يثير تساؤلاتنا حول مدى سيطرة إسرائيل ورقابتها على نشاط الفلسطينيّين الرقميّ، لا سيما وأنّ كلّ هذا التطوّر جارٍ تحت سقف الاحتلال ورقابته، فالضفّة الغربيّة جزء من الغلاف الرقميّ الإسرائيليّ.

30. الجهاز المركزيّ للإحصاء الفلسطينيّ، مصدر سابق.

2.2 عدد ساعات استخدام الإنترنت

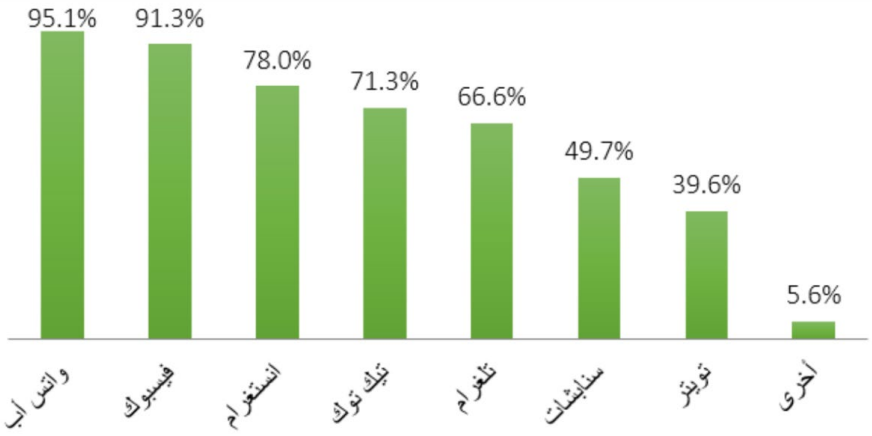
الشكل (6): نسب المشاركين حسب ساعات استخدام الإنترنت



حسب نتائج الاستطلاع؛ يقضي نحو 67% من المشاركين 7 ساعات يوميّة على الأقلّ باستخدام الإنترنت، وهو ما وصفه المشاركون في المجموعات البؤريّة، ولا سيما الشباب وطلبة المراحل الثانويّة، بـ"الإدمان"، وعدم القدرة على الابتعاد عن الشبكة رغم أنّهم يرون فيها مكانا غير آمن، لكنّها توفّر لهم مجموعة لا بأس بها من المميّزات، ومن ضمنها القدرة على التواصل مع الأصدقاء ومعرفة الأخبار والتعبير عن الذات والدراسة. وتبيّن أنّ المشاركين في المجموعات البؤريّة يقضون ساعات أكثر في الشبكة، واستغراقا[31] أعمق على مستوى طبيعة العلاقة والاستخدام، فهم "مستغرقون بعمق" داخل الشبكة، وهو أمر يمكن تفهّمه، بما أنّ مفاصل حياة الشباب كافّة تستند على الاتّصال بالشبكة، أو بكلمات بعض المشاركين في المجموعات البؤريّة "الاتّصال بالإنترنت لا يمكن الاستغناء عنه إطلاقا".

2.3 أنواع الحسابات على مواقع التواصل الاجتماعيّ

الشكل (7): نسب امتلاك المشاركين واستخدامهم لحسابات على مواقع التواصل الاجتماعيّ



31. الاستغراق مفردة تستخدم لوصف علاقة المستخدم مع الشبكة، فهو يبحر في الشبكة وكأنّه يغرق في الماء، في إشارة ودلالة على أنّ المسألة ليست دخولًا للشبكة وعملية استخدام تقليديّة.

أبرز النتائج الظاهرة أنّ الغالبية العظمى من المشاركين يستخدمون (ولديهم حسابات) تطبيقَي "واتس أب" – 95% و"فيسبوك" -91%-؛ يليها تطبيق "الانستغرام" - 78%؛ تطبيق "تيك توك" - 71%؛ تطبيق "تلغرام" - 66.6 %، تطبيق "سناب شات" - 59 %، تطبيق "إكس/تويتر" - 39.6 %، عن هذا السؤال كان بمقدور المشاركين اختيار عدّة إجابات.

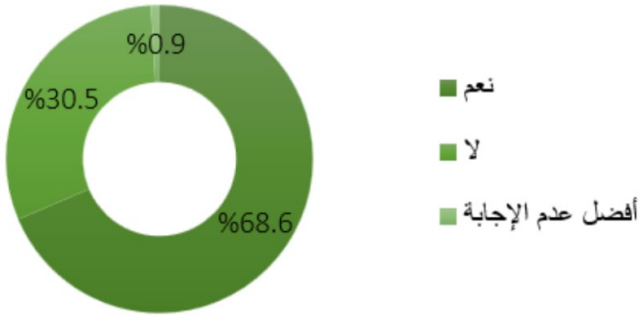
يستخدم المشاركون أكثر من منصّة اجتماعيّة للتواصل ومتابعة الأخبار، خاصّة في ظلّ الأحداث السياسيّة الراهنة. ولعلّ اللافت في هذه النتائج أنّ المنصّات الأكثر شيوعًا بين المستخدمين هي التي الأكثر قمعا للرواية الفلسطينية ، لا سيما تلك التابعة لشركة ميتا.

علّلت إجابات المشاركين في المجموعات البؤريّة أسباب شيوع منصّة إنستغرام بين الشباب وتفضيلها عن غيرها من المنصّات بأنّ فيسبوك تُعتبر منصّة "رسميّة" لا تتماشى مع "حيويّة الشباب ومرونتهم" على حدّ قولهم، إلى جانب تصاعد تطبيق سياسات الحظر والقمع الرقميّ على منصّة فيسبوك.

3. معرفة الأمان الرقميّ وإدراك المخاطر الرقميّة

3.1 معرفة المستطلعين ببرامج التجسّس وتهديداتها

الشكل (8): نسبة المشاركين الذين يعرفون/ لا يعرفون برامج التجسّس وتهديداتها



تشير النتائج إلى أنّ نسبة لا بأس بها -نحو ثلثي المشاركين- على معرفة ما (دون تحديد طبيعة المعرفة) ببرامج التجسّس والتهديدات التي تلحق بها. قد يعود ذلك إلى كثرة الحديث عن هذه البرامج في السياق الفلسطينيّ خاصّة. إذ تستهدف إسرائيل مجموعة من الناشطين والحقوقيّين بواسطة برنامج التجسّس الإسرائيليّ "پچاسوس" (Pegasus)، كي تخترق هواتفهم النقّالة الذكيّة.[32] وفي المقابل نحو 30% من المشاركين لم يسمعوا، أو ليست لديهم أيّ معلومات عن برامج التجسّس وتهديداتها، رغم نشاطهم الدائم عبر الشبكة.

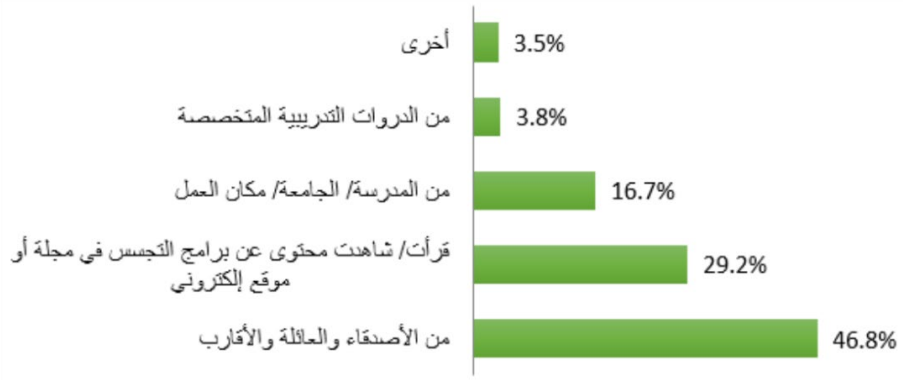
32. برمجيّة تجسّس طوّرتها وتبيعها شركة "إن إس أو غروب" (NSO GROUP).

ليس باستطاعتنا قراءة هذه الأرقام إلّا بعين القلق، فإذا أخذنا بالحسبان أنّ إجابات المعرفة عن برامج التجسّس لا تعني بالضرورة أنّ المجيب يملك الوعي الكامل أو القدرة على العمل وتوفير الحماية وتجنّب ضرر برامج التجسّس ومخاطرها، سنجد أنّنا أمام واقع يطرح علامات سؤال جدّيّة حول أثار وحجم المخاطر التي يتعرّض لها الفلسطينيّ في شبكة الإنترنت.

أظهرت النقاشات داخل المجموعات البؤريّة أنّ جزءًا من طلبة الجامعات الفلسطينيّة، وطلبة المراحل الثانويّة في مدينة القدس حصلوا على تدريبات حول الأمان الرقميّ، لكنّها غير منتظمة ونفذتها جهات فلسطينيّة أو عربيّة أو دوليّة، على سبيل المثال: مركز حملة، شبكة أريج في الأردن، واليونيسف؛ بينما ذكر المشاركون من المجموعة البؤريّة لطلبة المراحل الثانويّة في مدارس القدس أنّ مجموعة من المحامين ومن الجهات الأهليّة المقدسيّة قدّمت تدريبات خاصّة للطلبة حول الوعي بالمخاطر الرقميّة، لا سيما ما يعتبره القانون الإسرائيليّ تحريضًا على الإرهاب. لا يمكننا ضمان أنّ التدريب وصل إلى جميع المدارس ومختلف الفئات، في ظلّ ازدياد مصادر التهديد منذ بدء الحرب على قطاع غزّة وتنوّع مظاهر التجسّس والرقابة وتهديداتهما.

مصادر المعرفة عن برامج المراقبة والتجسّس وتهديداتها

الشكل (9): نسب مصادر المعرفة عن برامج التجسّس وتهديداتها

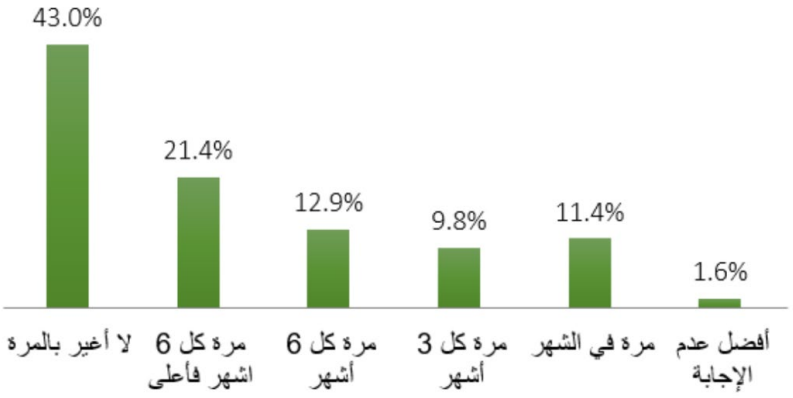


تشير النتائج إلى أنّ نسبة المعرفة الصادرة عن لدائرة الاجتماعيّة الأولى -العائلة والأقارب والأصدقاء- (46 %)، هي الأعلى من بين مصادر المعرفة، ولا سيّما المعرفة الصادرة عن لمدرسة/الجامعة/مكان العمل والدورات التدريبيّة المتخصّصة (16.7% و 3.8% على التوالي). هذه النتائج في غاية الأهميّة وتدفعنا للتساؤل حول طبيعة المعرفة الصادرة عن لدائرة الاجتماعيّة الأولى، التي يمكن وصفها بأنّها ليست متخصّصة، وقد تكون غير دقيقة ومليئة بالمبالغة، وقد تكون معرفة معزّزة للمخاوف والقلق في ضوء غياب مهنيّتها وعلميّتها، وتحديدًا في ظلّ تراجع المعرفة من مؤسّسات إنتاج المعرفة التقليديّة مثل: المدرسة والجامعة ومكان العمل.

لقد عزّزت هذه النتائج النقاشات مع المجموعات البؤريّة (طلبة مراحل ثانويّة، طلبة جامعات، نشطاء ومؤسّسات عاملة)، وطرحت هذا الخلل المرتبط بغياب ملحوظ للتوعية في قضايا التجسّس والهجمات أو الاعتداءات الرقميّة، وخاصّة في صفوف فئات مجتمعيّة تعتبر الأكثر تعرّضًا للخطر والأكثر استهدافا - فئات المراحل الثانويّة-. وممّا جاء على لسان المشاركين في المجموعات البؤريّة أنّ الطلبة، والطالبات على وجه الخصوص قد تعرّضوا/ن لاعتداءات رقميّة في سنّ مبكرة (12-10 عامًا وأحيانًا أقلّ من ذلك)، وأنّ فئة كبار السن (50 عامًا فما فوق) تعرّضوا للابتزاز والتهديد. وعلينا أن نأخذ ، على محمل الجدّ، النسبة المتدنيّة للمعرفة من مصادر متخصّصة – الدورات التدريبيّة- التي تعتبر أهمّ مصدر للمعرفة السليمة ببرامج التجسّس وتهديداتها وكيفيّة معالجتها وتفاديها.

3.3 وتيرة تغيير كلمة المرور

الشكل (10): وتيرة تغيير كلمة المرور



بهدف معرفة مدى اتّخاذ المشاركين للإجراءات التي تعتبر من أساسيّات الأمان الرقميّ، طُرحت عليهم مجموعة من الأسئلة تخصّ هذه الأساسيّات، ومن ضمنها السؤال عن وتيرة تغيير كلمة المرور لحساباتهم المختلفة. تبيّن أنّ نحو 43% من المشاركين لا يغيّرون كلمات المرور بتاتًا، في حين 21.4% منهم يغيّرون كلمات المرور بمعدّل مرّة بالسنة على الأكثر، ونحو 13% يغيّرون كلمات المرور بمعدّل مرّة كلّ نصف سنة، ونحو 10% يغيّرون كلمات المرور بمعدل مرّة كلّ 3 شهور، و11.4% يغيّرون كلمات المرور شهريًّا.

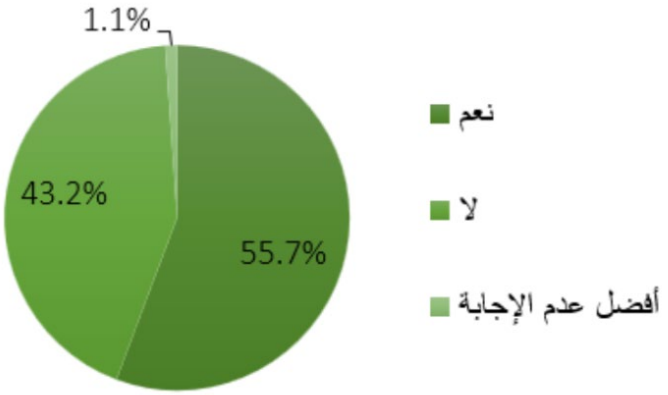
يُعتبر تغيير كلمات المرور من أبسط أسس الأمان الرقميّ، وتشير النتائج إلى أنّ نحو نصف المشاركين لا يغيّرون كلمات المرور، وقد يكون سبب هذا : أوّلا، غياب الوعي والمعرفة لأهميّة كلمات المرور وتغييرها؛ ثانيًا، قد يكون لدى المشاركين المعرفة الأساسية لأهميّة تغيير كلمات المرور ولكنّهم لا يأبهون لتغييرها ولا يعيرونها أيّ اهتمام. وقد نستدلّ من السبب الثاني أنّ ثمّة ضرورة لتحفيز المستخدمين على تغيير سلوكهم، تقع هذه المسؤولية على عاتق الجهات المختصّة.

هنا لا بدّ من الإشارة إلى أنّ النقاش في المجموعات البؤريّة كشف عن تعرّض غالبيّة المشاركين فيها إلى هجمات مثل: سرقة حسابات أو محاولة سرقة حسابات، ابتزاز، تهديد رقميّ. وهو ما عرّضهم لحالات من

القلق والتوتّر والشعور بعدم الأمان والخطر. وقد ظهر في المجموعات البؤريّة الخاصّة بطلبة الجامعات والطلبة في المراحل الثانويّة أنّ ثمّة علاقة طرديّة بين التعرّض للهجمات الرقميّة و مدى المعرفة بها وسبل الحماية منها. بحسب أقوالهم فإنّ استهدافهم أو الاعتداء عليهم رقميًّا دفعهم لتطوير معرفتهم بالأمان الرقميّ وتطبيقها، وجاء على لسان إحدى المشاركات "إنّها معرفة ووعي من وجع ومعاناة [...] لقد غيّر الاعتداء عليّ حياتي كليّا، تغيّرت نظرتي للحياة وللشبكة، ولكلّ من يحيط بي".

4.3 إعدادات الأمان على الشبكات الاجتماعيّة

الشكل (11): نسبة المشاركين الذين يحدّدون إعدادات الأمان

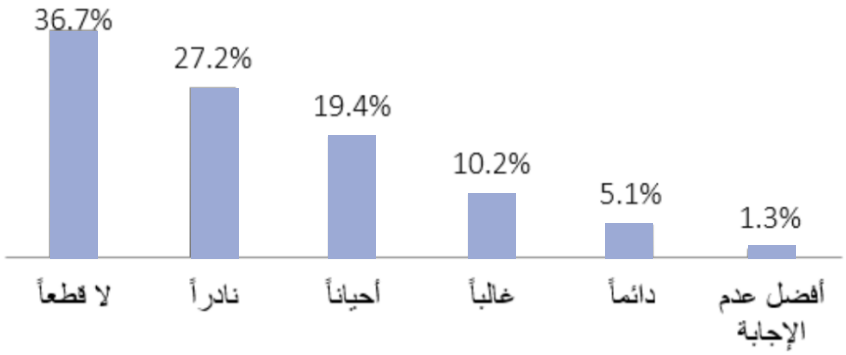


تعتبر إعدادات الأمان والخصوصيّة (السلامة) في الشبكات الاجتماعيّة مسألة غاية في الأهمية بالنسبة لصفحات الأفراد أو المجموعات أو المنظّمات. تتضمّن الإعدادات مجموعة من الأسئلة الرئيسيّة، على المستخدم أن يطرحها على نفسه أثناء تحديد هذه الإعدادات، منها على سبيل المثال، طبيعة مشاركة المنشورات مع العامّة أو مع مجموعة معيّنة من الأشخاص، ومن يمكنه التعليق أو الردّ أو التفاعل مع رسائل أو منشورات المستخدم، وإمكانيّة العثور على المستخدم أو على المنظّمة التي يعمل بها، ومدى رغبة المستخدم في مشاركة موقعه تلقائيًا عند النشر، ومدى الرغبة في حظر الحسابات المعادية أو كتم صوتها، ورغبته في حظر كلمات معيّنة أو علامات كلمات رئيسيّة. تتيح هذه الإعدادات للمستخدمين قائمة من الخيارات التي تضمن لهم "سلامة ما" فيما لو استخدمت وكانت نابعة من إدراك بها وعلى نطاق جيّد.

وتعكس النتائج في الشكل (11) أنّ نحو نصف المستطلَعين لا يستخدمون إعدادات الأمان مطلقًا، وهو ما يجعلهم عرضة للهجمات والاعتداءات والاختراقات والتتبّع وإتاحة انتهاك الخصوصيّة، وقد أكّدت المجموعات البؤريّة هذه النتائج، وشدّد بعض المشاركين على أنّهم أنشأوا حسابات خاصّة بهم، دون أن يكون لديهم أيّ معرفة بإعدادات الأمان التي توفّرها المنصّات للمستخدمين. وقال بعض المشاركين في المجموعات البؤريّة إنّ بعض الأمّهات ينشئن حسابات لأبنائهنّ وبناتهنّ دون أن يأخذن بالحسبان طبيعة استخدام الحسابات أو دون أن يدركن المخاطر الكامنة في هذه المنصّات. هذا السلوك يصل حدّ السذاجة في فهم طبيعة المنصّات أو البيئة الرقميّة التي يُزج اليافعون والأطفال في أتونها. علاوة على هذا، ساد شعور عميق بعدم الأمان على الشبكة بين مشتركي المجموعات البؤريّة.

3.5 إضافة أشخاص غير معروفين على حساباتي في الشبكة

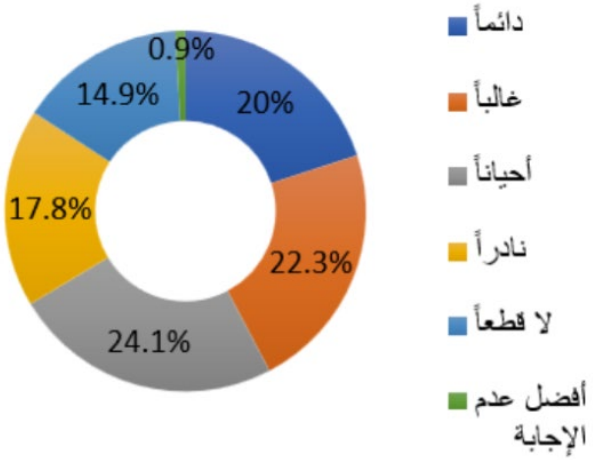
الشكل (12): وتيرة المصادقة على طلبات صداقة من أشخاص غير معروفين في الشبكة



تُظهر النتائج أنّ نحو ثلثي المستطلعة آرائهم يصادقون على طلبات الصداقة أو يضيفون أشخاصًا لا يعرفونهم عبر منصّات التواصل الاجتماعيّ. تتراوح وتيرة المصادقة بين نادرًا (27.2%) وبين غالبًا ودائما (سوية 15%). ومن المتعارف عليه أنّ هذا السلوك سيجعلهم عرضة للمخاطر، ويزداد احتمال تعرّضهم للمخاطر بسبب سياسات الاحتلال الإسرائيليّ، إلى جانب ارتفاع حالات الاحتيال التجاريّ والسرقة والابتزاز والتلاعب بالمشاعر والتضليل. هذا السلوك يدلّ أيضًا على نقص معرفيّ في بيئة الشبكة وفي طبيعة التهديدات التي يمكن أن يتعرّض لها المستخدمون.

وأشارت المجموعات البؤرية المؤلّفة من طلبة المراحل الثانويّة إلى مجموعة من المشاكل الجدّيّة التي نتجت عن إضافة أشخاص غير معروفين لقوائم أصدقائهم. وذكر الطلبة أنّ المجموعة الأكثر استهدافًا هي الإناث في جيل المراهقة، وبعض الأحيان في جيل ما قبل مرحلة المراهقة؛ وقالوا إنّ سلوك الأشخاص المجهولين يتّخذ أسلوبا وديًّا في البداية وينتهي بمعاناة وابتزاز وتهديد وتحرّش.

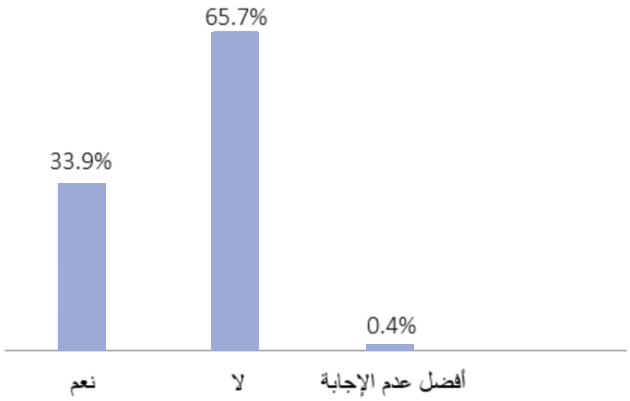
3.6 مشاركة صور وأمور شخصيّة عبر الشبكة



تشير النتائج إلى أنّ نحو 66% من المستطلَعين شاركوا صورًا وأمورًا شخصيّة عبر الشبكة، بتفاوت (غالبًا، دائمًا وأحيانًا بنسب متقاربة). يمكن الاستنتاج من هذه النتيجة أنّ ثمّة اعتقادًا سائدًا بين المستخدمين بأنّ الشبكة آمنة، وأن لا مخاطر قد تترتّب على مشاركة أمور شخصيّة. لا يمكننا الجزم أنّ من أجاب بنُدرة مشاركته الصور والأمور الشخصيّة فعل ذلك نتيجة معرفته بالمخاطر، فقد يكون ذلك نتيجة أسباب وعادات ثقافيّة. ومن الأهمية بمكان، الإشارة إلى المخاطر النابعة من السياق الفلسطينيّ عند مشاركة الصور والأمور الشخصيّة، فهي تستخدم مصدرًا لاستقاء المعلومات والرقابة على الناشطين والفاعلين السياسيّين قد تؤدّي إلى ملاحقتهم واعتقالهم، هذا إلى جانب المخاطر الاجتماعيّة المتعارف عليها مثل الابتزاز والتهديد.

3.7 استخدام برامج الحماية في الإنترنت

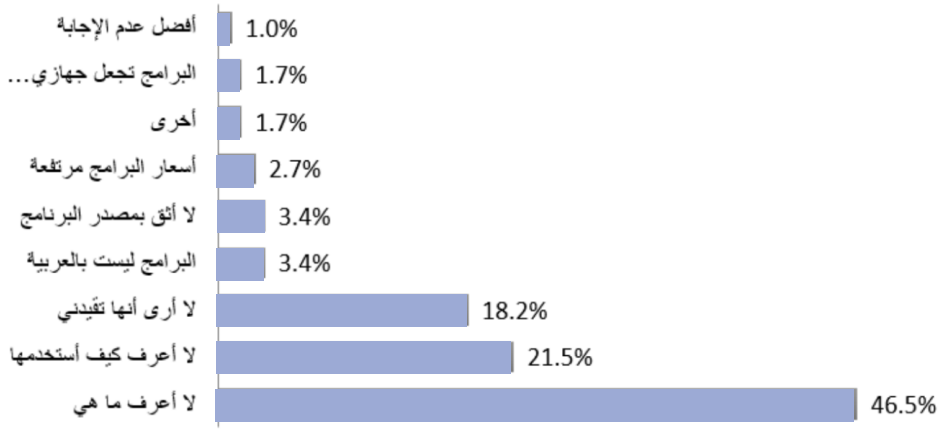
الشكل (14): نسبة المشاركين الذين يستخدمون برامج الحماية



تشير النتائج إلى أنّ نحو 66% من المستطلَعين لا يستخدمون برامج حماية لأجهزتهم، بينما يستخدمها نحو ثلث المستطلَعين. سلوك المستخدمين هذا يعزّز من فرص استهدافهم في البيئات الرقميّة، لا سيما فئة الشباب. ولعلّ السؤال الأبرز الذي علينا طرحه هنا: ما هي الأسباب التي تمنع ومنعت المستطلَعين من استخدام برامج الحماية الأساسيّة؟ سنجيب عن هذا السؤال في البند التالي.

3.8 أسباب عدم استخدام برامج الحماية على الأجهزة الإلكترونيّة

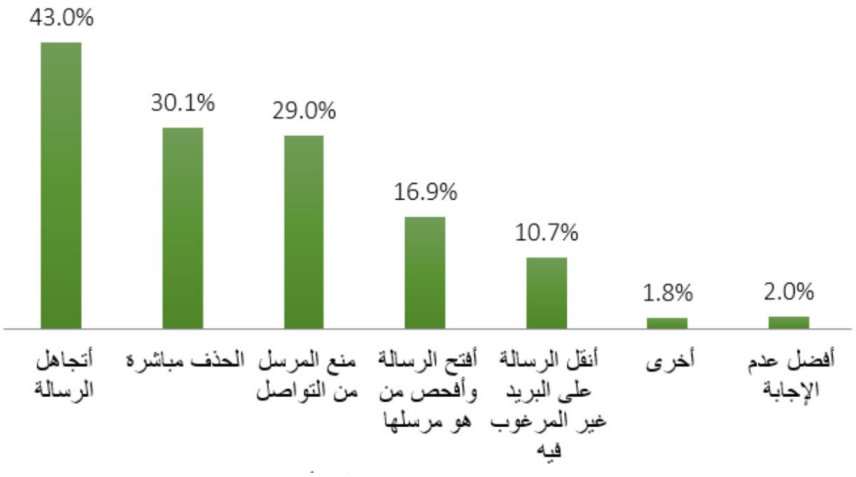
الشكل (15): توزيع أسباب عدم استخدام برامج الحماية من قبل المستطلَعين



تفسّر نتائج هذا البند ما جاء في البند السابق من انعدام استخدام برامج الحماية، نستطيع تصنيف الإجابات في مجموعتين: المجموعة التي لا تعرف ما هي برامج الحماية - 46.5% من المستطلَعين الذين أجابوا بأنّهم لا يستخدمونها؛ والمجموعة التي تعرف ما هي برامج الحماية، لكنّها لا تستخدمها - 53.5%. واللافت في المجموعة الثانية أنّ قرابة نصف من اختاروا عدم استخدام البرامج؛ كانت أسبابهم عدم تمرّسهم (نحو 25%)، والنصف الآخر كانت أسبابهم تقنيّة. تعكس هذه النتائج أزمة عميقة في المعرفة وفرصة سانحة لنشر الوعي حول هذه البرامج والتدريب على استخدامها. وهذا ما أكّدته مجموعة المؤسّسات والنشطاء البؤريّة عند طرح هذا السؤال، التي أشارت إلى أهميّة وضرورة تكثيف العمل على تدريبات الحماية والوقاية الرقميّة.

3.9 السلوك عند استلام رسائل من مصدر مجهول

الشكل (16): توزيع سلوك المستطلَعين عند استلامهم رسائل من مصدر مجهول

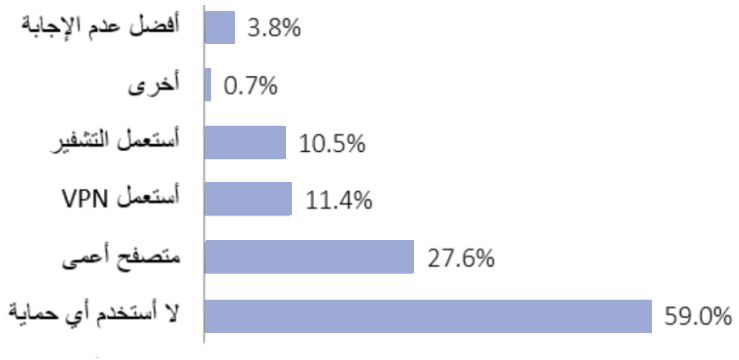


يتناول هذا البند سلوكيّات المستطلَعين عند استلامهم رسائل من مصدر مجهول (كان بإمكانهم اختيار أكثر من إجابة)، بيّنت النتائج أنّ السلوك الأكثر شيوعًا بينهم، نحو النصف (43%)، هو تجاهل الرسالة والمرسِل، ومنهم من اختار سلوكيّات قد تُعتبر سلوكيّات وقاية وحماية، على سبيل المثال الحذف مباشرة ومنع المرسِل من التواصل نحو 30% كلّ واحد منهما.

قد يُعتبر تجاهل الرسائل مجهولة المصدر مسألة جيدة، بيد أنّه فعل لم يُتّخذ عن وعي وإدراك حول الجهات المُرسِلة أو طبيعة الاستهداف (أمنيّ/ تجاريّ/ سياسيّ، اجتماعيّ). وإذا أخذنا بالحسبان احتمال أن يتكرّر فعل إرسال رسالة من ذات الجهة، واحتمال أن يفتح المستخدم هذه الرسالة، فقد تكون العاقبة وخيمة؛ ولا سيما في ظلّ تطوّر أساليب الاحتيال والرقابة والاختراق.

3.10 الحماية الرقميّة أثناء استخدام الإنترنت

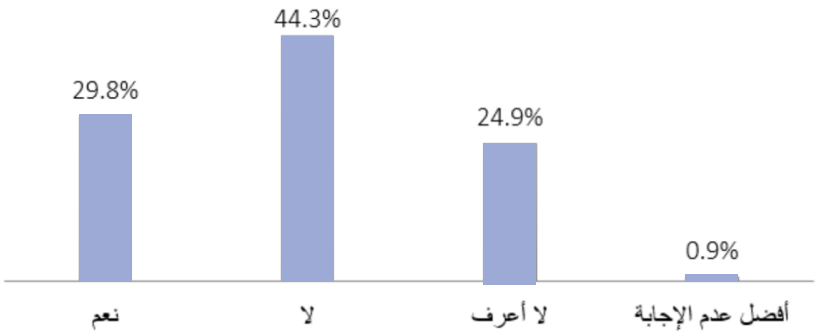
الشكل (17): توزيع أساليب الحماية التي يتّخذها المستطلَعون أثناء تصفّح الإنترنت.



تتلاءم الإجابات عن هذا السؤال مع إجابات المستطلَعين عمّا سبق من أسئلة تتعلّق بالحماية والوقاية الرقميّة. أظهرت النتائج أنّ أكثر من نصف المستطلَعين لا يستخدمون أيّ وسيلة حماية رقميّة (59%). ومن تبقّى من المستطلَعين صرّحوا أنّهم يستخدمون وسائل حماية مختلفة أبرزها استخدام المتصفّح الأعمى[33] (27.6%)، في حين صرّح 11.4% و10.5% من المستطلَعين أنّهم يستخدمون "في بي إن"[34] والتشفير[35] (على التوالي). تُعتبر وسائل الحماية التي طُرحت في الإجابات عن هذا السؤال أساسيّة وسهلة الاستخدام وبمقدورها أن توفّر حماية رقميّة واستخدامًا آمنًا للإنترنت. نستطيع أن نقرأ هذه النتائج كمتمّمة للصورة التي رسمت في الإجابات السابقة، وهي أنّ الجمهور لا يعرف ما هي برامج الحماية التي يمكنها أن توفّر له استخدامًا آمنًا للإنترنت، وعلى ما يبدو أنّ ثمّة حاجة ماسة لإيصال هذه المعرفة للمستخدِمين كافّة.

3.11 خاصيّة تحديد الموقع الجغرافيّ

الشكل (18): نِسَب تشغيل خاصيّة تحديد الموقع الجغرافيّ بين المستطلَعين



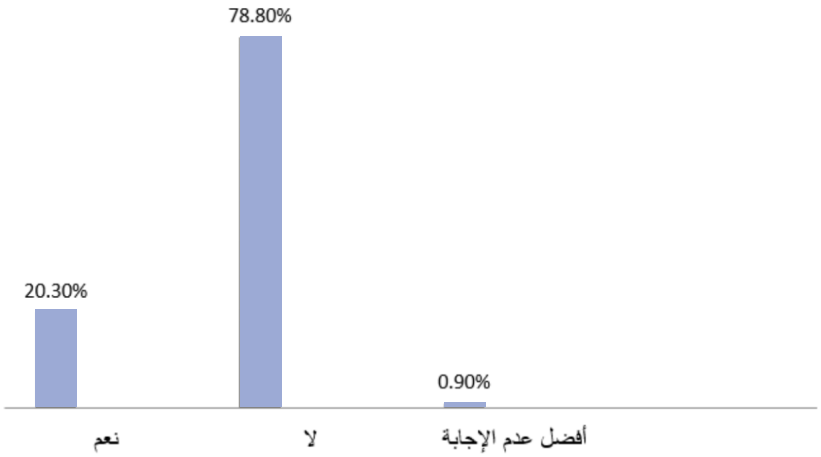
33. المتصفّح الأعمى يوفّر إمكانية عدم تتبّع وتقفّي المواقع التي يتصفّحها المستخدِم.
34. في بي إن ("VPN") يوفّر إمكانية الاتّصال بالإنترنت دون الكشف عن مكان الاتّصال.
35. التشفير يوفّر إمكانيّة تحويل نصّ الرسائل إلى معلومات مشفّرة بواسطة خوارزميّات خاصّة.

تُظهر النتائج أنّ ثلث المستطلَعين (29%) يستخدمون خاصيّة تحديد الموقع الجغرافيّ، هذا يعني كشفهم للأماكن التي يتواجدون فيها. بينما صرّح 44% منهم أنّهم لا يستخدمون هذه الخاصيّة، وعلى ما يبدو أنّ هذه الخاصيّة متعارف عليها أكثر من باقي وسائل الحماية. أظهر النقاش مع مختلف المجموعات البؤريّة تناقل حكايات وقصص عن عمليّات سرقة حدثت بسبب كشف الموقع الجغرافيّ للمستخدِمين. وقد يكون الضرر اللاحق بالشباب الفلسطينيّين جسيمًا على المستوى السياسيّ في ظلّ تصعيد سياسات القمع والتهديد والاعتقال، فعلى سبيل المثال؛ تستطيع السلطات تحديد أماكن تواجدهم وتجمهرهم وتنقّلهم ونشاطهم السياسيّ بواسطة هذه الخاصيّة. تجدر الإشارة إلى أنّه في حال نشر المستخدِم صورًا، وكانت خاصيّة كشف الموقع الجغرافيّ فعّالة، تستطيع السلطات الأمنيّة استخدامها دليلًا للتهديد والاعتقال، إلى جانب تعزيز احتمالات انتهاك خصوصيّتهم الرقميّة.

4. الهجمات والاعتداءات الرقميّة

4.1 التعرّض للإساءة أو الهجوم أو الابتزاز من متطفّلين، أو "هكرز"

الشكل (19): نسبة المتعرّضين للهجمات والاعتداءات الرقميّة

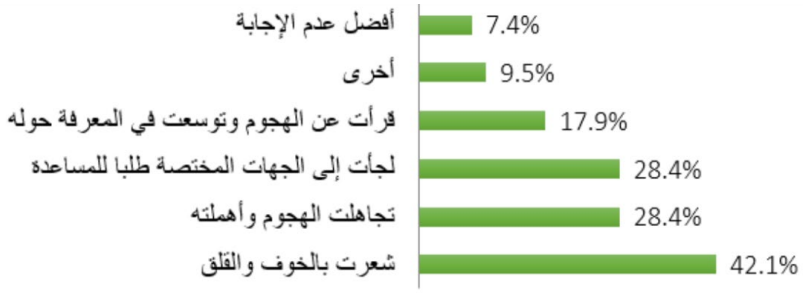


تُظهر النتائج أنّ الغالبية العظمى من المستطلَعين (79%) لم يتعرّضوا لإساءات أو هجمات أو تهديدات أو اعتداءات أو ابتزازات رقميّة من متطفّلين أو "هكرز؛ في حين قال 20% من المستطلَعين أنّهم تعرّضوا لاعتداءات رقميّة.

لا يمكننا الاستخفاف بهذه النسبة، مع أنّها قد تبدو للوهلة الأولى ضئيلة، فهي تُعتبر مرتفعة نوعًا ما، وهي مؤشّر لمشاكل وسلوكيّات مستخدمي الإنترنت مِن طرفي الهجوم -انظروا البنديْن التاليْن- حسبما جاء في نقاشات المجموعات البؤريّة. فنسبة من تعرّض للهجمات من عيّنة البحث تشير إلى مشاكل عميقة في ظلّ غياب الوعي والمعرفة تارة، وتجاهل التهديدات والتعامل معها وكأنّها غير موجودة تارة ثانية، أو التعامل باستخفاف مع الهجمات الرقميّة بحيث لا ينعكس إدراك المخاطر الرقميّة باكتساب المهارات والممارسات التي تضمن تحصينًا في البيئات الرقميّة.

4.2 تعامل المستطلعين مع الهجوم أو الاعتداء الرقميّ

الشكل (20): سلوك المستطلَعين بعد الهجوم الرقميّ

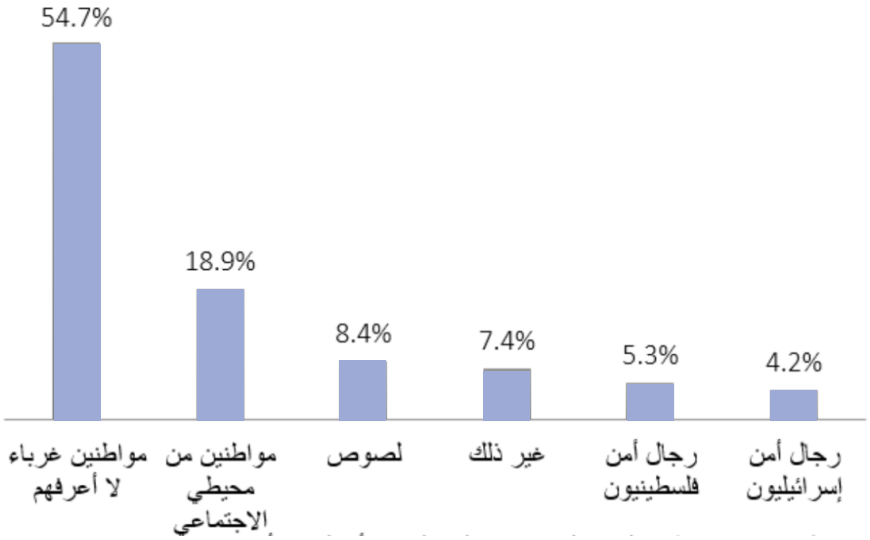


تُظهر النتائج أنّ ردّ فعل غالبية المستطلَعين الذين تعرّضوا للهجوم هو الخوف والقلق من هذا الهجوم (42%)، وبنسب متساوية (28.4%) أجاب المستطلعون أنّهم تجاهلوا الهجوم أو لجأوا للجهات المختصّة للمساعدة، و 18% قالوا إنّهم اختاروا توسيع معرفتهم عن الهجوم.

تعكس النتائج مشاكل وتناقضات في التعاطي مع الهجمات الرقميّة، ففي حين أنّ الهجمات تُشعر المستخدِمين بالخوف والقلق، إلّا أنّ جانبا لا بأس به من المتعرّضين لها يتجاهلونها ويهملونها عوضًا عن التعامل معها. ومما تبيّن عند نقاش هذه المسألة في المجموعات البؤريّة كافّة؛ أنّ غالبيّتهم لا يتّخذون التدابير الضروريّة عند البحث عن معالجة الاعتداء أو الهجوم الرقميّ، برز هذا في مجموعتي طلبة المراحل الثانويّة وطلبة الجامعات.

4.3 الجهات خلف الهجوم أو الاعتداء

الشكل (21): الجهات التي تقف خلف الهجمات والاعتداءات الرقميّة



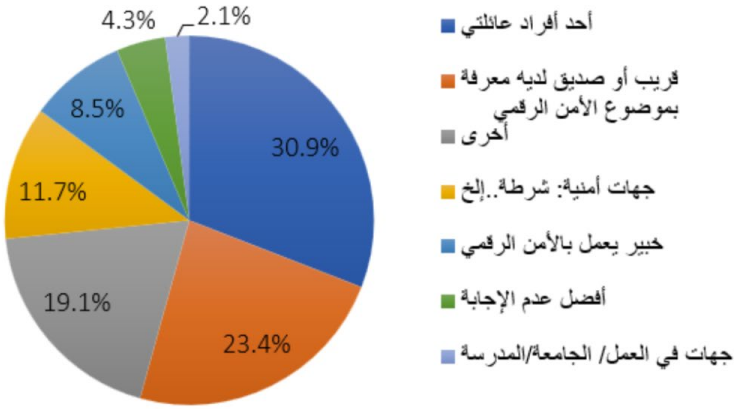
يظهر من النتائج أنّ نحو 55% من المعتدين كانوا أفرادًا مجهولين/غرباء بحسب أقوال المستطلَعين، بينما قال نحو 20% إنّ من اعتدى عليهم كانوا أفرادًا من محيطهم الاجتماعيّ؛ نحو 9% قالوا إنّ لصوصًا اعتدوا عليهم؛ أمّا الاعتداءات الصادرة من جهات أمنيّة فلسطينيّة أو إسرائيليّة فكانت 5.3% و4.2% على التوالي.

عند قراءة هذه النتائج علينا الأخذ بالحسبان نتائج البند السابق، لا سيما مجموعة المستطلَعين الذين يتجاهلون الهجوم والاعتداء الرقميّ عليهم. فإذا كان المهاجمون أفرادًا مجهولين واخترنا تجاهل الهجوم فالاحتمال أن يكرّر المهاجمون فعلتهم حتميّ الحدوث، لأنّه لم يبلَّغ عنهم. عادة ما يحتمي المعتدون بالإمكانيّات التي توفّرها شبكة الإنترنت وشبكات الاتّصال المتعدّدة في الضفّة الغربيّة، إذ يلجأ جزء منهم لاستخدام مزوّد الاتّصالات الإسرائيليّ لفتح حسابات وهميّة بغية الاعتداء على المستخدمين، وهو ما يصعّب عملية اقتفاء تفاصيل المهاجمين والمعتدين في الضفّة الغربيّة.

من أبرز ما أظهرته نقاشات المجموعات البؤريّة بهذا الصدد، أنّ ثمة تزايدًا في الهجمات الصادرة من أفراد من المحيط الاجتماعيّ للمعتدى عليه (أقارب/ أصدقاء). وعلى ما يبدو، نحن بصدد آفة وآليّة اجتماعيّة جديدة للاعتداء والتنمّر بين أفراد العائلة والأصدقاء.

4.4 الجهات التي لجأ إليها المستطلَعون بعد الهجوم أو الاعتداء الرقميّين

الشكل (22): الجهات التي يلجأ إليها المستطلَعون بعد التعرّض لهجوم أو اعتداء رقميّيْن



تُظهر النتائج أنّ نصف المستطلَعين يفضّلون اللجوء للدائرة القريبة منهم، نحو 30% يلجؤون لأحد أفراد العائلة ونحو 23% يلجؤون لقريب أو صديق يملك معرفة بالأمان الرقميّ. بينما يلجأ النصف الآخر لجهات أخرى غير التي ذكرت في السؤال بنسبة 19%، و12% يلجؤون لجهات أمنيّة وشرطيّة، و8.5% يلجؤون لخبير في مجال الأمان الرقميّ.

عند قراءة هذه النتائج علينا أن نلتفت إلى أمريْن في غاية الأهميّة: الأوّل، أنّ المستطلَعين يلجؤون للأقارب والمعارف، وقد يرتبط هذا مع نتائج البند السابق بأنّ 19% من الاعتداءات يقف خلفها أفراد من الدائرة

ذاتها، وبذلك هم يفضّلون حلّ المشاكل داخليًّا؛ الثاني، أنّ مسار التوجّه لجهات أمنيّة وشرطيّة، وهو المسار المتعارف عليه لتقديم شكاوى ضدّ المعتدين، ليس الخيار الأساسيّ في التعامل مع الاعتداءات الرقميّة. إلى جانب ذلك، قد تكون هذه النتائج مؤشّرًا لمواضع ثقة الشباب الفلسطينيّين، ومؤشّرًا للمؤسّسات بضرورة التوعية في مجال الأمان الرقميّ على المستوى الأُسريّ.

دعمت النقاشات في المجموعات البؤريّة ما جاء في نتائج الاستطلاع، وانقسمت الآراء داخل مجموعة القدس البؤريّة حول الجهات المختصّة التي على المستخدمين اللجوء إليها، لأنّ الجهة التي عليها أن توفّر الحماية والأمان الرقميّ لفئة الشباب هي جهاز أمنيّ إسرائيليّ يمارس سياسات احتلال وقمع ضدّهم، وهو أساسًا مصدر تهديد وليس مصدر حماية وأمان.

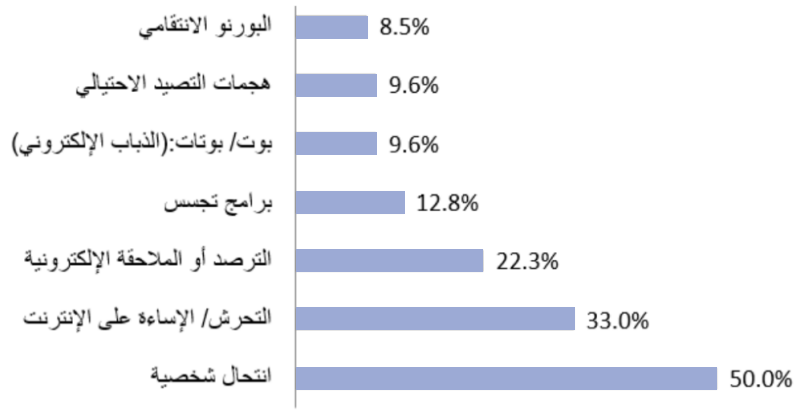
أظهرت النقاشات في مجموعات طلبة المرحلة الثانويّة والجامعات أنّ اللجوء إلى الأهل كان بمثابة الخيار الأخير، وذلك بعد استنفاد كلّ محاولات التعامل مع الاعتداء شخصيًّا، ولعلّ هذه النتيجة المقلقة تستوجب بحثًا معمّقًا للوصول إلى تفسيرات حول الأسباب التي تدفع الشبّان الصغار إلى عدم مصارحة الأهل بتعرّضهم لهجمات رقميّة.

طغى على النقاش في المجموعة البؤريّة التي خصّصت للمؤسّسات العاملة في مجال الحقوق الرقميّة، عمق إشكاليّة الخيارات المتاحة أمام المواطنين عند طلب الحماية، ولا سيما في الضفّة الغربيّة بسبب عدم ثقة الشباب بالأجهزة الأمنيّة، وضعف قدرة هذه الأجهزة التقنيّة، وعجزها عن التعامل مع الهجمات التي تستخدم خدمات إنترنت إسرائيليّ (شرائح إسرائيليّة)، إلى جانب ترهّل عملها في ظلّ بيروقراطيّة عمل عالية، وعدم جديّتها في التعاطي مع شكاوى المواطنين، ولأنّها تستند في ممارساتها الشرطيّة إلى قانون الجرائم الإلكترونيّة، الذي يحمل الكثير من علامات الاستفهام من مؤسّسات حقوقيّة ومدنيّة.

تعكس نقاشات المجموعات البؤريّة أنّ ثمة أزمة ثقة حقيقيّة سائدة بين المستخدمين ومحيطهم على عدّة مستويات، منها الشخصيّة والمهنيّة والرسميّة. فإذا أردنا التغلّب على مخاطر الهجمات الرقميّة علينا إعادة بناء هذه الثقة، وعلينا إعادة تأهيل للجهات الرسميّة، وعلينا توفير تدريبات للمستخدمين كافّة في مجال الأمان الرقميّ.

4.5 أنواع الهجمات والاعتداءات الرقميّة

الشكل (23): أنواع الاعتداءات والهجمات التي تعرّض لها المستطلَعون



حاولنا بواسطة المسح الميدانيّ معرفة طبيعة ونوع الهجمات والاعتداءات التي تعرّض لها المستطلَعون، في هذا البند قُدِّم لهم تعريف بسيط حول الإجابات المقترحة من أجل توحيد المفاهيم لدى المشاركين. أظهرت النتائج أنّ نصف الهجمات/ الاعتداءات كانت من نوع "انتحال الشخصيّة" – والمقصود: إنشاء حسابات تواصل اجتماعيّ وهميّة تستخدم اسم وصورة الشّخص المستهدَف، أو سرقة حسابات والسيطرة عليها-. ثلث الهجمات/الاعتداءات (33%) كانت من نوع "التحرّش والإساءة الرقميّان" – المقصود: استخدام الشبكات الاجتماعيّة استخدامًا عدائيًّا بهدف التنمّر والتهديد وإزعاج شخص ما، بواسطة التعليق على محتويات نشرها المعتدى عليه أو علّق عليها-.

هجمات/اعتداءات من نوع "الترصّد والملاحقة الإلكترونيّة" – المقصود: مطاردة تشمل الاتّهامات الكاذبة والتشهير والقذف، أو المراقبة أو نشر المعلومات الشّخصيّة الحسّاسة لشخص ما عبر الإنترنت- كانت رائجة بنسبة 22.3%.

هجمات/اعتداءات من نوع "برامج تجسّس" – المقصود: برامج تثبت على الجهاز دون موافقة صاحب الجهاز تخترق كلّ الحسابات وتسيطر عليها، على سبيل المثال بيچاسوس- كانت شائعة بنسبة 12.8%. وتبيّن من النقاش في المجموعات البؤريّة أنّ فئة الشباب قد تعرّضوا أكثر من غيرهم لهذا النوع من الهجمات.

وتبيّن أنّ هجمات من نوع "الذباب الإلكترونيّ بوت/ بوتات" – المقصود: برامج كمبيوتر آليّة تنفّذ مهامّ تكراريّة من حسابات وهميّة مبرمجة لإرسال رسائل مسيئة- كانت نسبتها نحو 10%.

أمّا هجمات "التصيّد الاحتياليّ" – المقصود: دودة أو ڤيروسات وهو نوع من هجمات الهندسة الاجتماعيّة يُستخدم لسرقة البيانات، على سبيل المثال، بيانات اعتماد تسجيل الدخول وأرقام بطاقات الائتمان- كانت بنسبة 9.6%.

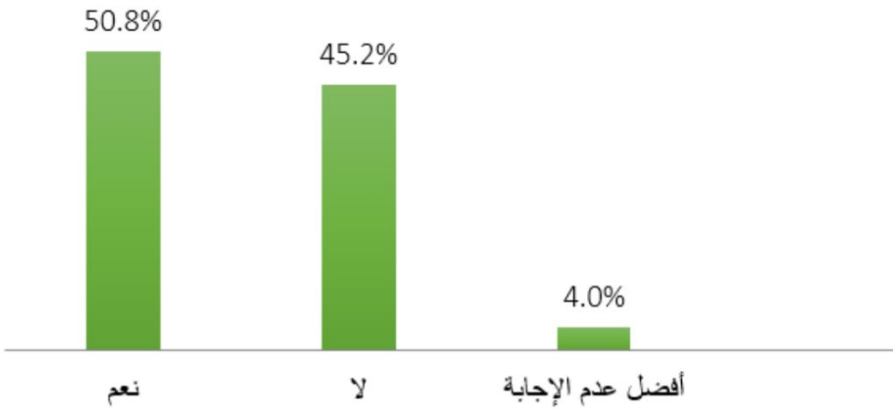
وأخيرًا هجمات/اعتداءات "الپورنو الانتقاميّ" – المقصود: نشر صور أو مقاطع ڤيديو ذات محتوى جنسيّ صريح دون رضا الضحية التي تظهر في هذه الموادّ، أو نشر وتوزيع الصور والڤيديوهات الحميميّة، الجنسيّة، أو الإباحيّة للأفراد دون موافقة منهم- كانت بنسبة 8.5%.

تشير النتائج إلى بروز الهجمات المرتبطة بفئات انتحال الشخصيّة، التحرّش والإساءة عبر المنصّات، وهو ما أكّدت عليه المجموعات البؤريّة، ولا سيما في صفوف الطلبة في المرحلة الثانويّة والجامعات. علاوة على ذلك، ركّزت المجموعات في نقاشها على الاعتداءات التي ترتبط بجهات أمنيّة إسرائيليّة وتهديدات أمنيّة بالاعتقال، وممارسة سياسات محاربة المحتوى الرقميّ الفلسطينيّ في المنصّات الرقميّة المختلفة.

5. المساءلة والتحقيق من قِبَل جهات أمنيّة

5.1 المساءلة أو التحقيق من قِبَل السلطات الإسرائيليّة حول منشورات "التعبير عن الرأي"

الشكل (24): نسبة المستطلَعين (أو شخص يعرفونه) الذين أُستدعوا للتحقيق من جهات أمنيّة إسرائيليّة



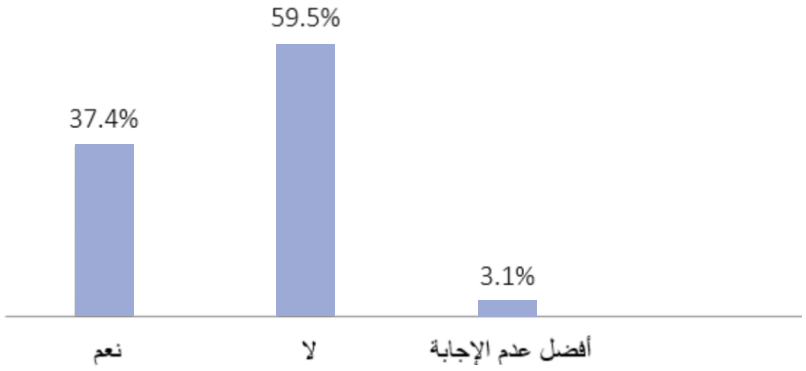
يتبيّن من النتائج أنّ نحو نصف المستطلَعين (51%) أو فرد من محيطهم الاجتماعيّ أُستدعوا للتحقيق أو المساءلة من قبل السلطات الإسرائيليّة بسبب منشورات عبر منصّات التواصل الاجتماعيّ. تُعتبر هذه النسبة نسبة مرتفعة مقارنة مع السنوات الماضية،[36] وتعكس تصاعد حدّة سياسات القمع والملاحقة التي تمارسها السلطات الإسرائيليّة تجاه الناشطين الفلسطينيّين. يمكننا التعامل مع هذه النتائج على أنّها مؤشّر لمستوى عدم الأمان والخوف اللذين يعتريان المستخدمين عند كلّ نقر أو نشر عبر منصّات التواصل الاجتماعيّ. هذا خرق صارخ للحقّ في حريّة التعبير، بما في ذلك التعبير الرقميّ والتفاعل مع المنشورات السياسيّة، ولا سيما المتعلّقة بممارسات السلطات الإسرائيليّة الاحتلاليّة في الضفّة الغربيّة والقدس. ومن أساليب القمع التي استخدمتها السلطات الإسرائيليّة (ضبّاط إسرائيليّون) كانت إرسال رسائل نصيّة لهواتف فلسطينيّين، فيها أمر بعدم دخول مدينة القدس وإلغاء التصاريح التي يحملونها لزيارة المدينة بحجّة نشرهم "محتوى تحريضيّ، ودعم حركة حماس عبر شبكات التواصل الاجتماعيّ"، حسب ما جاء في الرسالة.

من بين الأسباب التي أسهمت في تزايد حدّة سياسات القمع والملاحقة تجاه الناشطين رقميًّا، هو نجاح الفلسطينيّين في حملاتهم الرقميّة عام 2021 خلال هبّة الشيخ جراح. إذ استطاعت ونجحت الحملات والنشاطات الرقميّة بموضعة قضيّة الحيّ وتهويد المكان في قمّة اهتمام الرأي العام المحلّيّ والعالميّ.

36. الرجوب، عوض. (2023، نوفمبر). **هكذا ينتهك الاحتلال خصوصيّة الفلسطينيّين.. تتبّع حساباتهم والنشر عليها**. شبكة الجزيرة.

5.2 المساءلة أو التحقيق من قبل أجهزة السلطة الفلسطينيّة الأمنيّة حول منشورات "التعبير عن الرأي"

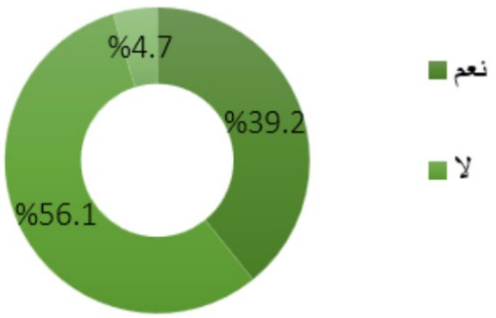
الشكل (25): نسبة المستطلَعين (أو شخص يعرفونه) الذين أُستدعوا للتحقيق من جهات أمنيّة فلسطينيّة



تُظهر النتائج أنّ 37% من المستطلَعين تعرّضوا شخصيّا أو أحد معارفهم للمساءلة والتحقيق من قبل جهات أمنيّة فلسطينيّة بشأن نشاطهم الرقميّ. نرى أنّ هذه النسبة قريبة نوعًا ما مع نسبة الملاحقين من قبل الأجهزة الأمنيّة الإسرائيليّة. هذا المعطى يشير إلى تصاعد سياسات القمع التي تنتهجها السلطات الأمنيّة الفلسطينيّة، من جهة؛ ويشير إلى حالة الخوف وعدم الأمان التي يعيشها الناشطون الفلسطينيّون منذ بدء الحرب على غزّة، من جهة أخرى. وكان من المتوقّع أن تكون الجهات الفلسطينيّة هي الحامية للمستخدمين الفلسطينيّين . أكّد المشاركون على هذه الحالة في المجموعات البؤريّة، ولا سيما مجموعة الناشطين والعاملين في المؤسّسات المهتمّة بالحقوق الرقميّة.

5.3 ضغوط من دوائر اجتماعيّة لحذف منشورات تعبّر عن آراء سياسيّة أو اجتماعيّة

الشكل (26): التعرّض لضغوطات لحذف منشورات سياسيّة أو اجتماعيّة



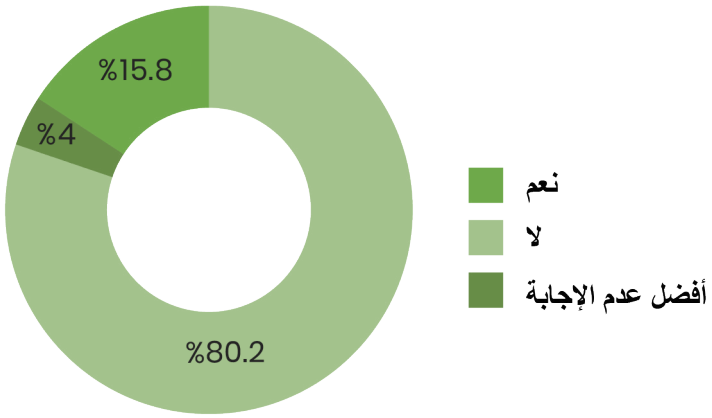
يَظهر من النتائج أنّ نحو 39% من المستطلعين خضعوا لضغوطات من محيطهم القريب لحذف منشورات سياسيّة واجتماعيّة.

وتبدو النتائج في الجدول صادمة من ناحية ارتفاع نسبة من تعرّضوا للضغوطات من أجل حذف منشورات ذات طابع سياسيّ أو اجتماعيّ، وهي تؤشّر إلى مكمن خطير مرتبط بسياسات القمع والمنع وتعزيز ثقافة الخوف، المنبثقة من أقارب من العائلة أو الدوائر الاجتماعيّة القريبة.[37]

سعى النقاش في المجموعات البؤريّة إلى معرفة الأسباب التي تعزّز المساءلة والمراجعة والضغوطات الصادرة من المحيط الاجتماعيّ (سياسيًّا واجتماعيًّا)، وتبيّن أنّ ثمّة سببيْن أساسيّيْن يدفعان إلى تكريس الضغط والرقابة الاجتماعيّة من أجل الحدّ من قدرات التعبير والمشاركة السياسيّة عبر الشبكة: الأوّل، ضغوط جهات أمنيّة فلسطينيّة تدفع إلى تعزيز الرقابة الذاتيّة المتمثّلة بالأقارب والأصدقاء، لا سيما مَن هم أكبر سنًّا؛ والسبب الثاني، يرتبط بتزايد احتمالات المخاطر السياسيّة والأمنيّة الصادرة من سلطات الاحتلال الإسرائيليّة، وتحديدا بعد السابع من أكتوبر 2023.

5.4 ضغوط من دوائر أمنيّة فلسطينيّة لحذف المنشورات السياسيّة أو الاجتماعيّة

الشكل (27): التعرّض لضغوطات رسميّة فلسطينيّة لحذف منشورات سياسيّة أو اجتماعيّة



بحسب النتائج، يظهر أنّ الدوائر الأمنيّة الفلسطينيّة الرسميّة مارست الضغوطات على المستطلَعين لحذف منشوراتهم بنسبة 15.8%، بينما أجاب نحو 80% منهم أنّه لم تمارس عليهم ضغوطات رسميّة لحذف منشوراتهم.

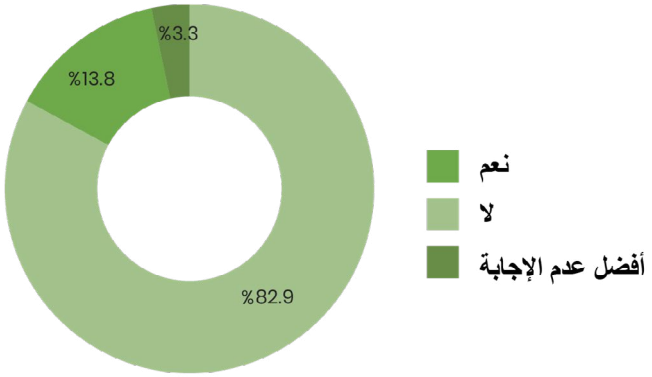
تعكس هذه النتيجة عند قراءتها مع نتائج سابقة تصعيدًا في سياسات الضغط على المواطنين، من أجل كبح مظاهر التعبير عن المواقف السياسيّة والاجتماعيّة. ونستدلّ في هذا السياق، من النقاشات في المجموعات البؤريّة أنّ الأجهزة الأمنيّة الفلسطينيّة لا تمارس ضغوطًا مباشرة على الشبّان والناشطين، فهي

37. للاستزادة انظروا:
مركز حملة. (2017). **الأمان الرّقميّ والشّباب الفلسطينيّ في مناطق الضفة الغربيّة وقطاع غزّة وأراضي 48، مسح ميدانيّ**.
بيرقدار، مهند. (2020). **الأمان الرقميّ للشباب المقدسيّ.. هاجس الملاحقة وغياب المرجعيّات**. حيفا – رام الله: حملة- المركز العربيّ لتطوير الإعلام الاجتماعيّ.

تلجأ في بعض الأحيان إلى الدوائر الاجتماعيّة القريبة من الناشط (أب، أخ، عمّ، خال، زوج، صديق.. إلخ) من أجل التأثير والضغط عليه لحذف المنشورات والتوقّف عن إبداء الرأي في القضايا السياسيّة الفلسطينيّة الداخليّة. وبحسب أقوال بعض المشاركين في المجموعات "إنّ هذه الممارسات أكثر فعاليّة من فكرة استدعائهم للتحقيق أو الطلب منهم مباشرة بحذف المنشورات أو التوقّف عن الكتابة في مواضيع محدّدة من الأجهزة الأمنيّة".

5.5 ضغوطات من دوائر أمن إسرائيليّة لحذف منشورات أو محتويات سياسيّة

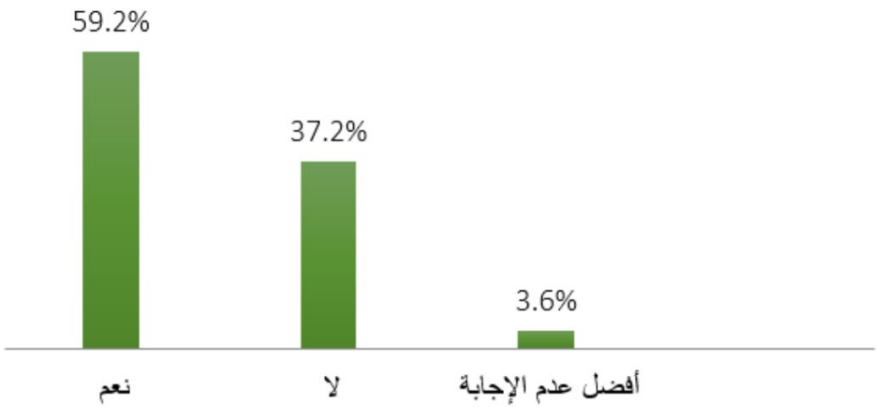
الشكل (28): التعرّض لضغوطات أمنيّة إسرائيليّة لحذف منشورات سياسيّة أو اجتماعيّة



تُظهر النتائج نسبة من تعرّضوا شخصيًّا لضغوطات أمنيّة إسرائيليّة مباشرة لحذف منشورات ذات طابع سياسيّ (13.8%). واللافت في هذه النسبة أنّها قريبة من نسبة المستطلَعين الذين تعرّضوا لضغوطات مثيلة من الأجهزة الأمنيّة الفلسطينيّة. إلى جانب ذلك، وجب تسليط الضوء على الفرق في إجابات المستطلعين التي وردت في البند 5.1، والذي تناول التعرّض للمساءلة والتحقيق من قِبَل جهات أمنيّة إسرائيليّة شخصيًّا أو يعرف فردًا تعرّض للمساءلة والتحقيق (51%). السؤال الذي علينا أن نطرحه، ما مدى إسهام هذا الفارق في تعزيز الخوف والرقابة الذاتيّة لدى المستخدِمين؟

5.6 الرقابة الذاتيّة

الشكل (29): مدى ممارسة الرقابة الذاتيّة

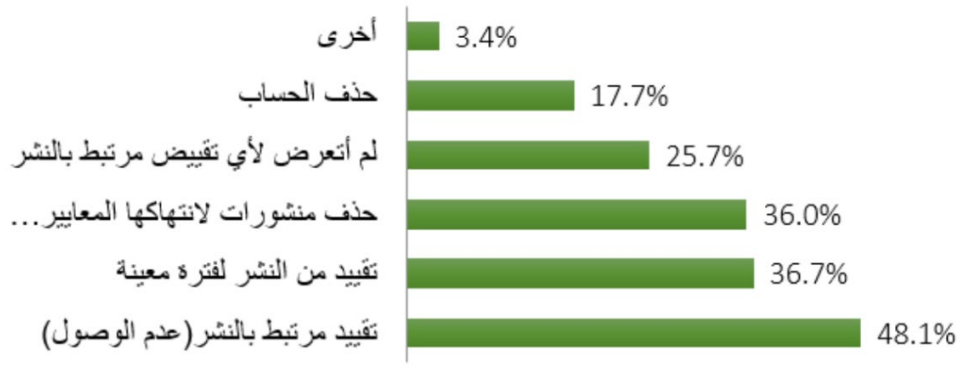


يتبيّن من النتائج أنّ نحو 60% من المستطلَعين يمارسون رقابة ذاتيّة عند النشر عبر منصّات التواصل الاجتماعيّ. وعلى ما يبدو أنّ هذه النتائج هي حصاد سياسات القمع الرقميّ والضغط الأمنيّ والاجتماعيّ (إسرائيليًّا وفلسطينيًّا) التي رأينا علامتها وتأثيرها في البنود السابقة. تؤكّد هذه النتائج مدى صواب استنتاجات تحليل بيانات هذه البحث، التي تشير إلى ازدياد المخاوف والقلق عند المستخدِمين الفلسطينيّين ولا سيما فئة الشباب.

6. أثر سياسات منصّات التواصل الاجتماعيّ على نشاط الشباب الفلسطينيّ منذ بدء الحرب على قطاع غزّة

6.1 تقييدات فُرضت على الحسابات من قِبَل شبكات التواصل الاجتماعيّ

الشكل (30): أنواع التقييدات التي فُرضت على حسابات المستخدِمين الشخصيّة من قِبَل شبكات التواصل الاجتماعيّ



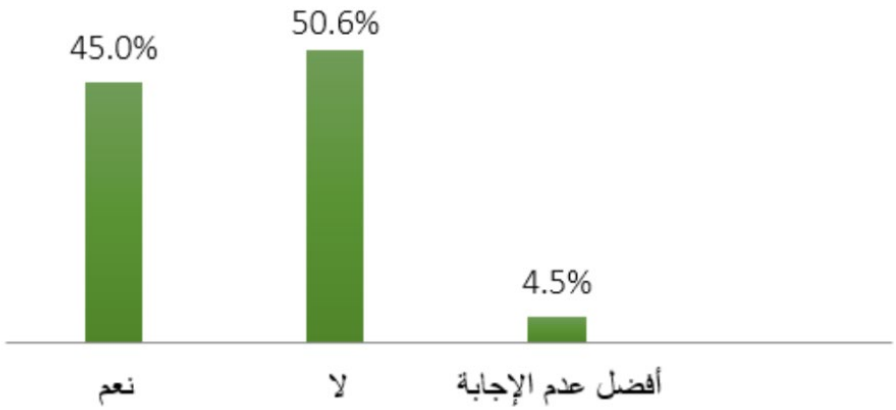
خُصّص هذا السؤال للتقييدات التي تعرّضت لها حسابات المستخدِمين في الشهور الثلاثة الأولى من بدء الحرب على غزّة، وكان على المستطلَعين أن يختاروا نوع التقييدات التي فُرضت على حساباتهم. تبيّن النتائج أنّ 48% منهم قالوا إنّ منشوراتهم خضعت لتقييدات في الوصول لشريط الأخبار والأصدقاء؛ وأجاب 36% منهم أنّهم تعرّضوا لتقييد نشر؛ ونسبة شبيهة قالوا إنّ منشوراتهم حُذفت بادّعاء انتهاك معايير المنصّات وسياساتها؛ فقط 25% قالوا إنّهم لم يتعرّضوا لأيّ تقييد أو حذف، بينما أجاب 17.7% أنّ حساباتهم الخاصّة قد حُذفت.

تُظهر قائمة الانتهاكات أعلاه أنّ التقييدات الأكثر شيوعًا كانت المرتبطة بالنشر، نتج عن هذه التقييدات عزوف عن المشاركة والكتابة والنشر في ظلّ سياسات القمع التي مارستها شركات التواصل الاجتماعيّ على المستخدِمين الفلسطينيّين، فضلًا عن السياسات الأمنيّة الإسرائيليّة والفلسطينيّة القامعة التي مورست بحقّ الناشطين في القدس والضفّة الغربيّة. وظهرت خلال هذه الفترة أشكال جديدة من الملاحقة الاحتلاليّة بحسب ما ظهر في النقاش مع المجموعات البؤريّة مثل: فحص الأجهزة الحديثة على الحواجز والدخول إلى تطبيقات المراسلة، وسُجّلت في ذات الفترة اعتقالات وملاحقات واعتداءات بحقّ

مواطنين من قِبَل جنود إسرائيليّين على الحواجز المختلفة، وهو ما عزّز من مشاعر الخوف واختيار العزوف عن النشر كما ستقدّم النتائج في البند التالي.[38]

6.2 تقييدات النشر عبر المنصّات وأثرها على التفاعل مع الأحداث السياسيّة

الشكل (31): مدى تأثير تقييدات النشر على التفاعل مع الأحداث السياسيّة منذ بدء الحرب على غزّة



بهدف معرفة أثر القيود الرقميّة التي فرضتها المنصّات على المستطلَعين قُرأت عليهم المقولة التالية: "تعرّضت حساباتي في شبكات التواصل الاجتماعيّ إلى تضييق مرتبط بالنشر، ما قلّل من تفاعلي مع الأحداث السياسيّة المختلفة، خلال الشهور الثلاثة الماضية" (بعد 7 أكتوبر 2023). اتّفق 45% منهم مع المقولة، فيما أجاب نحو 50.6% بـ"لا".

تعكس النتيجة تأثير سياسات المنصّات الرقميّة المنحازة للاحتلال الإسرائيليّ والمحارِبة للمحتوى الفلسطينيّ، فضلًا عن المخاوف المرتبطة بالملاحقة الأمنيّة الإسرائيليّة، على درجة تفاعل المستطلَعين مع الأحداث السياسية في غزّة والضفّة الغربيّة بعد السابع من أكتوبر العام الماضي.

عكست المجموعات البؤريّة الخمس هذه النتيجة، حيث أكّد نحو 90% من المشاركين في المجموعات تراجع نشاطهم عبر المنصّات التي يستخدمونها بكلّ ما يخصّ الشأن السياسيّ واقتصاره على المتابعة دون النشر أو المشاركة. وبدا ذلك واضحا من خلال النقاشات داخل المجموعات البؤريّة، ولا سيما، مع المجموعة الخامسة التي خصّصت للناشطين والمؤسّسات ذات الاهتمام بالحقوق الرقميّة. فقد أكّد المشاركون أنّهم يلمسون تصعيدًا حادًّا في سياسات التضييق على المنصّات الرقميّة بشكل عام وهو ما تثبته نتائج المسح الميدانيّ.

38. مركز حملة. (2023، نوفمبر). **الحقوق الرقميّة الفلسطينيّة تحت الحرب: قمع الأصوات، تضليل وتحريض**. **ورقة إحاطة**.

نقاش، استنتاجات عامّة وتوصيات

تسلّط هذه الدراسة الضوء على مشهد الأمان الرقميّ في الضفّة الغربيّة والقدس من خلال اقتفاء أثار تجارب مستخدمي شبكة الإنترنت الفلسطينيّين. تأتي هذه الدراسة في مرحلة غاية في الحساسيّة والاضطراب والتحوّل، وبغية استخلاص استنتاجات لها مصداقية؛ استخدمت الدراسة طريقتين لجمع البيانات وهما: المجموعات البؤريّة، والمسح الميدانيّ (استطلاع الرأي).

أظهرت النتائج التي عرضتها الدراسة أنّ قضيّة الأمان الرقميّ، في السياق الفلسطينيّ، أصبحت مركّبة ومعقّدة وتراكميّة في ظلّ اختلاف الجهات التي تنتهك الحقوق الرقميّة الفلسطينيّة، وتنوّع مصادر التهديدات الرقميّة. فقد وجدت الدراسة أنّ الاحتلال الإسرائيليّ، المنصّات الرقميّة، والجهات الفلسطينيّة الرسميّة، إلى جانب الأفراد والشركات التجاريّة الخاصّة، كلّها تنتهك الحقوق الرقميّة وبعضها بات مصدرًا للتهديد والابتزاز.

حملت نتائج الدراسة مؤشّرات قويّة على وجود فجوة عميقة من المعرفة والوعي بقضايا وممارسات الأمان الرقميّ عند المستخدِمين، جعلتهم عرضة للهجمات والتهديدات الرقميّة المتنوّعة. واتّضح من النتائج أنّ ثمة نقصًا في المعرفة والبناء المعلوماتيّ الأساسيّين لضمان الحدّ الأدنى من الأمان الرقميّ عند الشباب الفلسطينيّ، على سبيل المثال، ضعف المعرفة ببرامج التجسّس؛ وعدم استخدام أساسيّات الحماية الرقميّة (تغيير كلمة السر دوريًّا، تحديد إعدادات الأمان، إضافة أشخاص مجهولين، مشاركة صور وأمور شخصيّة، عدم استخدام وتشغيل برامج حماية للأجهزة الموصولة بالإنترنت).

بالتوازي، يدرك المستخدمون الفلسطينيّون أنّ الشبكة غير آمنة البتة، فهي تحتوي على مجموعة مخاطر تتعاظم عند تفاعل المستخدِمين مع الموضوعات السياسيّة (الوطنيّة المرتبطة بالاحتلال الإسرائيليّ)، ولا تختفي تلك المخاطر إذا تفاعل المستخدِمون مع مواضيع تتعلّق بالشأن الفلسطينيّ السياسيّ الداخليّ كذلك.

بيّنت النتائج أنّ التعرّض للتهديدات والهجوم الرقميّ دفع المستخدمين للتعلّم والتعرّف على سبل الحماية والوقاية من هذه التهديدات؛ بالمقابل، تبيّن أنّ مجموعة لا بأس بها من المستخدمين ليس لديها أيّ معرفة ببرامج الحماية. لكنّ المشترك لهذه المجموعات هو شعور الخوف والقلق والتوتّر وعدم الأمان، وتبيّن أنّ هذا الشعور كان أحد الدوافع للرقابة الذاتيّة عند المستخدمين، يضاف له ممارسات الضغط الاجتماعيّ لكتم صوت المستخدِمين وحذف منشوراتهم. يعكس الواقع السياسيّ المتشظّي والهجين فلسطينيًّا، غياب الحرّيّات، وسيادة سياسات تكميم الأفواه عبر نصوص قانونيّة أو ممارسات أمنيّة، حالة أصبحت مستدامة كرّست غياب الحقوق الرقميّة وفقدان الأمان في البيئات الرقميّة، لقد ذكر نحو 60% من المستطلَعين أنّهم يمارسون الرقابة الذاتيّة على أنفسهم، وذَكر أكثر من نصفهم أنّهم تعرّضوا لضغوطات من دوائر اجتماعيّة لحذف منشورات سياسيّة واجتماعيّة.

أشارت النتائج إلى مشكلة اجتماعيّة تُضرّ بمستخدمي الإنترنت، وتُفاقم أزمة الثقة التي يعانون منها، فمن جهة وجدنا أنّ إحدى جهات الاعتداء (ابتزاز، تحرّش، انتحال شخصيّات، الترصّد والملاحقة الإلكترونيّة) هم

أفراد من دوائر اجتماعيّة محيطة بالمستخدِمين، ومن جهة أخرى لا ثقة كافية لدى الضحايا باللجوء لجهات الاختصاص الرسميّة للتعامل مع المعتدين ومعاقبتهم إن لزم الأمر، ووجدنا أنّ خيار المستخدِمين الأخير هو التوجّه للشرطة بصفتها جهة تنفيذ القانون، وعادة ما يفضّلون اللجوء للأهل والأقارب.

وكشفت النتائج أنّ نسبة عالية (نحو 50%) من المستخدِمين تعرّضوا شخصيًّا للمساءلة والتحقيق من جهات أمنيّة إسرائيليّة أو سمعوا عن حالات تحقيق ومساءلة من جهات أمنيّة إسرائيليّة. ونسبة لا بأس بها (ما يربو عن ثلث المستطلَعين) قالوا إنّهم تعرّضوا شخصيًّا أو سمعوا عن أفراد تعرّضوا للتحقيق والمساءلة من قبل جهات أمنيّة فلسطينيّة.

في النهاية، أظهرت النتائج أنّه مع بدء الحرب الإسرائيليّة على قطاع غزّة بعد السابع من أكتوبر 2023 دخلت الحالة الرقميّة الفلسطينيّة إلى واقع جديد، من حيث ممارسات المنصّات الرقميّة بحقّ المحتوى الرقميّ الفلسطينيّ وسياسات الرقابة وتقليل الوصول، وحذف المنشورات، وهو ما أدّى إلى تراجع مشاركة الشباب السياسيّة الفعّالة في الشبكات الاجتماعيّة.

مقترحات ومساحات للعمل:

من وحي نتائج الدراسة الميدانيّة والنقاشات مع المجموعات البؤريّة خلصت الدراسة إلى مجموعة من الاقتراحات للعمل ويمكن إيجازها على النحو التالي:

أوّلا: مؤسّسات المجتمع الفلسطينيّ

* يعتبر الفضاء الرقميّ مساحة لا غنى عنها للفلسطينيّين بجميع فئاتهم، وتحديدا فئة الشباب، وهي مساحة يتضاعف الحديث عنها مع كلّ مواجهة مع سلطات الاحتلال الإسرائيليّ، ومن هذه الحقيقة وفي ظلّ ما أصاب المشهد الرقميّ الفلسطينيّ من حالات قمع وتنامي الهجمات الرقميّة وسياسات الملاحقة وانحياز المنصّات ومعاداتها للخطاب الحقوقيّ الفلسطينيّ، هناك مكان لعمل مؤسّساتيّ جماعيّ وجمعيّ لمكافحة سياسات القمع والتصدّي على الصعيدين المحلّيّ والعالميّ، من خلال المشاركة الفعّالة في مجموعات حقوقيّة وتفعيل مواقع بديلة، بغية تقديم مقاربة نضاليّة رقميّة جديدة.

* **ثمّة ضرورة لأن تكون تكامليّة في الجهود المبذولة في تقديم الدعم المهنيّ ما بين الخطوط التقنيّة والنفسيّة والقانونيّة**، من أجل توفير دعم مباشر وفوريّ للمواطنين على مدار الساعة، وعلى امتداد الجغرافيا الفلسطينيّة (الضفّة الغربيّة، القدس، قطاع غزّة، فلسطينيّي ال 1948)، مع الأخذ بالحسبان خصوصيّة كلّ منطقة منها.

* في ظلّ قلّة المؤسّسات العاملة في مجال الأمان الرقميّ (الثقافة الرقميّة عمومًا) وكذلك المتخصّصين والخبراء في هذا المجال، ثمّة حاجة إلى تكامليّة في أنشطة وبرامج المؤسّسات العاملة، وتكثيف في أنشطة الائتلاف الوطنيّ للتربية الإعلاميّة، **للتركيز على زرع وتنمية مفاهيم الأمان الرقميّ والحقوق الرقميّة**. المحدوديّة في المؤسّسات والإمكانيّات تعزّز فكرة الائتلاف الجامع، وتقاسم المهامّ والتخطيط

المشترك. وفي ظلّ عدم قدرة جهة فلسطينيّة واحدة تَحمّل جميع متطلّبات العمل على الجهد التوعويّ والتثقيفيّ لفئات المجتمع كافّة، تتعمّق الاعتداءات والانتهاكات للحقوق الفلسطينيّة التي بدأت تتغلغل لتطبيقات الذكاء الاصطناعيّ. هذا الواقع **أصبح يفرض تكاملًا في العمل والمهامّ، ويستدعي فتح خطّ نافذ وتعاون مستمرّ مع الجهات الرسميّة الفلسطينيّة أيضا**.

ثانيا: الشباب

هناك ضرورة لتجاوز الأنشطة التوعويّة في موضوعات وقضايا الأمان الرقميّ، فهي ليست الخيار الوحيد، **فهناك أهميّة للتفكير بإنشاء مؤسّسات تعنى بالجرائم الإلكترونيّة و الحقوق الرقميةّ، وهو ما يفرض ضرورة تشكيل مجموعات شبابيّة أهليّة مستقلّة تعمل على بناء اختصاصات للعمل في كلّ ما له علاقة بالنشاط الرقمية**.

ثالثا: السلطة الفلسطينيّة

* من وحي النتائج، ثمّة ضرورة لأن يستجيب المنهاج الفلسطينيّ والقائمون عليه للواقع الرقميّ الراهن وتحوّلاته، فالتربية للأمان الرقميّ مسألة يفترض أن تكون على رأس سلّم التحديثات في ظلّ تطوّر وسرعة ابتكار طرق الهجوم والاعتداء، وهو ما يفترض أن يقابله تطوّر وسرعة في ابتكار طرق الحماية وتوفير الأمان. وهذا ما يستوجب توعية وتثقيفًا مبرمجًا، وطرح مناهج مرنة تمتلك القدرة على إجراء التعديلات **في حقل يشهد تسارعًا وتقدّمًا لا مثيل لهما**.

* في ظلّ تصاعد الهجمات الرقميّة وتوسّع رقعتها، يفترض على الأجهزة الأمنيّة الفلسطينيّة (الشرطة) أن تطوّر من طريقة عملها وأدواتها التقنيّة، لبناء جسر من الثقة مع الشباب الفلسطينيّ، فالهجمات الرقميّة تتزايد كمًّا وكيفًا، ومعها تزداد المخاطر والتهديدات في ظلّ تزايد حضور الفلسطينيّين عبر الشبكة.

*

رابعا: الجهات المانحة والمجتمع الدوليّ

* على ضوء تعقيدات مشهد الأمان الرقميّ في المجتمع الفلسطينيّ وتداخل عوامل كثيرة في مسبّبات الانتهاكات والاعتداءات الرقميّة، يُفتَرض أن تتعاطى الجهات المانحة والمجتمع الدوليّ مع هذه الخصوصيّة، سواء من حيث الوعي بطبيعة البيئة المعقّدة المعزّزة لحالة فقدان الأمان الرقميّ، أو من حيث مساحات العمل والاشتغال من أجل تعزيز الحقوق الرقميّة وتكريسها، وهي مسألة تفرض أنشطة ومقاربات عمل محلّيّة خاصّة تتعاطى مع هذه الخصوصيّة وتنطلق منها إلى تمويل ودعم وإقامة حملات وخطط عمل لبيئة رقميّة تنمو باضطراد كبير، أو من خلال حشد دعم دوليّ يدفع لتعزيز سياسات الأمان الرقميّ.

اتصلوا بنا:

info@7amleh.org | www.7amleh.org

Find us on social media : **7amleh**