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

دراسة استكشافيّة:

واقع الخصوصية وحماية البيانات الرقميّة في فلسطين

آب 2021

دراسة استكشافية: واقع الخصوصيّة وحماية البيانات الرقميّة في فلسطين

الباحث: د. عمر أبو عرقوب

تحرير الدّراسة: منى شتية، وإيناس خطيب

نقله إلى الإنجليزية: شركة رتاج للحلول الإدارية

تدقيق لُغوي: شركة رتاج للحلول الإداريّة

تصميم: أمل شوفاني

صدر هذا البحث بتمويل من الممثّليّة النرويجيّة.

The Representative Office of Norway
to the Palestinian Authority

فهرس

الملخّص التّنفيذي

تسعى هذه الدراسة إلى التعرّف على واقع الخصوصيّة وحماية البيانات الشخصيّة الرقميّة في فلسطين[1]، من حيث جمع ومعالجة واستخدام بيانات المستخدمين الفلسطينيّين، وتتطرّق إلى بعض الانتهاكات الحقوقيّة، التي يتعرّض لها المستخدمون الفلسطينيّون والجهات الأساسيّة، الذين تُنتهك بياناتهم، إلى جانب التعرّف على الملامح والمبادئ الأساسيّة، لقانون الخصوصيّة وحماية البيانات المنشود فلسطينيًّا.

استخدِمت في إعداد هذا البحث آليّة البحث النّوعي، من خلال استخدام أداتين لجمع وتحليل البيانات: الأولى، المجموعات المركّزة، التي شاركت فيها ثلاث مجموعات موزعة جغرافيًّا، الضفة الغربيّة، وقطاع غزة، وشرقيّ القدس، وقد تراوحت أعداد المشاركين فيها من 14- 16 مشاركًا. والأداة الثانية، كانت المقابلات الشخصيّة المعمّقة لأصحاب العلاقة والخبرة والمعرفة بالقضيّة المبحوثة لعينّة من 12 مفردة.

أظهرت المجموعات المركّزة أن مفهوم الخصوصيّة والبيانات الشخصيّة يعدّ لديها حديثًا نسبيًّا، وليس معروفًا بأكمله، عند جميع الفئات لا سيما في القدس، وأنّ ثمّةَ حاجةً إلى جهود للتعريف به وبأهميّته.

وهذا ما نعدّه سببًا أساسيًّا في تدنّي نسبة من يقرأون ويَطّلِعون على سياسات الخصوصيّة، في المواقع والتطبيقات والخدمات قبل استخدامها أو يتأثرون بها، في حين أن غالبية المشاركين لا تختلف على ضرورة وأهمية سَنّ قانون فلسطينيّ شامل، للخصوصيّة وحماية البيانات، يطبّق في كلّ المناطق الفلسطينيّة، ويكون هدفُه الأساسيّ حمايةَ بيانات الفلسطينيّين، ومنعَ انتهاك خصوصيتهم.

من جهة أخرى، ولخصوصيّة الظرف السياسيّ والأمنيّ والحقوقي، المرتبط بالقضيّة الفلسطينيّة وأبعادها، تتنوّع الجهات، التي تسعى لانتهاك واختراق خصوصيّة الفلسطينيّين وبياناتهم الخاصة، حسب ما أشار إليه المشاركون في المجموعات المركّزة، وحتّى المقابلات الشخصيّة؛ حيث يمكن ترتيبها على النحو الآتي: الاحتلال الإسرائيليّ، السّلطة الفلسطينيّة، شركات القطاع الخاص، وجِهات خارجيّة، مثل، مِنصّات التواصل الاجتماعيّ العالميّة، كشركة فيسبوك، وتعدّدت الأهداف من هذه الانتهاكات ليكون أبرزها الأهداف الأمنيّة، ثم الأهداف السياسية، ثم الأهداف التجارية والإعلانية.

وقد أبدى غالبية المشاركين، في المجموعات المركّزة والمقابلات المعمّقة، بجميع تصنيفاتهم ومناطقهم الجغرافيّة، اهتمامًا بالغًا بأهمية سنّ قانون وتشريع فلسطينيّ، خاصٍّ بحماية خصوصيّة وبيانات الفلسطينيّين، تشترك جميع مؤسّسات المجتمع المدنيّ وفئاته، وبالعمل مع الجهات الحكوميّة والجهات القانونيّة، على دعم سنّ هذا القانون واعتماده في كافة المناطق الفلسطينيّة. وكان التّركيز على دور المجتمع المدنيّ الفلسطينيّ الاستباقيّ في عملية التّوعية المجتمعيّة للقانون، ولأهميّة الخصوصيّة وحماية البيانات الشخصيّة، على المستويين الشعبيّ والرسميّ. وهي الخطوة التأسيسيّة الأولى لمرحلة سنّ القانون، حيث تجب توعية المواطنين بالخصوصيّة، وحماية البيانات، في ظلّ العصر الرقميّ، قبل سَنِّ القانون، وفي ظلّ تدني نسبة مَن يعرفون مفهوم الخصوصيّة، والبيانات الشخصيّة جيّدًا.

ويمكن مقارنة ذلك بتصوّرات المواطنين الأوروبيّين، عن الخصوصيّة وحماية البيانات، من خلال استطلاعات للرّأي، حول توجّه الرأي العام الأوروبيّ، فيما يتعلّق بالخصوصيّة، وحماية البيانات، خلال العام (2012)، حيث أظهرت النتائج أن المواطنين الأوروبيّين على وعي بالمبادئ الأساسيّة لمفهوم الخصوصيّة وحماية البيانات، إلا أنّ الوعيَ بالجوانب العميقة للخصوصيّة، وكونها حقًّا فرديًّا ومبدأً اجتماعيًّا، كان نادرًا، وأنّ الغالبيّة العظمى من الأوروبيّين فقدت السّيطرة على بياناتها الشخصيّة، إلى جانب اعتقادها أنّ بياناتها غير محميّة، وهو ما يحتاج إلى قوانين ناظمة.[2]

1. المقصود بفلسطين في هذا التقرير، الضفة الغربيّة وقطاع غزة وشرقيّ القدس.

2. Hallinan, Dara, Friedewald, Michael, & McCarthy, Paul. (2012). Citizens' perceptions of data protection and privacy in Europe. **Computer Law and Security Review**, 28(3). Pp. 263–272. https://doi.org/10.1016/j.clsr.2012.03.005

وقد ظهر من خلال المقابلات المعمقة أنّ هناك جهاتٍ عدّةً، قد تعمل على جمع البيانات الشخصيّة للفلسطينيّين، سواء خاصة أو عامة. وعلى الرّغم من أنه ليست لديها القدرة الكافية، تقنيًّا ولوجستيًّا على معالجة هذه البيانات وتحليلها، ضمن خوارزميات وتقنيات ذكاء اصطناعيّ، والاستفادة من مخرجاتها بالشّكل الأفضل، بَيْدَ أنّ الأمر، خلال السّنوات القادمة، قد يصبح سهلًا ومتاحًا للجميع، وأنّ القضيةَ قضيّةُ وقت، حتّى يصبح لدى هذه الشركات والجهات القدرة على ذلك، لأنّ هذا المستوى من التّحليل والمعالجة مستخدم في كبرى الشركات العالميّة، مثل فيسبوك وغيرها. وحتّى لا تُخلَق فوضى من تحليل بيانات وسلوك المستخدمين، فمن الضروريّ توفير قانون ناظم يدير ويحمي خصوصيّة المستخدمين الفلسطينيّين ويكون بمثابة الخطوة الأساسيّة، الّتي يجب أن يُبنى عليها المسموح والممنوع، في إطار جمع ومعالجة واستخدام البيانات.

وفي السياق ذاته، لا بدّ من أن تكون سياسات الخصوصيّة الخاصة بالشركات والجهات المختلفة، التي يجب أن يوافق عليها المستخدمون والمشتركون واضحة، ومنسجمة مع القانون ذاته، وعلى القانون أن يفصّلها، بحيث يضع حدًّا لسياسات الخصوصيّة العشوائيّة، والمنسوخة من الإنترنت، أو التي تنتهك خصوصيّة الأفراد، بطرق ملتوية وغير مباشرة، وأن يصبح المعيار ليس فقط موافقة المستخدمين عليها، وإنما – أيضًا- أن تكون سياسات خصوصيّة تحفظ بيانات المستخدمين ولا تنتهكها.

واحدة من أكبر المشاكل والفجوات، التي تظهر في ظل غياب القانون، هي أنّ باب الاجتهادات، في قضيّة الخصوصيّة وحماية البيانات مفتوح، فليس مفهومًا ما هو مسموح أو ممنوع، من بيانات وكيفية تحليلها واستخدامها والاستفادة منها، وهو ما يجعل المستخدم الفلسطيني يتعامل مع سياسات خصوصية مختلفة لكل شركة و/أو جهة، بحسب ما تراه مناسبًا لها، ويلبّي احتياجاتها، الأمر الذي قد يضع هذه الجهات في موقع مساءلة ومحاسبة، إذا وقع منها خطأ فاضح، أو لم تلتزم بمعايير الخصوصيّة، غير المنصوص عليها محليًّا، لذلك نحن أمام مشكلة حقيقية.

وقد أظهر التقرير أن هناك الكثيرَ من المعلومات، التي لا تُصرّح الشركات بجمعها، وطبيعة استخدامها ومعالجتها وتبادلها، مع أطراف ثالثة داخلية أو خارجية، حيث إنّ هذه العملياتِ كلَّها تتمُّ في الخفاء وبشكل سرّي، وفي ظل عدم وجود جهة مسؤولة، عن رقابة ومتابعة هذه القضيّة، لا يمكن لنا معرفة إلى أيّ مدى يتمّ اختراق بياناتنا يوميًّا!

وقد بدا من الواضح التّعارُض في الأقوال بين أصحاب شركات القطاع الخاص، والجهات الحقوقية والمشاركين، في المجموعات المركّزة، الذين أشاروا على سبيل المثال، أنّ الجهات الأمنيّة الفلسطينيّة، سواء في قطاع غزة أو الضفة الغربيّة، لديها القدرة على الوصول إلى أية معلومات، لدى شركات القطاع الخاص، سواء كان ذلك بالطّرق القانونيّة أو من خلال التعاون مع هذه الجهات، واستخدام الطرق الخفيّة والمحسوبيّة والواسطة، لأهداف عامة أو شخصيّة. كما أن القوانين المقرّة، والمطبّقة في الضفة وغزة، تسهّل وتبسّط كلّ ذلك، وهذا الأمر بحاجة إلى مراجعة حقيقيّة ومصيريّة، للقوانين والأنظمة السابقة، بشكل جادٍّ، من أجل التّغيير، وجعلها متوائمة مع المعايير الدوليّة، ونخصّ هنا بالذِّكر (قانون الجرائم الإلكترونيّة).

تُبدي الوزارات والجهات المسؤولة عن متابعة قضايا الخصوصيّة، لدى شركات القطاع الخاص اهتمامًا بقضيّة الخصوصيّة، من خلال إيجاد أنظمة محوسبة، تحاول حمايةَ الخصوصيّة، والحفاظ عليها، وتَحُدُّ من إمكانية الوصول للبيانات والاطّلاع عليها. إلا أنّ ضوابط هذه الأنظمة المحوسبة تبقى ناقصة وغير دقيقة، أو مرتبطة بقانون يوضّح ما يجب أن تتيحه من معلومات وما يجب أن تحجبه، ومن لديه صلاحية الاطّلاع على هذه الأنظمة وبرمجتها وصيانتها.

وما زالت الجهات الحكوميّة والوزارات تعمل على الاجتهاد في هذا الأمر ليس أكثر، فغياب القانون الذي تستند إليه في كلّ ذلك يعتبر الثّغرة الكبرى، الّتي يمكن تمرير أيّ انتهاك للخصوصيّة من خلالها، فلا يمكن

الحديث عن قضيّة الخصوصيّة، في ظلّ عدم وجود جهة رقابية، تستند إلى القوانين والتّشريعات والمعايير والأحكام المقرّة قضائيًّا، في مراقبة بيانات الفلسطينيّين.

وقد أوصى التّقرير في النّهاية، بمجموعة من التّوصيات، مثل: تشكيل هيئة فلسطينيّة؛ لحماية وتنظيم الخصوصيّة والبيانات الشخصيّة، وضرورة إقرار قانون "الخصوصيّة وحماية البيانات الفلسطينيّ الشامل". وقد قدّم التقرير أهمَّ ملامح القانون الفلسطيني المنشود في هذا السياق، بالإضافة للتّشديد على أهمية التوعية بقضيّة الخصوصيّة وحماية البيانات في فلسطين، شعبيًّا ورسميًّا.

الباب الأول: المقدمة

أدّى التّطور التكنولوجيّ الهائل لوسائل الاتصال الرقميّ على شبكة الإنترنت، إلى توليد بيانات ضخمة (Big Data) للمستخدمين. هذا الكمّ الهائل من البيانات العامّة والشخصيّة، عن المستخدمين وتفاعلاتهم على شبكة الإنترنت، خلق ثروة جديدة باتت تعرف بالنّفط الرّقميّ (نفط البيانات الرقميّة). تستخدم المؤسسات والمنظمات الربحيّة والغير الربحيّة والخاصة والحكوميّة هذه البيانات بطرق شتى، حيث يتوقف مسار اتخاذ القرارات في هذه المؤسسات والمنظمات على البيانات المُوَلَّدة.

ليس بالضرورة أن يعود استخدام البيانات الشخصيّة بالنفع على الأفراد، وليس بالضرورة، أيضًا، أن يكون استخدامها ملموسًا وظاهرًا للعيان، وهنا تكمن مخاطر امتلاك والسيطرة على هذه البيانات.

تُجمع غالبية البيانات، دون ملاحظة أو موافقة صاحبها، وفي معظم الأحيان تشمل هويتهم ومعلوماتهم الشخصيّة، ومن ثم تحفظ وتُؤَرشف وتحلّل لتُستخدم حسب حاجة مالكها. وهذا ما يجعل الأفراد عُرضة لمخاطر حتميّة، في ظل غياب قانون يحميهم ويحمي خصوصيتهم، من جامعي البيانات، لا سيما في ظل غياب الحقّ في النّسيان الرّقميّ. وبالتّالي، أصبح لزامًا على الجهات الرسميّة والمختصة أن تتحرك؛ لحماية حقوق الإنسان وخصوصيّة المستخدمين، وتنظيم جمع واستخدام البيانات الشخصيّة للمستخدمين، بما يحفظ خصوصيّتهم ويمنع إساءة استخدامها أو استغلالها.

ليس بوسعنا فصلُ خصوصيّة وحماية البيانات الشخصيّة للمستخدمين عن مفهوميّ حقوق الإنسان والديمقراطيّة، حيث إنَّ خصوصيّة الأفراد وبياناتهم الخاصة مكفولة، في مواثيق واتفاقيّات حقوق الإنسان العالمية، وهو ما تنصُّ عليه المادة 12 من الإعلان العالمي لحقوق الإنسان بأنه "لا يجوز تعريض أحد لتدخُّل تعسُّفي في حياته الخاصة، أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص الحق في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات".[3]

علاوة على ذلك، تعدّ الاستقلالية والحرية الشخصيّة مبدأً أساسيًّا، حسب النظام الديموقراطيّ، وعليه فهو من أهم شروط وأساسيات الكفاءة للدّول الديمقراطية، فالخصوصيّة وحماية البيانات شرطان أساسيان للتفكير والتصرف المستقلّ والحرّ. ولهذا، من واجب الدساتير الديمقراطية حماية الخصوصيّةن وتشريع القوانين واللوائح، التي تحمي بيانات المستخدمين الشخصيّة والرقمية، التي تدفع باتّجاه حماية حقوق الإنسان في هدفها العام.4 في العام 2016 أقرّ الاتّحاد الأوروبي قانون الخصوصيّة وحماية البيانات، بعد مداولات وتعديلات حثيثة، بُدئ العملُ بهذا القانون عام 2018، يركّز القانون على معالجة البيانات الشخصيّة، وحدود حركة تلك البيانات، داخل وخارج الاتحاد الأوروبي، وما زالت باقي الدول متفاوتة في مسار إقرار قوانين مماثلة لديها.[5]

3. الأمم المتحدة. (1948، 10 كانون الأوّل). الإعلان العالميّ لحقوق الإنسان. منظمة الأمم المتحدة. ص2. تاريخ الاسترداد 2021.

4. Boehme-Neßler, Volker. (2016). Privacy: A matter of democracy. Why democracy needs privacy and data protection. **International Data Privacy Law**, 6(3). Pp. 222–229. https://doi.org/10.1093/idpl/ipw007

5. European Union. (2018). General Data Protection Regulation (GDPR). Retrieved May, 2021.

أمّا في فلسطين، فالقضيّة أكثر تعقيدًا، في ظلّ الاحتلال الإسرائيليّ، والتّعثّر السياسيّ الداخليّ، والانقسام الفلسطينيّ. هذه العوامل أدّت إلى تغييب سلطة مركزيّة مسؤولة، عن تنظيم حياة الأفراد وخصوصيّاتهم وحمايتها. وفي ظل غياب سلطة تشريعيّة فاعلة وُلدت الفوضى، التي سببت نوعًا من مشاعيّة البيانات الخاصة، وقدرة أيّ جهة كانت رسميّة، أو خاصة أو أمنيّة على استغلال بيانات المواطنين المتواجدين على الأراضي الفلسطينيّة، لانعدام إجراءات الخصوصيّة، وحماية البيانات فيها، ولقصور في القوانين والأنظمة والسّياسات المتعلّقة بها.

إنّ القوانين والأنظمة والسياسات الفلسطينيّة لا تزال قاصرة، فيما يتعلق بالخصوصيّة وحماية البيانات، والجرائم الإلكترونيّة المتعلقة بها، وإتاحة الحقّ في الحصول على المعلومات. وهو ما سبّب إشكاليّات حقيقيّة، تستحقّ تقييم الواقع واتّخاذ إجراءات وقوانين، تنظّم كلّ هذه المستجدّات، وهو ما تسعى هذه الدراسة لبحثه ومناقشته.

ترمي هذه الدراسة إلى التعرّف على واقع الخصوصيّة، وحماية البيانات الشخصيّة الرقميّة في فلسطين، من خلال مسح آليّات جمع البيانات، وكيفية معالجتها واستخداماتها؛ ومن ثمّ عرض الانتهاكات الحقوقيّة، التي يتعرض لها المستخدمون الفلسطينيّون، فيما يخصّ بياناتهم الشخصيّة، بهدف تسليط الضوء على الملامح والمبادئ الأساسيّة، التي على قانون الخصوصيّة وحماية البيانات الارتكازُ عليها.

الباب الثاني: مراجعة الأدبيّات

مفهوم الخصوصيّة والبيانات الشّخصيّة

الخصوصيّة هي حقّ الفرد في الحفاظ على معلوماته الشخصيّة، وحياته الخاصة، بشكل اختياري وحر، ومنع الحصول عليها بشكل غير طوعيّ. تشير الخصوصيّة إلى الحياة الخاصة، بما في ذلك البيانات الشخصيّة، على سبيل المثال، البيانات الطبيّة، والبيانات الخاصّة (الصّور والمحادثات)، والبيانات البنكيّة ومعلومات التواصل والاتصال، وغيرها من البيانات. وهي منظومة متكاملة ومتناسقة من الخصائص والسّمات الماديّة والروحيّة، وأسلوب الحياة والأخلاقيّات، ورؤية الذّات والآخر.[6]

فالخصوصيّة هي رسم للحدود، التي تنظّم قدرة المجتمع على التّدخل في حياة الأفراد، ولها أربعة حدود أساسيّة، الأول، خصوصيّة المعلومات الشخصيّة وجمعها ومعالجتها. الثّاني، خصوصيّة الجسد من التّدخل الفيزيائي. الثالث، خصوصيّة الاتصال والتّواصل وأمن المراسلات بكافة أشكالها. الرّابع، خصوصيّة الحيّز المكانيّ، الذي يتواجد فيه الفرد. وللخصوصيّة وجهان أساسيّان، الأول: الحقّ في حرية الحياة الخاصة. والثّاني: الحقّ في سريّة هذه الحياة.[7]

مع تطوّر تكنولوجيّا المعلومات، وما تبع ذلك من تطوّرات، طالت البيانات الضّخمة وشكلها ومجالات استغلالها، أصبحت مبادئ البيانات الضّخمة تتعارض مع مبادئ الخصوصيّة، وحماية البيانات الشخصيّة، كتلك التي أقرّها القانون العام الأوروبي لحماية البيانات.[8] وقد سرّع العصر الرّقمي من تآكل الخصوصيّة المعلوماتية للمستخدمين، على شبكة الإنترنت؛ حيث إنّ الكمّ المعلوماتيّ الهائل، المتوفّر في الفضاء الرقميّ، جعل البيانات تنتقل من الملكيّة الخاصة إلى الملكيّة العامة.

6. قوتال، ياسين. (2013). حق الخصوصيّة الإلكترونيّة بين التقييد والإطلاق. جامعة عباس لغرور. ص 56.
7. المصدر السابق.
8. Wolford, Ben. (2018). What is GDPR, the EU's new data protection law? Retrieved May, 2021.

تكمن خطورة هذه المعلومات، كالتي تجمعها مواقع التواصل الاجتماعي، في استخدامها لأغراض إجراميّة لإيذاء الآخرين أو لأغراض أمنيّة وعسكريّة في بعض الأحيان. وباعتبار الخصوصيّة حقًّا من حقوق الإنسان، وجزءًا من الحقوق الرقميّة، التي تشكّل امتدادًا لحقوق الإنسان في الفضاء الرقميّ، فإن مَن ينتهكها يكون عرضة للمساءلة القانونية، وبحسب معهد القضاء الأمريكي "كلُّ شخص يَنتهك، بصورة جديّة ودون وجه حقٍّ، حقَّ شخص آخر في ألّا تصل أموره وأحواله إلى علم الغير، وألا تكون صورته عرضة لأنظار الجمهور، يعتبر مسؤولا أمام المعتدى عليه".[9]

ويظهر الواقع أن انتهاك الخصوصيّة أمر مستمرّ، حتى في الدول الديمقراطية، التي تعمل وفق تشريعات لحماية الخصوصيّة، لغياب أدوات تطبيق القوانين، ففي الكثير من البلدان تعطى أجهزة الشرطة والأمن صلاحيات تفوق قوانين الخصوصيّة، ما يجعل الانتهاكات أمرًا سهلًا. أمّا في الدول العربية فالتّشريعات غير قادرة على مواجهة الانتهاكات الحاصلة على الحقِّ في الخصوصيّة، وهناك ضرورة للعمل على نشر الوعي الثقافيّ بالحق في الخصوصيّة، ومعانيه وتبيان أبعاده وأضراره.[10]

ارتبط مفهوم الجريمة المعلوماتيّة بما تتضمَّنُه وسائل الاتصال والإعلام، من بيانات ومعلومات، تُجمع وتُتَداول وتُخَزَّن وتُعالَج آليًّا ورقميًّا أو إلكترونيًّا. وهو ما سهّل وسرّع ووسّع الوصول إليها وقرصنتها واختراقها، وقد تكون هذه البيانات مرتبطة بدول وكياناتن أو بأفراد وأشخاص بعينهم، وهو ما دفع الدول والمجتمعات لإعادة النّظر بمنظومتها القانونيّة والتشريعيّة، وتجريم مثل هذه الأفعال. وبالتّالي أصبحت الجريمة المعلوماتية خطرًا يهدّد المجتمعات الحديثة والرقميّة، المعتمدة على استخدام شبكة الإنترنت والأجهزة الإلكترونيّة.[11] ويمكننا الإشارة إلى أنّ مخاطر الجريمة المعلوماتيّة لا تكمن في أجهزة الحاسوب والتّقنيات الرقمية ذاتها، فهي بطبيعتها محايدة إلا أنّ طريقة استعمالها أو استغلالها، هي التهديد الحقيقيّ في ظل عدم وجود تنظيمات وقوانين حديثة، تضبط استعمال هذه التقنيات.[12]

البيانات الشخصيّة

تُعرَّف البيانات الشخصيّة، حسب القانون الأوروبي للخصوصيّة وحماية البيانات (GDPR)، على أنّها أيّ معلومات ترتبط بالأفراد، نستطيع من خلالها التعرف عليهم بشكل مباشر أو غير مباشر، على سبيل المثال الاسم، الإيميل، العنوان، الموقع الجغرافيّ، العرق، الجنس، الصورة، الدّين، المعتقدات، معلومات التّصفح الخاصة بالمواقع، الآراء السياسيّة، الأسماء المستعارة والكنية، وكلّ ما يمكن اعتباره من البيانات الشخصيّة، التي قد تكون طرف خيط، في التعرّف على هويّة شخص بعينه.[13]

تكشف البيانات الشخصيّة والرقميّة، المتوفرة على شبكة الإنترنت أو لدى الشركات/ المؤسسات/ الحكومات الكثير عن الأفراد وأفكارهم ونمط حياتهم وتحركاتهم. وأصبح من السهل استغلال هذه البيانات؛

9. قوتال، ياسين. مصدر سابق. ص 57-58.

10. الضناوي، زينب. (2019). الحماية القانونيّة للخصوصيّة على الإنترنت في ظل الجهود الدوليّة والداخليّة. لدى سرور، طالبي. (مشرف). كتاب أعمال المؤتمر الدوليّ المحكم حول الخصوصيّة في مجتمع المعلوماتيّة (ص 22-37). لبنان: طرابلس. مركز جيل البحث العلمي.

11. خلايفة، هدى. (2019)، الإطار القانونيّ الدوليّ والداخليّ لحماية الخصوصيّة على الإنترنت، التشريع الجزائري نموذجًا. لدى سرور، طالبي. (مشرف). كتاب أعمال المؤتمر الدوليّ المحكم حول الخصوصيّة في مجتمع المعلوماتيّة (ص 39-58). لبنان: طرابلس. مركز جيل البحث العلمي.

12. نسمة، بطيحي. (2019). الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصيّة الرقمية في التشريع الجزائري. لدى سرور، طالبي. (مشرف). كتاب أعمال المؤتمر الدوليّ المحكم حول الخصوصيّة في مجتمع المعلوماتيّة (ص 59-86). لبنان: طرابلس. مركز جيل البحث العلمي.

13. Wolford. Ibid.

لإيذائهم والإيقاع بهم والتأثير عليهم وعلى خياراتهم. فعلى سبيل المثال، استغلّت بعض الحكومات القمعيّة، البيانات الشخصيّة الرقمية لصحفيين وناشطين مناهضين لها؛ لملاحقتهم وقتلهم. لا يقتصر استغلال البيانات على الحكومات والمؤسسات، فحتى الأفراد يمكنهم استغلال بيانات شخصيّة لأفراد آخرين، لابتزازهم وإلحاق الضّرر بهم. لذلك، أصبح من الضروريّ الحرص على حماية البيانات الشخصيّة والرقميّة لكل فرد، وتوفير الحق لهم في اختيار الجهة، التي يرغبون بمشاركة معلوماتهم معها، ومَن لديه حق الوصول إليها، إلى جانب المدة الزمنيّة، التي يمكن الاحتفاظ، بها في قواعد البيانات، فضلًا عن قدرة الفرد على تعديل هذه البيانات متى شاء.[14]

تقنيات جمع واستخدام البيانات الشخصيّة

أفرزت تكنولوجيّا الاتصال الحديثة وشبكة الإنترنت، مجموعة من التقنيات والطرق والأساليب، القادرة على جمع وتحليل واستخدام البيانات الشخصيّة الخاصة بالمستخدمين. ولعل التقنية الأوسع انتشارا هي ملفات تعريف الارتباط (الكوكيز Cookies)، التي تتبع المستهلك عبر شبكة الإنترنت. فهي تمكن المواقع الإلكترونيّة من جمع المعلومات عن المستخدمين، على سبيل المثال نوع الجهاز والمعالج، ورقم الـIP الخاص بالمستخدم، وطريقة الاتّصال بالإنترنت، والمواقع التي زارها، وعدد الساعات التي يقضيها على الانترنت، طبيعة اهتماماته، وما يبحث عنه، ومشترياته الإلكترونيّة، بالإضافة إلى كافة المعلومات الشخصيّة، التي يضعها المستخدم في أي استمارة تسجيل على الانترنت، من أرقام بطاقات ائتمانية وهواتف وعناوين، وغالبًا لا يعلم زوار المواقع الإلكترونيّة بذلك. كما أنّ المعلنين يستغلّون هذه المعلومات لصالح إعلاناتهم، حيث يتم استخدامها، بالعادة، من قبل أطراف ثالثة، وهو ما يحتاج إلى تنظيم شامل من قبل الجهات المختصة، لأوجه جمع واستخدام هذه البيانات.[15]

وفي السياق ذاته، فإن استخدام الهاتف المحمول بما يحتويه من تقنيات، كالتعرّف على الموقع الجغرافي ومشاركته على مواقع التّواصل الاجتماعي، قد أفاد المسوّقين في توجيه الإعلانات التسويقيّة بشكل أساسيّ، حسب البيانات، التي تجمعها هذه التقنية بهدف توجيه الرسائل الإعلانية المناسبة له، واختياره كجمهور مستهدف بناء عليها.[16]

وينضاف إلى كل ذلك، وبناء على الكمّ الهائل من المعلومات، الذي أصبح متاحًا، من خلال التقنيات الحديثة والتطور الاتصالي، سهولة اختراق المواقع الإلكترونية، وقواعد البيانات والبيانات الشخصيّة، من خلال هجمات الهاكر المنظمة، التي تستهدف أفرادًا أو مؤسسات بعينها، الذي يشكّل حربًا مفتوحة، على قاعدة الاستفادة من الثّغرات الإلكترونيّة المتاحة. وتتمّ، عادة، عبر برامج معقّدة، وطرق احتيالية واختراقات للأجهزة، وكل ما هو متّصل بشبكة الإنترنت. وحسب الموسوي وفضل الله فإن خرق الخصوصيّة، على شبكة الإنترنت يمكن أن يتم من قبل ثلاث جهات أساسية، * مزوّد خدمات الإنترنت، حيث باستطاعته رصد كل ما تقوم به على الانترنت (مكان وزمان الدخول إلى الشبكة، المواقع التي يزورها المتصفح، والأوقات، والكلمات التي جرى البحث عنها، والحوارات، والرسائل الإلكترونية، وغيرها). * المواقع التي يزورها المتصفّح، قادرة بدورها على تحديد حركته فيها، وذلك من خلال ملفات المواقع الإلكترونية الكوكيز.

14. الصيادي، آمنة. (2019، 25 كانون الثاني). البيانات الشخصيّة: ما مدى أهميّة حمايتها وهل من تشريع؟ منظمة أكسس ناو. تاريخ الاسترداد: أيّار/ مايو، 2021.

15. عزي، عبير. (2015). تأثير استخدام المعلنين لملفات تعريف الارتباط (الكوكيز Cookies) لتتبع المستهلك عبر شبكة الانترنت على حماية الحق في الخصوصيّة. المجلة المصريّة لبحوث الإعلام. جامعة القاهرة. ص 301-346.

16. عزي، عبير. (2018). تأثيرات استخدام المعلنين لتقنيات التتبع الجغرافي للمستهلكين عبر الهواتف الذكية. المجلة العلميّة لبحوث العلاقات العامة والإعلان. ص 509 - 549.

*مخترقو شبكة الإنترنت "الهاكر"، من خلال التّركيز على ثغرات المنتديات الإلكترونيّة، ومواقع التواصل الاجتماعي.[17]

بعد أن تُجمع بيانات المستخدمين، من قبل المؤسسات والشركات، تُستغل لاستهدافهم بدقّة أكثر، وهناك مؤسسات وشركات تبيع هذه البيانات لأطراف ثالثة، وهذا يقع في صلب خرق الخصوصيّة.[18]

تُخترق الخصوصيّة أيضًا على مواقع التواصل الاجتماعيّ، من خلال إتاحة معلومات مستخدميها الشخصيّة، للمطورين وشركات الخدمات الرقميّة، لتمكينهم من الوصول إلى تفاعلات المستخدمين، دون مراقبة من مواقع التواصل الاجتماعي. وفي السّنوات الأولى لعمل منصات التواصل الاجتماعي لم يسيطر ولم يتحكّم المستخدمون ببياناتهم الشخصيّة، ولم ترَ هذه المنصات أن هناك ضرورةً لإعلام المستخدمين أيًّا من بياناتهم منشورة، ويستطيع الآخرون الحصول عليها، كل هذا عرّض هذه المنصات للمساءلة القانونية، وهو ما أجبرها على إدخال تعديلات لحماية البيانات، على نحو دائم، إلا أنّها ما زالت غير كافية.[19]

يشكّل المستقبل الرقميّ تحدِّيًا للخصوصيّة، سيّما على مواقع التواصل الاجتماعي، التي باتت تسيطر على المواقع والتطبيقات، وذلك من خلال إتاحة استعمال حساباتها للتسجيل وتعبئة البيانات الشخصيّة الفورية، لمواقع وتطبيقات مختلفة.[20]

إضافة لإتاحة أو بيع هذه البيانات طوعيًّا، أو الحصول عليها بأساليب القرصنة، هناك، أيضًا، موظّفو معالجة البيانات الشخصيّة الخاصة بالعملاء والمستخدمين، الذين تُوكل إليهم مهمة البحث ومعالجة وتخزين البيانات الرقمية، ما يجعلهم قادرين على انتهاك الخصوصيّة.[21]

من جهة أخرى، تجمع الحكومات بيانات مواطنيها، بموجب قوانين إدارية مختلفة، تشمل تسجيلات السيارات والإقامة والضرائب، بالإضافة إلى المعلومات الماليّة والحالة الاجتماعية، واستخدام الكهرباء والمياه وغيرها، تمكّن هذه المعلومات الجهات الحكوميّة تنفيذ مهامّها بكفاءة، إلا أنّ الخطر وارد من كشف بيانات المواطنين، والاطلاع عليها لأغراض غير شرعية وغير قانونية، من قبل الحكومات ذاتها، ومن قبل طرف ثالث.[22]

تكمن أهمية الحديث عن حماية الخصوصيّة والبيانات الشخصيّة، بأنّ الطرق والوسائل والأساليب، التي يمكن استخدامها على شبكة الإنترنت كثيرة ومتعددة، وبعضها ما زال غير مكتشف أو موثّق، وهي تكنولوجيا تتطوّر بالتّوازي مع التّطوّر الحاصل في تكنولوجيا وتقنيات الاتصال وشبكة الإنترنت، لذلك، من الأهمية بمكان توافر الوعي بالقواعد الأساسية، التي قد تساعد في تقليل حجم المعلومات والبيانات الشخصيّة، التي يمكن أن يعرفها الغير عن المستخدم.

17. الموسوي، منى؛ وفضل الله، جان. (2013). الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها. مجلة كليّة بغداد للعلوم الاقتصاديّة الجامعة العدد الخاص بمؤتمر الكليّة.

18. جابر، أشرف. (2015). استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصيّة. مجلة العلوم الإنسانيّة.

19. فضيلة، تومي. (2017). إيديولوجيا الشبكات الاجتماعيّة وخصوصيّة المستخدم بين الانتهاك والاختراق. مجلة الباحث في العلوم الإنسانيّة والاجتماعيّة، العدد 30. ص 41-50.

20. Weber, Rolf. H. (2015). The digital future - A challenge for privacy? **Computer Law and Security Review**, 31(2). Pp. 234–242. https://doi.org/10.1016/j.clsr.2015.01.003

21. Ibid.

22. Ibid.

قوانين الخصوصيّة وحماية البيانات عالميًّا

بحسب بيانات مؤتمر الأمم المتحدة للتجارة والتطوير، فإنّ 128 دولة من أصل 194 دولة أقرّت قوانين أو تتداول إقرار قوانين لحماية الخصوصيّة والبيانات الرقمية.[23] ويشكّل القانون العام للاتّحاد الأوروبي، الخاص بالخصوصيّة وحماية البيانات الشخصيّة (GDPR)، الذي سُنّ في العام 2018، إطارًا إيجابيًّا لحماية المستخدمين والأفراد، على استعادة السيطرة على معلوماتهم الشخصيّة والرقمية. يعدّ هذا القانون الأكثر شمولًا، وقد أصبح مصدر إلهام للكثير من الحكومات والجهات التشريعية والقانونية. يشدّد القانون الأوروبي لحماية البيانات، على أنّ أحد المحاور الأساسيّة، للخصوصيّة وحماية البيانات، بعد تقييد عملية جمع البيانات هو مرحلة معالجة البيانات. حيث عرّفها على أنها أيُّ معالجة أو عملية، تنفّذ على المعلومات الشخصيّة، سواء كانت مؤتمتة من خلال برامج وخوارزميات أو يدوية، وهو ما يشمل عملية (جمع، تحليل، تسجيل، تنظيم، تقسيم، تصنيف، استخدام، مسح) لبيانات المستخدمين/الأفراد الرقميّة، الذين قد يكونون عملاء أو مستخدمين، أو زوّارًا للموقع الإلكترونيّ. إضافة إلى ضرورة معرفة مَن الشّخص، الذي يحقّ له الاطّلاع على البيانات ومعالجتها، وتحديد صلاحيّاته بشكل واضح ومعلوم، وإن كان موظفًّا أو مالكًا لبيانات المستخدمين، أو طرفا ثالثًا، يدير هذه البيانات، بشكل قانوني وآمن.[24]

تُلزم سياسات الخصوصيّة وحماية البيانات، والقوانين المتعلّقة بها، جميع الجهات التي تمتلك بيانات شخصيّة، أو تعمل على جمعها ومعالجتها، بأن يكون لدى كلّ موقع ويب مثلًا سياسة خصوصيّة، تشرح لمستخدميه ما هي المعلومات، التي يتم جمعها وكيفية استخدامها وكيفية مشاركتها وكيفية تأمينها. وهو ما يمكن أن يكون مستوحىً من قوانين وتشريعات الخصوصيّة وحماية البيانات، التي هي في أغلبها قوانين أمريكيّة وأوروبيّة، وتعدّ الأهمية الجوهريّة لأصحاب الأعمال والمؤسسات بالالتزام بما تنصّ عليه قوانين الخصوصيّة وحماية البيانات، حيث سيكون من الأسهل والأقل تكلفة التوافق مع هذه المعايير، بدلاً من تطبيق قواعد مختلفة، تسبّب مخالفات قانونيّة وحقوقيّة، أو تؤثّر سلبًا على قرارات المستخدمين والعملاء، الّذين باتت قضيّة حماية بياناتهم قضيّة جوهريّة وأساسيّة، تؤثّر سلبًا على سمعة المؤسسة/الشركة.[25]

شدّدت منظّمة أَكسس نَاو، وبالاعتماد على قانون حماية البيانات الأوروبيّ، أنّه يجب على جميع الأطر القانونيّة في الدّول، التي تسعى إلى إقرار قوانين خصوصيّة وحماية بيانات، أن تراعي فرض عقوبات كافية بحقّ مَن لهم علاقة بالبيانات الشخصيّة والخصوصيّة، بما في ذلك تجريم: الوصول غير المصرّح به إلى أنظمة الهُويّة، أو قواعد البيانات الأخرى، التي تحتوي على بيانات شخصيّة، والمراقبة غير المصرّح بها لأنظمة الهُويّة أو قواعد البيانات، التغيير غير المصرّح به للبيانات، التي تمّ جمعها أو تخزينها، التّداخل غير المصرّح بهن مع أنظمة الهويّة أو قواعد البيانات، التي تحتفظ بالبيانات الشخصيّة.[26]

أمّا في الولايات المتحدة لا يوجد قانون فيدرالي شامل، يحكم خصوصيّة البيانات، حيث إنّ هناك خليطًا معقّدًا من القوانين، الخاصة بالقطاعين العام والخاص، بما فيها تلك القوانين واللوائح، الّتي تتناول الاتصالات والمعلومات الصحيّة، والمعلومات الائتمانيّة والمؤسسات الماليّة والتسويق، التي- في أغلبها- صدرت في ولايات محدّدة.[27]

23. UNCTAD. (2021). Data protection and privacy legislation worldwide. United Nations Conference on Trade and Development. Retrieved June, 2021.
24. Wolford. Ibid.
25. Carson, Angelique. (2021). Data privacy laws: What you need to know in 2021.Osano. Retrieved June, 2021.
26. The World Bank. (2019). Data protection and privacy laws. Retrieved June, 2021.
27. Carson, Angelique.Ibid.

نورد في ما يلي سبعة مبادئ لحماية البيانات الشخصيّة وتمكين المساءلة حولها، نَصَّ عليها القانون الأوروبيّ لحماية البيانات، وذلك لشموليّة القانون وحداثته:[28]

1. التعامل مع البيانات الشخصيّة بصورة قانونيّة، شرعيّة، شفّافة وعادلة، تجاه صاحب البيانات.
2. تحديد الغرض المباشر والدقيق من معالجة البيانات، وإعلام صاحب البيانات به عند جمعها.
3. تقليل حجم البيانات، التي تُجمع واقتصارها على المعلومات الضروريّة، للغرض المحدد.
4. الحفاظ على دقة البيانات الشخصيّة وتحديثها، بحيث لا تكون مغلوطة أو مضلِّلة.
5. وضع قيود واضحة وصارمة، على تخزين البيانات الشخصيّة، الذي يكون للضرورة المحدّدة بغرض.
6. الالتزام بالنّزاهة والسّريّة التامة في معالجة البيانات، بما يضمن الأمان والسّلامة، كالتّشفير.
7. مساءلة مراقب البيانات، المسؤول عن جمع وحفظ ومعالجة البيانات أمام القانون.

واقع الخصوصيّة وحماية البيانات فلسطينيًّا

يواجه مستخدمو الإنترنت الفلسطينيّون تحدّياتٍ على مستويات عدة، بكلّ ما يتعلق بالخصوصيّة وحماية البيانات. فعلاوة على الانتهاكات، من قِبل شركات عالميّة، التي يتعرّض لها جميع المستخدمين، يواجه الفلسطينيّ الانتهاكات الإسرائيليّة، والانتهاكات المحليّة الفلسطينيّة. يتحكّم الاحتلال الإسرائيليّ في البُنية التحتيّة لتكنولوجيا المعلومات والاتّصالات الفلسطينيّة، إلى جانب أدوات مراقبة إلكترونيّة، تجمع بيانات وتنتهك خصوصيّة كلّ فلسطينيّ، بحجّة دواعٍ أمنيّة. أمّا على الصعيد المحليّ فإنّ غياب سلطة تشريعيّة، قادرة على سَنِّ القوانين وتشريعات مُواكِبة للتطورات، في عالم التّكنولوجيا، يفتح باب انتهاك الخصوصيّة، وحماية البيانات الشخصيّة، في القطاعين الحكوميّ والخاص على مصراعيْه. حتّى اللحظة، لا يتوفّر قانون خصوصيّة وحماية بيانات شخصيّة ورقميّة فلسطينيّ واضح وشامل.

يجرّم القانون الأساسيّ الفلسطينيّ، الذي يُعدّ بمثابة الإطار الدّستوريّ للنّظام القانونيّ الفلسطينيّ، الاعتداءَ على حُرمة الحياة الخاصة. وحسبما جاء في القانون، فإنّ "كلّ اعتداء على أيٍّ من الحرّيات الشخصيّة أو حُرمة الحياة الخاصة للإنسان، وغيرها من الحقوق والحريات العامّة، التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدّعوى الجنائية ولا المدنية، الناشئة عنها بالتّقادم، وتضمن السلطة الوطنية تعويضًا عادلًا لمن وقع عليه الضرر".[29]

تبدو الجهود على أرض الواقع، لحماية خصوصيّة الأفراد الفلسطينيّين، وحفظ معلوماتهم الشخصيّة محدودة؛ حيث أعطت السلطة الفلسطينيّة الأولويّة لاعتماد قانون الجرائم الإلكترونيّة، رغم الجدل العميق حوله.[30]

أُقِرَّ "القانون 16 لسنة 2017 بشأن الجرائم الإلكترونيّة" بموجب مرسوم رئاسيّ في يوليو/تموز، بَيْد أنّ السلطات الفلسطينيّة وجّهت لاحقًا اتّهامات إلى عدد من الصحفيّين، استنادًا إلى هذا القانون. ورغم تعديل القانون في العام 2018 إلا أنّه ما زال يواجه معارضة شديدة، من قبل النشطاء والصحفيّين والمجتمع المدنيّ الفلسطينيّ؛ نظرًا لتضمُّنه بنودًا ذات صياغة فضفاضة، من شأنها أن تهدّد حريّة التّعبير، والحقّ في

28. Wolford .Ibid.

29. القانون الأساسيّ المعدل. المقتفي. تاريخ الاسترداد: حزيران/ يونيو 2021.

30. هيومن رايتس ووتش. (2017، 20 كانون الأوّل). على فلسطين إصلاح قانون الجرائم الإلكترونيّة التقييديّ. تاريخ الاسترداد أيّار/ مايو 2021.

الخصوصيّة على الإنترنت، كما يمكّن السلطات الفلسطينيّة من إساءة استخدامه، بهدف قمع المعارضة السياسيّة ووسائل الإعلام.[31][32]

تطرّق قانون الجرائم الإلكترونيّة إلى الخصوصيّة وحماية البيانات الشخصيّة، حيث نصّت المادة (22) على أنّه:

1. يحظر التدخّل التعسفيّ أو غير القانونيّ، في خصوصيّات أيّ شخص أو في شؤون أسرته أو بيته أو مراسلاته.
2. "كلّ مَن أنشأ موقعًا أو تطبيقًا أو حسابًا إلكترونيًّا، أو نشر معلومات على الشبكة الإلكترونيّة، أو إحدى وسائل تكنولوجيا المعلومات، بقصد نشر أخبار أو صور أو تسجيلات صوتيّة أو مرئيّة، سواء كانت مباشرة أو مسجلة، تتّصل بالتّدخل غير القانونيّ في الحياة الخاصة أو العائليّة للأفراد، ولو كانت صحيحة، يعاقب بالحبس مدّة لا تقلّ عن سنة، أو بغرامة لا تقلّ عن ألف دينار أردنيّ، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، أو بكلتا العقوبتين".[33]

وفي العام 2019 أصدر مجلس الوزراء الفلسطينيّ، في رام الله، القرار رقم (3) لسنة 2019، الخاص بحماية البيانات الشخصيّة الخاصة بالمواطنين الفلسطينيّين، على أن يكون ساريَ النفاذ في الضفة الغربيّة وقطاع غزة. القانون من مادتين تنصّان على:

المادة 1: يُحظر استخدام البيانات الشخصيّة (المباشرة/غير المباشرة)، الخاصة بالمواطنين، متلقّي الخدمة من الشّركات والمؤسّسات المزودة بها، لأغراض تجاريّة، دون الحصول على إذن مسبق منهم، تحت طائلة المسؤوليّة القانونيّة.

المادة 2: على الجهات المختصة كافة، كلّ فيما يخصّه، تنفيذ أحكام هذا القرار، ويعمل به من تاريخ صدوره، ويُنشر في الجريدة الرسميّة.[34]

ولعل أزمة تسريب البيانات الطبيّة الفلسطينيّة، التي كُشِف عنها العام المنصرم (2020)، تعكس حجم الفوضى، التي تعمّ مجاليّ حماية الخصوصيّة، والبيانات الشخصيّة للفلسطينيّين. وفي ندوة رقميّة نظّمها مركز حملة يوم 29 آذار/مارس 2021 ضمن فعاليّات منتدى فلسطين للنشاط الرقميّ، صرّح الدكتور وسام صبيحات، مسؤول ملف كورونا شمال الضفة الغربيّة المحتلة، أنّ هذه التسريبات تُعدّ إحدى التحديات، التي تواجهها وزارة الصحة، وهي نتاج تصرفات فرديّة تعمل الوزارة على ضبطها. من جهة أخرى، تعدّ المنصة الرقميّة، التي تعرض عليها نتائج فحص كورونا على موقع وزارة الصحة إحدى الأدوات، التي يمكن من خلالها اختراق الخصوصيّة الطبيّة للفلسطينيّين، حيث يمكن لأي شخص إدخال رقم هويّة شخص آخر ومعرفة نتيجة فحصه مباشرة.[35]

31. المصدر السابق.

32. عابدين، عصام. (2020). الحقوق الرقميّة في فلسطين بين الطوارئ و جائحة كورونا. حيفا: حملة - المركز العربيّ لتطوير الإعلام الاجتماعيّ. تاريخ الاسترداد: أيّار/ مايو 2021.

33. قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونيّة. المقتفي. تاريخ الاسترداد: أيّار/مايو 2021.

34. قرار مجلس الوزراء رقم (3) لسنة 2019م بالبيانات الشخصيّة الخاصة بالمواطنين. موسوعة القوانين وأحكام المحاكم الفلسطينيّة. تاريخ الاسترداد: حزيران/ يونيو 2021.

35. حملة. (2021). هاشتاغ فلسطين 2020. حيفا: حملة- المركز العربيّ لتطوير الإعلام الاجتماعيّ. تاريخ الاسترداد: حزيران/ يونيو 2021.

خصوصيّة الفلسطينيّين وسيطرة الاحتلال الإسرائيليّ

ترى منظمة أكسس ناو في تقريرها، حول الخصوصيّة وحماية البيانات الشخصيّة في فلسطين، أن تبنّي السلطة الفلسطينيّة قانونًا لحماية البيانات، لن يوفّر سوى مستوى محدود من الحماية؛ نظرًا لخضوع البُنية التحتيّة الخاصة بتكنولوجيا المعلومات والاتصالات الفلسطينيّة للسّيطرة الكاملة الإسرائيليّة، منذ احتلالها للأراضي الفلسطينيّة، في سنة 1967، ورغم توقيع اتّفاقية أوسلو للسلام عام 1993، إلّا أن السّلطات الإسرائيليّة لا تزال تسيطر على المعلومات والاتصالات والموجات الكهرومغناطيسيّة، بالإضافة إلى تحكّمها في عمليات استيراد وتركيب أي معدات، من قبل شركات الاتّصالات الفلسطينيّة ومقدمي خدمات الإنترنت، وذلك "لدواعٍ أمنيّة" غير معلنة. حيث لعبت البُنْيتان، القانونيّة والتّحتيّة دورًا جوهريًّا للسّماح بالمراقبة الجماعيّة للمجتمع الفلسطينيّ، واستغلال بياناتهم الشخصيّة لعقود دون أيّ مساءلة.[36]

ومن الجدير التأكيد على أنّ إسرائيل تستخدم تقنيات مراقبة وتجسّس، أُعدت خصيصًا للتّجسس على الأفراد وتتبّعهم مثل الصحفيين/ات والمعارضين/ات والناشطين/ات مثل تقنيّة ("أني فيجين"). إلى جانب تعاون كبريات الشركات العالميّة، التي تدير منصات التواصل الاجتماعيّ مع وحدات الأمن الإسرائيليّة، بكلّ ما يخصّ المستخدم الفلسطينيّ، كما وثّقها مركز حملة.[37]

منهجيّة الدراسة

اعتمدت الدّراسة الحاليّة المنهج النّوعي؛ لفهم حجم وواقع مشكلة انتهاك الخصوصيّة، والبيانات الشخصيّة الرقميّة في فلسطين، التي نحن بصددها، وذلك من خلال المقابلات الشخصيّة المعمّقة، مع شخصيّات لها علاقة مباشرة بكلّ ما يتعلّق بتكنولوجيا المعلومات، ومن خلال المجموعات المركّزة، التي شملت ناشطين وأكاديميين ومتخصّصين بهذا الشأن.

عيّنة الدّراسة

العيّنة الأولى، المقابلات الشخصيّة المعمّقة. أُجريت 12 مقابلة مع شخصيات، ذات علاقة بموضوع البحث، بشكل مباشر، كما يُبيّن الجدول (2) في الملحق (1).

العيّنة الثّانية، المجموعات المركّزة. شاركت في الدّراسة ثلاث مجموعات مركّزة، من الضفة الغربيّة وقطاع غزة وشرقيّ القدس.[38] ضمت كلّ مجموعة نحو 14 إلى 16 فردًا، ناشطين/ات رقميّين/ات، على شبكات التواصل الاجتماعيّ المختلفة، صحفيّين/ات متابعين/ات لقضيّة الخصوصيّة وحماية البيانات، طلبة ماجستير في مجالات الاتصال، ممثلين/ات عن مؤسّسات مجتمع مدنيّ، مؤسسات حقوقيّة، تقنيّين/ات وخبراء في مجال البرمجة والبيانات الضخمة والتسويق الإلكترونيّ، تتراوح أعمار أفراد المجموعات بين 22- 50 عامًا، يُبيّن الجدول (3) في الملحق (2) التفاصيل الديموغرافيّة للمجموعات المركّزة.

36. فطافطة، مروة. وسمارو، ديما. (2021، 22 آذار). عُرضة للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال أفريقيا. أكسس ناو.

37. حملة. (2021). مصدر سابق.

38. كل واحدة من هذه المناطق الجغرافيّة لها خصائصها السياسيّة التي تتميز فيها ولهذا ستُبيّن لنا صورة أشمل بكل ما يتعلق بالخصوصيّة والبيانات الشخصيّة الرقميّة.

عرض النّتائج

المجموعات المركّزة

في بداية اللّقاءات مع المجموعات المركزة، طُرِحت عليهم مجموعة من الأسئلة؛ للوقوف عند مدى اطّلاعهم على مفهوميّ الخصوصيّة والبيانات الشخصيّة الرقميّة وحمايتهما (الجدول 1) على العموم، ومن ثمّ تابعت المجموعات النقاش، كل حسب خصائصه الجغرافيّة والسياسيّة.

جدول 3: من أجاب بنعم عن الأسئلة المغلقة، موزّعين حسب المجموعات.

الرقم	السؤال	الضفة الغربية (16)	قطاع غزة (15)	شرقي القدس (14)	المجموع (45)	النسبة (100)
1	هل تعرف بوضوح ما معنى الخصوصيّة الرقمية؟	10	10	2	22	%49
		62	%55	%14		
2	هل تعرف بوضوح ما معنى البيانات الشخصيّة الرقمية؟	11	12	8	31	%69
		%68	%80	%57		
3	هل هناك حاجة لحماية البيانات الشخصيّة والخصوصيّة الرقمية؟	15	13	13	41	%91
		%93	%86	%92		
4	لا يوجد في فلسطين قانون خصوصيّة وحماية بيانات؟	12	12	3	27	%60
		%75	%80	%21		
5	هل تقرأ عادة سياسات الخصوصيّة للمواقع والتطبيقات قبل استخدامها؟	5	6	5	16	%36
		%31	%40	%35		
6	هل تشجّع سن قانون الخصوصيّة والبيانات الشخصيّة، بشكل شامل وسريع؟	16	10	14	40	%89
		%100	%66	%100		

يلخص الجدول اعلاه إجابات المشاركين في المجموعات المركّزة الثلاث، والموزعة على الضفة والقدس وغزة، ومن أبرز المؤشرات التي نراها في الجدول:

- أن مفهوميّ الخصوصيّة والبيانات الشخصيّة غير معروفين بوضوح، بين غالبيّة أفراد المجموعات.
- أن نسبة ضئيلة من أفراد المجموعات تطّلع على سياسات الخصوصيّة للمواقع، والتطبيقات قبل استخدامها، فقط نحو ثلث الأفراد يقرأون سياسات الخصوصيّة قبل استخدام المواقع أو التطبيقات.
- غالبية المشاركين يتّفقون على ضرورة وأهميّة سن قانون فلسطينيّ شامل، لحماية الخصوصيّة والبيانات الشخصيّة الرقميّة من الانتهاك.
- برزت مجموعة شرقيّ القدس بعدم معرفتها لمفهوميّ الخصوصيّة والبيانات الشخصيّة وما يتعلّق بهما قانونيًّا، فضلًا عن عدم اطّلاع غالبية أفراد المجموعة على سياسات الخصوصيّة في المواقع والتطبيقات قبل استخدامها.

- أما مجموعة غزة، فبينما اتّفق نحو 90% من الأفراد أنّ ثمّةَ حاجة لسنِّ قانون لحماية الخصوصيّة والبيانات الشخصيّة، إلّا أنّ نحو 60% منهم يشجّعون سَنّ القانون.

مفهوما الخصوصيّة والبيانات الشخصيّة وسياقهما

لم تختلف مجموعتا الضّفة الغربيّة وغزة في تعريفهما لمفهوميّ الخصوصيّة والبيانات الشخصيّة، وإنْ كان التعريف غيرَ وافٍ. إلى جانب ذلك، اتّفقت المجموعتان على مدى أهميّة حماية البيانات، وسهولة انتهاكها، فضلًا عن ضرورة ولزوم موافقة المواطن على استخدام بياناته. أما مجموعة شرقيّ القدس فلم تتطرق إلى مفهومي الخصوصيّة والبيانات الشخصيّة ومعناهما. اختلفت المجموعات عند الحديث عن سياقات الخصوصيّة والبيانات الشخصيّة، فبينما تحدّث عنها أفراد مجموعتيّ غزة وشرقيّ القدس، في سياق الاحتلال الإسرائيليّ وانتهاكاته المتكررة، تطرّقت مجموعة الضفة الغربيّة لاستعمالات الجهات الحكوميّة لبياناتهم، لتحسين جودة الخدمات، التي لا يرون فيها انتهاكًا، بعكس استخدام هذه البيانات من قبل شركات خاصة، بهدف الدّعاية والتّسويق.

انتهاك خصوصيّة المستخدمين الفلسطينيّين

سُئلت المجموعات عن الجهات التي تنتهك خصوصيّة المستخدمين، حسب رأيهم وأهدافها. برز لدى مجموعة الضفة الغربيّة أن الجهات الحكوميّة هي الأكثر انتهاكا لخصوصيّة المستخدمين؛ فهي تتيح للجهات الأمنيّة الفلسطينيّة الاطّلاع على بيانات المستخدمين الشخصيّة، إلى جانب تبادل البيانات مع الجهات الأمنيّة الإسرائيليّة، ولا تكتفي الجهات الحكوميّة في انتهاك خصوصيّة المواطنين لدواعٍ أمنيّة فقط، بل تتبادل البيانات الشخصيّة مع شركات القطاع الخاص. ولخّص أفراد المجموعة أن غالبيّة الانتهاكات تأتي لأسباب تجاريّة، ومن ثم سياسيّة وأمنيّة فلسطينيّة، ومن ثمّ أمنيّة إسرائيليّة. وعبّر أفراد المجموعة عن قلقهم إزاء جمع بياناتهم، وطرق استخدامها وحفظها من قبل شركات الاتّصالات، والقطاع الماليّ والمؤسسات والوزارات. وتساءل المشاركون عن الجهات الرسميّة المسؤولة عن المعلومات، وعن جمعها، وعن استخدامها وعن حمايتها.

أمّا مجموعة قطاع غزة، فتمثّلت أبرز وأهم الجهات التي تخترق وتنتهك البيانات الشخصيّة للفلسطينيّين هي الاحتلال الإسرائيليّ، من خلال متابعة ومراقبة كافة المعلومات المتعلّقة بالأفراد، وسيطرة الاحتلال على التكنولوجيا. وتعدّ أجهزة السلطة الفلسطينيّة، في قطاع غزة، ثاني أهمّ جهة تنتهك خصوصيّة المستخدمين الفلسطينيّين، لا سيما انتهاك حقوق الصحفيّين والنشطاء، الّذين يشاركون في مظاهرات أو منشورات معادية لسلطة حماس، باعتبارها الجهة الحاكمة، إلى جانب انتهاك الخصوصيّة الرقميّة للمعتقلين، الذين قُدمت بحقّهم شكاوى، على سلوك معارض للسّلطة الحاكمة.

تأتي شركات القطاع الخاص، من إنترنت ومزودي خدمات الاتصالات، في المرتبة الثالثة، حيث تتيح هذه الشّركات للحكومة الاطّلاع على البيانات الشخصيّة للمستخدمين، إلى جانب استخدام هذه البيانات لأهداف تجاريّة وإعلانيّة. علاوة على ذلك، ذكر أعضاء المجموعة أنّ هناك أطرافًا خارجية خاصة، تنتهك الخصوصيّة الرقميّة والبيانات الشخصيّة للغزّيين، لمصالحها ومطامعها السياسيّة الشخصيّة.

لم تختلف مجموعة شرقيّ القدس عن المجموعتين الأخريين، على اعتبار سلطات الاحتلال جهة أساسيّة، تستهدف وتخترق خصوصيّة الفلسطينيّين المقدسيّين، سواء لأسباب أمنيّة أو مدنيّة أو تجاريّة إعلانيّة. لا

تكتفي إسرائيل بانتهاك الحقوق الرقميّة للفلسطينيّين، من خلال تتبّع تحرّكاتهم على مواقع الإنترنت، الرسميّة وغير الرسميّة، بل تعمل أيضًا على مراقبتهم، بواسطة أجهزة مراقبة وتنصّت رقميّة وغير رقميّة. وأشار أفراد مجموعة شرقيّ القدس إلى أنّ ثمة تنسيقًا بين السلطات الإسرائيليّة والسلطة الفلسطينيّة، لتبادل بيانات المستخدمين المقدسيّين، وبالتالي استهدافهم أيضًا من جانب السلطة الفلسطينيّة.

دور الاحتلال في السيطرة على خصوصيّة الفلسطينيّين

أجمعت المجموعات الثلاث على سيطرة السلطات الإسرائيليّة التّامة على بيانات الفلسطينيّين، وعلى انتهاكها المتواصل والمستمر لخصوصيّتهم؛ بُغية ملاحقتهم السياسيّة والمدنيّة والصحيّة (منذ بدء جائحة كورونا، في العام المنصرم). سلّطت مجموعة الضّفة الغربيّة الضوء على الأدوات، التي تستخدمها السلطات الإسرائيليّة لتعقّبهم، وعلى إلزامهم استخدام هذه الأدوات، تطبيق المنسق على سبيل المثال، وإدخال بياناتهم الشخصيّة، الّتي تجمعها السلطات الإسرائيليّة بغية تتبّعهم وملاحقتهم.

وشدّدت مجموعة غزة على الأساليب والأدوات والخوارزميّات، التي تستخدمها السلطات الإسرائيليّة في جمع البيانات واستخدامها، لتقييم الغزيّين اجتماعيًّا ونفسيًّا للتنبؤ مَن هو المقاوم، ومَن الّذي يشكّل خطورة على إسرائيل، على حدّ قولهم. إلى جانب ذلك ذكرت المجموعة الغزيّة دور إسرائيل في حجب المحتوى الفلسطينيّ وتقييده على مواقع التواصل الاجتماعيّ.

وقد أجمع أفراد مجموعة شرقيّ القدس على أنّ مستوى الخصوصيّة وحماية البيانات الشخصيّة للمقدسيّين هو صفر بالمئة. وذكروا أنّه من أبرز أسباب انتهاك الخصوصيّة واستغلال البيانات هو الملاحقات السياسيّة والأمنيّة. لا تقتصر انتهاكات السلطات الإسرائيليّة لبيانات المقدسيّين على أهداف سياسيّة وأمنيّة، فهي تلاحقهم لأسباب صحيّة (منذ جائحة كورونا) وديموغرافيّة، وذلك من خلال تتبّع هواتفهم وبطاقاتهم الشخصيّة بهدف تهجيرهم من منازلهم في القدس، لمناطق السلطة الفلسطينيّة.

نحو قانون خصوصيّة وحماية بيانات فلسطينيّ

أجمع أفراد المجموعات الثلاث على أهمية إيجاد قانون يوائم التطور التكنولوجيّ، الذي يشهده العالم لحماية وتنظيم موضوع الخصوصيّة، بما في ذلك تحديد سياسات الخصوصيّة لكل موقع وخدمة، وأن يتّصف بالشمول ويعالج كافة القضايا بنصوص، وتحديد ما هي الجريمة وما هي عقوبتها، بما يحفظ حقوق الإنسان، وأن لا يشمل استثناءات إلا بمبرر قضائي، وينظّم عمليات جمع البيانات ومعالجتها ومشاركتها أو استخدامها وشروط كلّ عملية، فجمع البيانات يجب أن يكون له غرض مصرّح به، مع ضرورة توفير آلية لمتابعة تطبيق سياسات الخصوصيّة، وأهمية توفير جسم رقابي لإنفاذ القانون. وأكدوا أيضًا أنّ القانون سيُسهم في وقف ملاحقة الصحفيّين والنّاشطين، لا سيّما في قطاع غزّة. وشدّد أفراد مجموعة شرقيّ القدس على أهمية موافقة المستخدمين على استعمال بياناتهم.

وأوصى المتحدّثون بمجموعة توصيات، يمكن الإشارة إلى أبرزها كما يلي: الخطر الأكبر أنّ مشكلة انتهاك الخصوصيّة تم تشريعها قانونيًّا بإقرار قانون الجرائم الإلكترونية. ضرورة التمسّك بتحقيق الشفافية، في مختلف المستويات والميادين، كإحدى الرّكائز الأساسية لحماية الحقوق الرقمية وحقوق الإنسان، ووجود قانون خصوصيّة يقود إلى تحقيق الشّفافية والنّزاهة والعكس تمامًا، ضرورة إنشاء جسم مستقلّ لإدارة قطاع الاتّصالات والبيانات الخاصّة بالمستخدمين، وأن يتمّ تضمين قانون الاتّصالات مع إمكانية فرض غرامات وعقوبات على شركات الاتّصالات، وضرورة الإفصاح عن الاتّفاقيات الموقّعة بين السلطة الفلسطينيّة والاحتلال، فيما يتعلق بالخصوصيّة وحماية البيانات.

دور الجهات المحليّة في تشريع قانون الخصوصيّة وحماية البيانات

اتّفق أفراد المجموعة على الضّرورة الملحّة لنشر حملات توعويّة، حول الخصوصيّة والبيانات الشخصيّة؛ بغية الضّغط على السّلطات لسنِّ قانون، يحمي الخصوصيّة والبيانات الشخصيّة للمستخدمين الفلسطينيّين. أشارت مجموعة الضفة إلى دَور مؤسسات المجتمع المدنيّ الفلسطينيّ في نشر التّوعية حول الخصوصيّة، وكذلك حملات توعية للجمهور بأهمية الخصوصيّة. علاوة على ذلك، أشارت المجموعة إلى إمكانية إنشاء هيئة فلسطينيّة لحماية خصوصيّة وبيانات الفلسطينيّين.

وحول تشكيل هيئة مستقلّة لحماية الخصوصيّة والحقوق الرّقمية أوصى المتحدّثون، في مجموعة قطاع غزة بوجوب إيجاد هيئة تنظّيم التّعامل مع الخصوصيّة، وتتابعها وتعمل على إنفاذ القانون، وإشراك الأطراف ذات العلاقة لوضع القانون، منها: جهة رسمية، قضائية، الاتّصالات، النقابات، الأقسام الأكاديمية، المجتمع المدني، وكلّ جهات الاختصاص.

ولخصوصيّة قضيّة الخصوصيّة في القدس، وبما أنّه لا يوجد قانون خصوصيّة إسرائيليّ، يشمل الفلسطينيّين/ات وتحديدًا المقدسيين/ات كونهم ليسوا مواطنين/ات إسرائيليّين/ات، ولا يوجد جهة موثوقة، يمكن اللجوء إليها للمحاسبة، في حال تعرّض أحد الأفراد لانتهاك خصوصيتهم، يقع على عاتق المجتمع المدني في مناطق شرقي القدس أن يعمل على توعية المقدسيين بطرق مواجهة اختراق الخصوصيّة، وكيف يعملون على حماية بياناتهم الشخصيّة، كما يقع على عاتق الصحفيين الفلسطينيّين في القدس دور توعية الأشخاص من انتهاك البيانات من خلال المواد الإعلامية، التي يقدمونها سواء كانت مسموعة أو مكتوبة أو مرئية، أو حتّى من خلال منشوراتهم على فيسبوك.

تحليل المقابلات الشّخصيّة

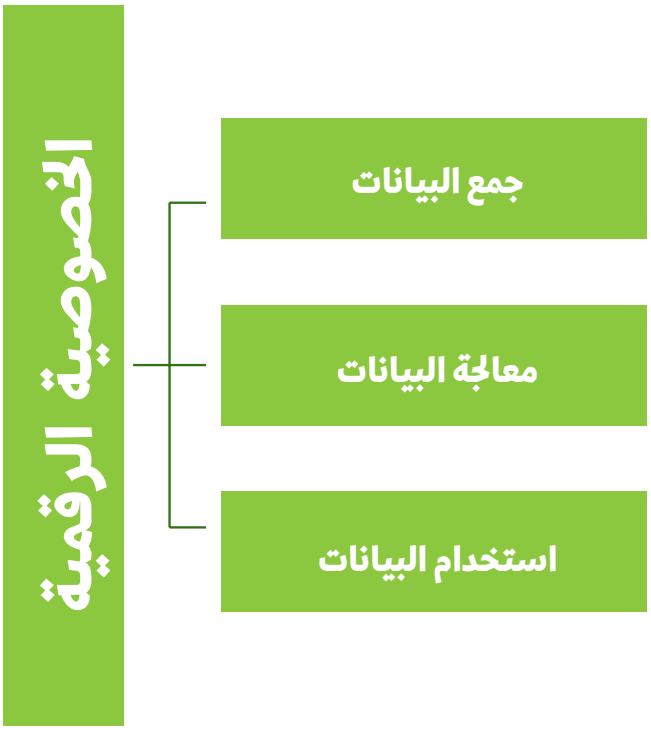
مفهوم الخصوصيّة والبيانات الشخصيّة الرقميّة

اتّفق عابدين[39] وجاموس [40] على أنّ مفهوميّ الخصوصيّة والبيانات الشخصيّة ذُكِرا في القوانين الأساسيّة الفلسطينيّة، بشكلها التقليديّ، دون توضيح وتفصيل وشمول للخصوصيّة الرقميّة. بَيْد أنّه يمكن البناء على المفهوم التقليديّ للخصوصيّة، في أنّها حقٌّ أساسيّ ثابت في الحقوق الدستوريّة الفلسطينيّة، ومخالفته تُرتّب جريمة دستورية ومساءلة وتعويضًا لمن وقع عليه الضّرر، حسب المواد 32, 17 من القانون الأساسيّ الفلسطينيّ. ومفهوما الخصوصيّة والبيانات الشخصيّة الرقميّة يشملان الحفاظ على الحريّات الشخصيّة للفرد، وحرمة شؤون الحياة الخاصة للإنسان كأسرته ومنزله ومكتبه وهاتفه، وأية بيانات رقميّة قد تدلّل على ذلك بشكل مباشر أو غير مباشر.

في ظلّ التّطوّر الرّقميّ لوسائل الاتّصال والتّواصل أصبح بالإمكان تقسيم الاستخدام أو الاعتداء على الخصوصيّة والبيانات الشخصيّة الرّقميّة - سواء لدى الشّركات أو الحكومات أو المواقع الإلكترونيّة والتواصل الاجتماعيّ وغيرها - إلى ثلاثة مراحل أساسيّة: مرحلة جمع البيانات الشخصيّة، مرحلة معالجتها، ومرحلة استخدامها.

39. عابدين، عصام. مقابلة شخصيّة. نيسان، 2021.

40. جاموس، عمّار. مقابلة شخصيّة. أيّار، 2021.



رسم توضيحي 1: مراحل عمليّة الاعتداء على الخصوصيّة والبيانات الشّخصيّة الرّقمية

مرحلة جمع البيانات

ثَمّة طرق متنوّعة وعديدة تُجمع فيها البيانات الشّخصيّة، أبرزها: التّسجيل للخدمات والاشتراكات (على سبيل المثال شركات الاتّصالات والبنوك)؛ تقنيّات ملفّات تعريف الارتباط (Cookies) المزروعة داخل المواقع الإلكترونيّة؛[41] تقنيات تحديد الموقع الجغرافيّ؛ الهاتف المحمول؛ تطبيقات الهاتف المحمول؛ التطبيقات الذكيّة كتطبيقات الدّفع الإلكترونيّ، وبطاقات الائتمان وغيرها. وعادة ما يطلب التطبيق الوصول للصّور والميكروفون والاستديو وجهات الاتّصال، وهذه عبارة عن بيانات يجمعها التطبيق بشكل مباشر، إذا وافقت على سياسات الخصوصيّة، وأحيانًا قد يكون جمع المعلومات بغير قصد من بعض الجهات، لأنّ استخدام الشّبكة العنكبوتية والتطبيقات أصبح يولّد ويجمع بيانات شخصيّة بشكل تلقائيّ.[42][43]

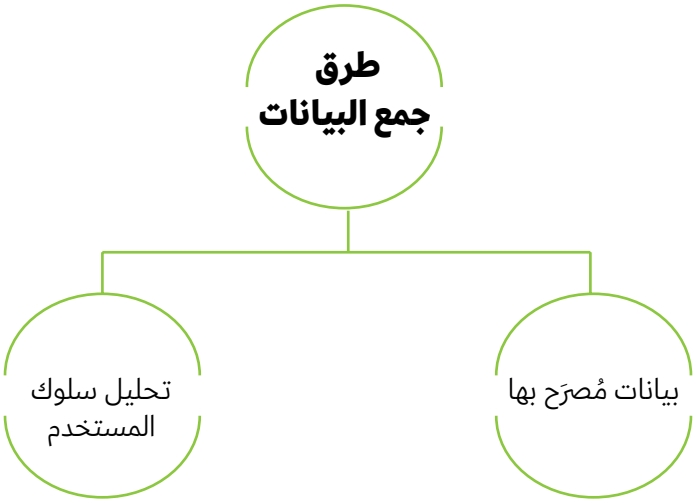
يمكن تقسيم مصادر البيانات الشخصيّة إلى مصدرين أساسيين، **أوّلا**: البيانات التي يصرّح بها المستخدم أو تُسجَّل بموافقته كمعلوماته الشخصيّة، وأية معلومة تدلّل على هويته، اسمه، منزله...إلخ. **ثانيًا**: البيانات التي تصف سلوك واهتمامات المستخدم وممارساته كعمليات التّصفح والشّراء والبحث والاهتمامات،

41. يعد الكوكيز الآليّة الأساسيّة في جمع البيانات فهو الطريق لأي عمليّة تجميع بيانات تحدث على الجهاز، تخبرك بالمواقع، التي زرتها والبيانات التي تخزنها على جهازك ويقوم برصدها، وبالتالي يمكن تخزين خارطة البيانات الخاصة بالشخص بناء على السلوك أو التصرف، فهو عبارة عن هويّة تشمل بيانات وسلوك المستخدم.

42. فطافطة، عبد المنعم. مقابلة شخصيّة. نيسان، 2021.

43. أبو بكر، إبراهيم. مقابلة شخصيّة. نيسان، 2021.

عادة ما تُجمَع بطريقة غير مباشرة، ومن دون وعي المستخدمين لذلك.[44]



رسم توضيحي 2: مصادر البيانات الشخصيّة الرقميّة التي تُجمع عن المستخدمين

مرحلة معالجة البيانات

معالجة البيانات المتوفرة لدى الجهات الفلسطينيّة بغالبيتها من أجل الوصول إلى بيانات عامة وإحصائيّة وأهداف تسويقيّة بالدرجة الأولى، على سبيل المثال معرفة الفئة العمريّة المشتركة في خدمة معينة، المنتجات الأكثر مبيعًا، التقسيم الجغرافيّ للعملاء أو المستخدمين ...إلخ. بَيد أنّ معالجة البيانات تحتاج إلى تقنيات متقدمة من برامج الذّكاء الاصطناعيّ والخوارزميّات، الّتي ما زالت غير متوفّرة لدى جهات القطاعين العام والخاص الفلسطينيّين، وإن كان بعضها يعمل على جمع المعلومات، إلّا أنّه غير قادر على التعمّق في تحليلها وتبقى الاستفادة منها محدودة.[45]

مرحلة استخدام البيانات

تُعتبر مرحلة استخدام البيانات مرحلة واسعة ومتشعبة ترتبط بأهداف كل جهة وحاجتها من المعلومات المتاحة، وغالبًا ما تُستخدم لتحديد مواصفات الجمهور لاستهداف مجموعة معيّنة لغرض معين.[46] تُستخدم البيانات إما في الإطار الطبيعيّ والقانونيّ، وإمّا في إطار الانتهاك والاستغلال غير القانونيّ لبيانات المستخدمين. ويمكن الجزم أن ثمة لا شيء اسمه حماية مطلقة للبيانات، بل هناك حماية نسبيّة تتفاوت وتتراوح ما بين برامج وما بين معدات وما بين جهات معينة.[47]

44. فطافطة، عبد المنعم. مصدر سابق.

45. أبو بكر، إبراهيم. مصدر سابق.

46. فطافطة، عبد المنعم. مصدر سابق.

47. جبارين، شعوان. مقابلة شخصيّة. آذار، 2021.

انتهاك واستغلال البيانات الشخصيّة

يُعدّ انتهاك الخصوصيّة واستغلال البيانات الشخصيّة أمرين بالغيّ الأهميّة وشديديّ الخطورة، وذلك لتوافر بيانات رقميّة ضخمة عن كلّ فرد، بالقدر الّذي يساعد على انتحال شخصيّته، ومعرفة حالته النّفسيّة والاقتصاديّة والاجتماعيّة وحتّى السياسيّة.[48] ويمكن فهم انتهاك خصوصيّة البيانات على أنّه الحصولُ على معلومات العملاء أو المستخدمين، وبياناتهم والاعتداء على ما يتعلّق بغلاف الفرد الخاص، على نحو الاطّلاع على الحسابات، والأرصدة في البنوك، بُغية إلحاق الضّرر والسّرقة، أو على نحو تتبّع جهات اتّصال الفرد، واستغلال سلوكه للإيقاع به أو التّجسّس عليه.[49] [50] علاوة على ما ذُكر، فإن الخطورة كامنة أيضًا بسريّة عمليّات بيع وتبادل البيانات الشخصيّة، التي لا يعلم بها أحد أو لا دليل بحوزته على انتهاكها واستغلالها، سوى مَن نفّذها وشارك بها.[51]

على الصّعيد المحليّ، تنتهك شركات الاتصالات والدّفع الإلكترونيّ والبنوك خصوصيّة مستخدميها، عندما تتيح للجهات الأمنيّة الفلسطينيّة الاطّلاع على بيانات العملاء والمستخدمين، وسلوكهم واهتماماتهم دون أمر قضائيّ أو طلب رسميّ، هذا ما جاء على لسان جبارين[52] في المقابلة الشّخصيّة، التي أجريناها معه لأغراض هذه الدراسة. وأضاف أن هذه الانتهاكات، أحيانًا، تكون لأهداف شخصيّة تتعلّق بالمسؤولين عن حماية هذه البيانات. إلى جانب ذلك هناك استباحة لبيانات المواطنين، ما يجعلها عُرضة للسّرقة واستغلالها لمطامع شخصيّة وسياسيّة، مثلما حدث خلال العام 2021 عندما اُخترق سجلّ الناخبين في بعض مناطق الضفة الغربيّة، بغية التّلاعب في أماكن اقتراعهم.[53] ومثلما حدث من تسريب لقوائم الأشخاص المصابين بفيروس كورونا، التي هي بملكيّة وزارة الصحة أساسًا.[54]

كما أنّ الأحداث السياسية التي تصاعدت مؤخرًا، بعد قتل النّاشط السياسي نزار بنات، على أيدي الأجهزة الأمنية الفلسطينية، وعلى إثرها نظّم الفلسطينيون/ات مظاهرات ضخمة في الشارع الفلسطيني احتجاجًا على ما حصل له والمطالبة بالعدالة، حيث قُمعت هذه المظاهرات من قبل أعضاء أجهزة الأمن الفلسطينية (بلباس رسمي ومدني)، وبعض المؤيّدين لحركة فتح في الضفة الغربية، الذين قاموا بمصادرة وسرقة الهواتف المحمولة الخاصة بالمتظاهرين/ات، خلال عملية القمع، ما أدى إلى اختراق حقّهم/ن في الخصوصيّة، لا سيّما بعد قيام مجموعة منهم بنشر صور ومقاطع فيديو شخصية، خاصة بالمتظاهرين/ات، بهدف التّحريض عليهم/ن والتّشهير بهم/ن لا سيّما الناشطات، وتحديد قدرتهم/ن و/أو منعهم/ن من المشاركة في المظاهرات السلمية في المستقبل.

وعلى ما يبدو، فإنّ الجهة الأكثر انتهاكا لخصوصيّة المستخدمين هي السلطة الفلسطينيّة ومؤسساتها الرسميّة. فهي تعمل أساسًا تحت غطاء قانون الجرائم الإلكترونيّة، الذي يسمح لأجهزة إنفاذ القانون بمراقبة الخطوط الهاتفية، والتّنصت على المحادثات، ومراقبة الإنترنت، والاختراق واعتراض الاتصالات، وتفتيش الأجهزة الإلكترونيّة والهواتف، والحصول على ما بداخلها.[55]

48. فطافطة، عبد المنعم. مصدر سابق.
49. الزيتاوي، إياد. مقابلة شخصيّة. نيسان، 2021.
50. عابدين، عصام. مصدر سابق.
51. جاموس، عمّار. مصدر سابق.
52. جبارين، شعوان. مصدر سابق.
53. عابدين، عصام. مصدر سابق.
54. سمارو، ديما. مقابلة شخصيّة. أيّار، 2021.
55. جاموس، عمّار. مصدر سابق.

من جهة أخرى، يتناول قانون الجرائم الإلكترونيّة مسألة الخصوصيّة، في بعض موادّه باقتضاب، وبمصطلحات فضفاضة. ورغم أنه يُعدّ أساسًا، يمكن البناء عليه، في حماية الخصوصيّة والبيانات الشخصيّة الرقميّة، إلا أن جزءًا من نصوصه ينتهك حق الخصوصيّة ويستبيحها.[56]

قانونيًّا، يُعدّ القانون فضفاضًا، ويتعارض مع التزامات فلسطين للمواثيق الدوليّة، والاتفاقيات الخاصة بحقوق الإنسان، والخاصة بالعهد الدوليّ للحقوق المدنيّة والسياسيّة. ويتعارض القانون مع الحقّ في حريّة الرأي والتعبير والحق في الحصول على المعلومات.

لا يطبّق قانون الجرائم الإلكترونيّة في قطاع غزة؛ فثمّةَ قوانين خاصة، عدّلتها وأقرّتها كتلة حماس التشريعيّة، فعلى سبيل المثال، عدّلت مادة في قانون العقوبات (قانون العقوبات رقم 74 لسنة 36 المادة 262 مكرّر) أطلق عليها "إساءة استخدام التكنولوجيا". وبالتّالي، كل ما له علاقة بالجرائم الإلكترونيّة والخصوصيّة يندرج تحت "إساءة استخدام التكنولوجيا". ينطبق على هذا التعديل ما ذكر من انتقاد حول قانون الجرائم الإلكترونيّة، المعمول به في الضفة الغربيّة، حيث يُترك للنيابة تفسير النّصوص القانونيّة حسب رؤيتها.[57]

لا يختلف حجم انتهاك الخصوصيّة، واستغلال البيانات الشخصيّة في قطاع غزة عما هو في الضفة الغربيّة، وانتهاك الخصوصيّة لا يقتصر على المؤسسات الحكوميّة، التي تتيح للجهات الأمنيّة الاطّلاع على بيانات المواطنين الشخصيّة، كما يستطيع الأفراد ذوو العلاقات الشخصيّة والمتنفّذون الاطّلاع على بيانات المواطنين الشخصيّة.[58]

الالتزام بسياسات الخصوصيّة وحماية البيانات الشخصيّة

أصبح توفير سياسات الخصوصيّة أمرًا أساسيًّا على كلّ خدمة أو موقع أو تطبيق ليُسهِم في حماية خصوصيّة الأفراد.[59] بيد أن المشكلة تكمن في وضع سياسات خصوصيّة، تنتهك الخصوصيّة عوضًا عن المحافظة عليها، وغالبًا ما يوافق المستخدمون عليها، دون وعي لمضمونها. وحسب القانون الفلسطينيّ الحالي، وكوننا نفتقر إلى قانون خصوصيّة شامل، فإنّه بموجب موافقة المستخدمين على سياسات الخصوصيّة، فإنّ القانون لا يحمي المستخدمين إذا وافقوا على استغلال بياناتهم، دون علمهم بذلك، فالأصل أن يكون هنالك تحديد لما يجب أن تتضمّنه سياسات الخصوصيّة بشكل قانونيّ.[60]

ترى الجهات الحكوميّة المنظمة لعمل القطاع الخاص، سلطة النقد الفلسطينيّة على سبيل المثال، المنظمة لعمل شركات الدّفع الإلكترونيّ، ووزارة الاتصالات، المنظِّمة لعمل شركات الاتصال، بأن هذه الشركات ملتزمة بسياسات الخصوصيّة الأساسيّة الموجودة في تراخيصها والمُقرّة من قبل كلّ وزارة. علاوة على ذلك، تعمل هذه الجهات على حماية حقوق المستخدمين وبياناتهم، وتحدّد الإسناد الخارجي التقني للشركات، وتمنع الاحتفاظ ببيانات الفلسطينيّين خارج البلد، فالتراخيص لمثل هذه الشركات مشروطة بإجراءات عدّة، تضمن الخصوصيّة وحماية البيانات فيها. تستند في ذلك على التشريعات، التي تتخذها سلطة النقد وشروط التراخيص، وقانون المدفوعات، حيث يتم العمل على تطوير كل ذلك باستمرار، من أجل أن تكون الخدمات مطابقة للمعايير الدولية مثل (Standardization for Organization International-ISO) كما هي مطابقة للاتفاقيات الاقتصاديّة، مع الجهات الدولية الخاصة بتقديم خدمات تحويل الأموال.[61][62]

56. عابدين، عصام. مصدر سابق.
57. حماد، حسين. مقابلة شخصيّة. نيسان، 2021.
58. المصدر السابق.
59. جبارين، شعوان. مصدر سابق.
60. عابدين، عصام. مصدر سابق.
61. أبو بكر، إبراهيم. مصدر سابق.
62. الزيتاوي، إياد. مصدر سابق.

أيضًا ترفض سلطة النقد الفلسطينيّة أن يكون هنالك وصول حر لبيانات المستخدمين في البنوك، وشركات الدفع الإلكتروني، أو أن يتم حفظ البيانات في مكان غير آمن، لأنها تعمل بموجب قوانين وأنظمة صارمة تحكم كل ذلك. ولا شكّ أن بيانات المستخدمين، في القطاعات المصرفيّة وشركات الدفع الإلكترونيّ، تخضع لنظام محوسب، وفي حال حدث أي تغيير أو انتهاك فإن النّظام يكشف ذلك بسهولة. ومن الأنظمة الحاسوبية المستخدمة والمعروفة عالميا (Registry Credit ،RTGS , Temenos)، حيث تعمل على منع مشاركة بيانات المستخدمين مع أطراف ثالثة، حتى لو وافق العميل على ذلك، وتمنع الوصول لغير المصرح لهم، ولا تعطي معلومات تفصيلية عن المستخدمين، ولا تسمح بتحليل بيانات المستخدمين، ومراقبة سلوكهم واهتماماتهم الشخصيّة. وفي حال انتهكت خصوصيّة المستخدمين فإن سلطة النقد لديها نظام عقوبات جزائيّة وعقوبات ماليّة كسحب تراخيص، والتوجّه الى القضاء.[63]

علاقة قانون الخصوصيّة بالديمقراطيّة وحقوق الإنسان

شدّد جبارين (2021) أن وجود قانون للخصوصيّة وحماية البيانات، هو مؤشّر قوي، يدلّ على ديمقراطية الدولة وشفافيتها ونزاهتها. فالعلاقة طردية، إذا توفّر احترام للخصوصيّة توفّر الجوّ الديمقراطي الذي يحترم حقوق الإنسان والحريات.[64] ويرتبط مفهوم الحرية بشكل وثيق بالخصوصيّة وحماية البيانات، فاحترام الحريّة الشخصيّة والحياة الخاصة، وعدم الاعتداء على حرية الآخرين وبياناتهم الشخصيّة، هو مبدأ أساسي في مفهوم الحرية وحقوق الإنسان.[65]

ويمكن اعتبار أن من أفضل القوانين القادرة على حماية حقوق الإنسان وحريته ومنع انتهاكها هو قانون الخصوصيّة وحماية البيانات.[66]

مفهوم الخصوصيّة بشكلها العام مرتبط بمدى شفافية النظام، والحوكمة الرّشيدة، بل مرتبط بمنظومة الحقوق الإنسانية كافة، لأنّ جميع الحقوق مرتبطة بالبيانات، والحقوق لا تُجزّأ. عمليًا قانون الخصوصيّة وحماية البيانات يفترض أن يهيمن على منظومة الحقوق الإنسانية، ولا يمكن أن تبني نظام نزاهة وطنيًّا دون احترام للخصوصيّة، وما دون ذلك سيكون تغوّل العسكر والأمن على الحياة المدنية، لينهيها ويحولها لنظام شمولي.[67] وللأسف فإنّ الواقع الفلسطينيّ في التّعامل مع قضايا الخصوصيّة وحماية البيانات، يعتمد بشكل كبير على مفاهيم الواسطة والمحسوبية، وستستمر الأخطاء المرتكبة في هذا الجانب، ما لم يتوفّر قانون شامل وناظم للخصوصيّة وحماية البيانات.[68]

ما يجب حمايته وما يجب إتاحة الوصول إليه

تجدر الإشارة إلى أن قانون الحصول على المعلومات لم يقرّ فلسطينيًّا حتّى الآن (2021)، علمًا أنه مقدّم كمقترح منذ العام 2005. ولا بدّ من فهم الفرق الجوهري بين ما يجب حمايته من معلومات وبيانات، من خلال قانون الخصوصيّة وحماية البيانات، وما يجب إتاحة الوصول إليه. يعبّر قانون الحصول على المعلومات عن البيانات العامة الخاصة بالجهات الرّسمية، وما يجب أن توفّره من معلومات واحصائيات

63. المصدر السابق.
64. جبارين، شعوان. مصدر سابق.
65. حماد، حسين. مصدر سابق.
66. جاموس، عمّار. مصدر سابق.
67. عابدين، عصام. مصدر سابق.
68. حماد، حسين. مصدر سابق.

وخدمات وطريقة إدارتها وإدارة المال العام، وكل ما يخص الجمهور والصّالح العام، مع مراعاة ما يمكن تصنيفه من معلومات، كمعلومات تخصّ الأمن القومي، وهناك معايير عالمية لذلك، ولِما يجب حجبه والإفصاح عنه.[69][70] يعبّر قانون الخصوصيّة وحماية البيانات عن البيانات الخاصة بالأفراد، وفي حال لم يوافق الفرد على انتقال هذه البيانات من الحيّز الخاص إلى الحيّز العام، يجب طرح السؤال التالي: هل ما حصل هو عملية تعرّض تعسفي غير مشروع للحياة والمعلومات الخاصة أم لا؟ ومثال ذلك قضيّة الخدمات الصحية، التي تقدمها وزارة الصحة، فهذا حيز عام للجميع، كمعرفة عدد المصابين بفيروس كوفيد 19، لكنّ السجل المرضي للفرد يجب أن يخضع للسّرية الطبية، وبالتّالي إذا اختُرِقت السّرية الطبية اخترقت الخصوصيّة.[71] والأصل هو الحماية لجميع البيانات، لكنّ منسوب الخصوصيّة يقلّ عند الشّخصيات العامة، فتناول الحالة الصّحية للرئيس أو رئيس الوزراء، أو أحد المسؤولين العموميين يكون بخلاف المواطن، الذي بإمكانه أن يرفع دعوى إذا انتهكت خصوصيته، وتم التّصريح عن حالته المرضية دون إذنه.[72]

الخصوصيّة وحماية البيانات في فلسطين من منظور دولي

ترى سماروو (2021) أن الخصوصيّة وحماية البيانات في فلسطين لها خصوصيّة، مقارنة بالسياق الدولي، ويعود ذلك لعدة أسباب، من أبرزها: التّحديات التي تواجه المجتمع الفلسطينيّ واستخدامه للإنترنت، حيث لا يمكن الحديث عن حماية الخصوصيّة وحماية البيانات، في ظلّ وجود قوانين عسكريّة، تابعة لسلطات الاحتلال الإسرائيليّ تتحكم بالفضاء الرقمي، وتسيطر على البنية التحتيّة لتكنولوجيا المعلومات والاتّصالات، فمثلًا خدمة الجيل الثالث للإنترنت (3G)، الذي احتاج سنوات ليصل للفلسطينيّين بداية العام 2018، بسبب منع سلطات الاحتلال، فالفلسطينيّون فعليا ليس لديهم سيادة كافية وسيطرة على البنية التحتية لشركات الاتصالات والإنترنت.[73]

أضف إلى ذلك، عمليات المراقبة الكبيرة والواسعة لبيانات الفلسطينيّين، التي تنفّذها سلطات الاحتلال، فحسب صحيفة هآرتس، عمليات المراقبة الإسرائيليّة في الضفة الغربية هي واحدة من أكبر عمليات المراقبة، فكيف يمكن فرض احترام الخصوصيّة وحماية البيانات الشخصيّة على دولة احتلال! أمّا على المستوى الداخلي فإن الانقسام الدّاخلي الفلسطينيّ، بين الضفة الغربية وقطاع غزة وتعطّل المجلس التشريعي، وعدم التّوافق في تطبيق القوانين المستحدثة، في شِقّي الوطن فكلّ هذا يعطّل التسريع في تشريع قانون الخصوصيّة وحماية البيانات، وعدم تمكّن المنظمات الدولية، والدول الداعمة المساعدة في ذلك.[74]

69. جبارين، شعوان. مصدر سابق.
70. عابدين، عصام. مصدر سابق.
71. المصدر السابق.
72. جاموس، عمّار. مصدر سابق.
73. سمارو، ديما. مصدر سابق.
74. المصدر السابق.

التّحكم الإسرائيليّ في خصوصيّة الفلسطينيّين

تقوم العقلية الذّهنية للحكومات على جمع أكبر قدر ممكن من البيانات عن المستخدمين، لأنّها تستمدّ كلّ نفوذها من المعلومات، والحكومات بارعة في استخدام البيانات.[75] ويوجد لدى السلطات الإسرائيلية تفوّق تكنولوجيّ، فنلاحظ أنّ شركات كبرى، عاملة في مجال الإنترنت وتصميم المواقع الالكترونية، هي شركات إسرائيليّة أو تستخدم تقنيات إسرائيليّة، فلو أردنا النّظر بالأمر من زاوية تقنية، فإسرائيل لديها القدرة التقنية على اختراق خصوصيّة الفلسطينيّين، وكذلك لديها الإرادة والرّغبة في ذلك.[76] ولا يمكن الاستهانة بعدد الفلسطينيّين/ات، الذين يستخدمون شركات اتصالات إسرائيليّة سواء مجبرين، مثل القدس والداخل الفلسطينيّ أو مخيّرين، كالضّفة وغزة لقدرتها التنافسية، مقارنة بالشركات الفلسطينيّة، فهذه الشركات بطريقة ما هي قادرة على جمع بياناتهم واختراق خصوصيتهم.[77]

أضف إلى ذلك، المراقبات الأمنيّة الإسرائيليّة للأفراد والمؤسسات الفلسطينيّة، لدرجة أنّها تعمل على مراقبة صفحات المؤسسات الحقوقية الفلسطينيّة، على وسائل التواصل الاجتماعي واستهدافها، ومحاولة تشويه صورتها من خلال التواصل مع الداعمين الدوليين لها، كما حصل مع مؤسستي الحقّ والميزان.

كما قامت المخابرات الإسرائيلية، بتاريخ 11 أيّار/مايو بإرسال رسائل نصية (SMS) إلى هواتف المصّلين في المسجد الأقصى، تعلّمهم أنّه قد تمّ "تصنيفهم كمشاركين في أعمال عنف في المسجد الأقصى، وبناء عليه ستقوم المخابرات الإسرائيليّة بمحاسبتهم لاحقا."[78] إنّ هذه الرسالة جاءت، في الغالب، نتيجة لاستخدام المخابرات الإسرائيلية نظام التّتبّع GPS، الّذي، بناء عليه، قامت بتحديد الموقع الجغرافيّ لهؤلاء المصلّين، الذي يعتبر انتهاكًا لحقّهم في الخصوصيّة.

يمكن القول إنّ السّيطرة الإسرائيليّة تطال بيانات الفلسطينيّين الرّقمية، من خلال وسائل التّواصل الاجتماعي والتّحكّم في البنية التّحتية للاتصالات الفلسطينيّة، ومعرفة كلّ ما يمكن أن يدخل عبر الحدود، أو يخرج من تقنيات وأجهزة، وكاميرات المراقبة بين المدن والمستوطنات، سواء بالضفة أو الداخل، وتقنيات التعرف على الوجه في القدس المحتلة تحديدًا، وعلى الحواجز، ما يعطيهم القدرة على مراقبة الفلسطينيّين بنسبة 100%. ويوجد في "إسرائيل" قانون خصوصيّة، اسمه "قانون خصوصيّة وحماية بيانات شخصيّة"، وهو موجود منذ سنة 1981، وأيضًا لديهم مبادئ توجيهيّة لهيئة الخصوصيّة الإسرائيليّة، التي تمّ تأسيسها في عام 2006، إلّا أنّ هذا القانون لا يسري على الفلسطينيّين، في القدس أو الضفة الغربية أو قطاع غزة، كونهم ليسوا مواطنين إسرائيليّين ولا يطبّق أيضًا على الفلسطينيّين في الدّاخل المحتل، في عملية تمييز واضحة ضدهم.[79]

بالتأكيد هناك إمكانية لمقاضاة دولة الاحتلال الإسرائيليّ، على انتهاكها لخصوصيّة الفلسطينيّين، ولكن ثمة عقبات أساسية، وهي أين ستتم مقاضاتها ووفق أيّ قانون؟ وكيف سيتم إثبات انتهاكها لبيانات الفلسطينيّين؟ فوحدات السايبر التابعة لها لا أحد يعلم عنها شيئًا، خاصة وحدة السايبر التابعة للاستخبارات العسكرية الإسرائيليّة.[80] ويمكن الإشارة إلى أنّه على الفلسطينيّين التّركيز على جذب الانتباه الدولي، لما

75. عابدين، عصام. مصدر سابق.

76. فطافطة، عبد المنعم. مصدر سابق.

77. حماد، حسين. مصدر سابق.

78. El-Kurd, Mohammed {@m7mdkurd}. (2021). Many Palestinians are receiving this message to their phones. "Hello! You have been identified to have taken part in violent acts at Al-Aqsa Mosque. We will hold you accountable.- Israeli intelligence". Israel is likely using a GPS system, like the one for corona outbreaks.Twitter. Retrieved June, 2021.

79. سمارو، ديما. مصدر سابق.

80. عابدين، عصام. مصدر سابق.

يعانيه الفلسطينيّون من اختراق وانتهاك لخصوصيتهم وبياناتهم الشخصيّة، على يد الاحتلال الإسرائيليّ، وقد يتمّ ذلك من خلال الاستمرار في الضغط على "إسرائيل" بشتى الطّرق، فمثلًا، التّوثيق لانتهاكات جيش وسلطات الاحتلال بلغات مختلفة يعتبر أمرًا مهمًّا، والتعاون مع أكثر من مؤسسة ومنظّمة دولية للضغط باتجاه حفظ حقوق الفلسطينيّين، وكذلك تدريب الصّحفيين والناشطين والحقوقيين، على تركيز التغطية لقضايا الخصوصيّة، وانتهاك بيانات الفلسطينيّين الشخصيّة، كما أنّ وجود قانون خصوصيّة وحماية بيانات فلسطينيّ، يتواءم مع القوانين الدولية ويحمي الأفراد وينصفهم سيكون بمثابة نقلة نوعية، في مستوى مناقشة مثل هذه القضايا ولفت انتباه المجتمع الدّولي لها.[81]

نماذج من القطاع الخاص الفلسطينيّ

لأهمية ودور القطاع الخاص الفلسطينيّ، في قضايا الخصوصيّة وجمع ومعالجة البيانات الشخصيّة، تستعرض هذه الدراسة ثلاثة نماذج من شركات فلسطينيّة خاصّة، تقدّم خدماتها للفلسطينيّين، ولديها قدر كبير من البيانات الشخصيّة المرتبطة بهم، بحيث تعطي هذه النماذج نظرة قريبة عن واقع الخصوصيّة وحماية البيانات الشخصيّة في الشّركات والقطاع الخاص الفلسطينيّ. تغطي النماذج ثلاثة مجالات مهمة وذات علاقة بالخصوصيّة، والبيانات الشخصيّة للمستخدمين، وهي الاتّصالات، والدّفع الإلكتروني، والتّزويد بخدمات الإنترنت.

نموذج 1: شركة الدفع الإلكترونيّ مالتشات (MaalChat)

مالتشات هي شركة محفظة إلكترونية فلسطينيّة، توفّر خدمات الدفع الإلكترونية، وتمكّن المستخدمين من إدارة عمليات الدفع، وتسهيل عادات الإنفاق وتسهيل عمليات التسوّق والتّفاوض، وعقد الصّفقات، إضافة إلى خدمات تحويل وطلب الأموال، وهي شركة متخصّصة في التّكنولوجيا المالية، تسعى لتلبية احتياجات أفراد المجتمع من أجل تحقيق الشمول المالي.[82]

تعمل شركة مالتشات على جمع البيانات الأساسيّة والضرورية للاشتراك بخدماتها، مثل الاسم ورقم الهوية وتاريخ الميلاد وغيرها، كما أيّ مؤسسة أخرى ويتم التصريح بها من المستخدم مباشرة وبإذنه، وهي تخضع لموافقة العميل، بناء على سياسة الخصوصيّة المعلنة على الموقع أو التّطبيق، ومن خلال هذه البيانات، وحسب سياسة الشركة والاتفاقيات الموقّعة مع سلطة النقد، يتمّ التحقّق ما إذا كان المشترك موجودًا على قوائم الإرهاب أم لا. وفي الوقت الحالي يمكن الجزم بأنه لا يتوفّر لدى الشركة ما يمكن تسميته تحليل سلوك العملاء (analysis behavior)، بسبب عدم وجود الكمّ الهائل من البيانات، وكذلك بحاجة إلى تقنيات الذكاء الاصطناعي كالخوارزميات، ولكنْ مستقبلًا قد يكون بالإمكان التعرّف على توجّهات الزبائن الشرائية، ومن الجدير بالذّكر أنّ بيانات المستخدمين لا يستطيع أحد الوصول إليها سوى شخص واحد وهو مراقب وأمين على بيانات المستخدمين.[83]

وأكد أبو شملة[84] أنه يُمنع أن يسأل موظّف داخل الشركة عن بيانات أحد العملاء، فهو مخالف للنّظام

81. سمارو، ديما. مصدر سابق.

82. مالتشات. مالتشات-المحفظة الذكية. تاريخ الاسترداد: أيّار، 2021.

83. أبو شملة، محمود. مقابلة شخصيّة. نيسان، 2021.

84. المصدر السابق.

الداخلي من جهة، ولا يوجد هنالك قدرة تقنية على الوصول لبيانات مستخدم معيّن، إلّا من خلال الموظّف المسؤول عن حماية البيانات، فالنّظام المستخدم على أجهزة الشركة، لا يعطي صلاحيات لأي موظف، ولا حتّى لمدير الشركة، فهو بحاجة لتصريح لذلك، كما يعمل النظام على تسجيل كل عملية اطّلاع على بيانات المستخدمين، ويمكن العودة إليها بالضبط، في حال تمّت. ولا يتمّ التصريح بأية معلومات عن المشتركين، إلا إذا توفّر حكم قضائي، وحتّى الآن لم تطلب أي جهة حكوميّة بيانات دون إذن قضائي.

يتم تحليل البيانات المتوفّرة من خلال تطبيق الشركة بشكل جماعي، لمعرفة بيانات عامة وليست شخصيّة، واستخدامها في مجال الإعلانات كإرسال رسالة للعميل إذا كان يرغب بالاشتراك بخدمة معينة حسب اهتمامه، بحيث نحن مَن يقوم بإرسال هذه الرسالة، ولا نعطي رقم العميل إلى أيّ طرف ثالث. ولكن، في الوقت ذاته من حق الشركات الاستفادة من بيانات العملاء بالطرق المشروعة كمعرفة توجّهات المستخدمين السلوكية والشرائية، بما يتّفق مع سياسة الخصوصيّة لقاء ما تقدّمه من خدمة، لهم دون إجبارهم، وبشكل قانوني يحمي الطرفين.[85]

يتم بناء سياسات الخصوصيّة بناء على تعميمات وقوانين سلطة النقد بشكل أساسيّ (سرية البيانات والمحافظة عليها، والاحتفاظ بسجلات البيانات لفترة طويلة فيما يتعلّق بالمستخدمين أو التجار، والقانون ينصّ على الاحتفاظ بهذه البيانات لمدة 10 سنوات من آخر تعامل)، وهناك بعض التفصيلات، التي لها علاقة بسياسة الشركة نفسها واتفاقيات حماية المستهلك. تقوم سلطة النقد بدور الإشراف والمراقبة على حماية البيانات وأنظمة الشركة والتأكد من أننا نطبّق سياساتهم وشروطهم، فأحيانًا تطلب عيّنة عشوائية عن المشتركين الموجودين لدينا، من تجار ووكلاء بأرقام دون معلومات شخصيّة، حتّى تتأكد من أن كلّ شيء يسير بشكل قانوني، إلا أنّ سلطة النقد لا تصدر تعليمات دائمة حول حفظ البيانات والتعامل معها، وعدد الأشخاص الذين يمكنهم الاطلاع على البيانات وغيرها من التفاصيل.[86]

نموذج 2: شركة تزويد خدمات الإنترنت كول يو Call U

تأسست شركة كول يو عام 2009 لمزاولة نشاطها الخدماتي، في مجال التزويد بخدمات الإنترنت في فلسطين. تعمل الشركة مع مشتركيها من خلال شروط اشتراك، يتم إخبار المشترك بها، وهي متوفرة على الموقع الإلكتروني للشركة، وحسب عليان[87] مدير الشركة، يمكن القول إنّه لا يوجد شروط خصوصيّة ضمن اتفاقية موقعة بين طرفين. كما يوجد لدى الشركة نوعان من البيانات **أولا**: بيانات المشترك، مثل رقم الهاتف الاسم، السكن... إلخ، **وثانيا**: البيانات التي لها علاقة باستخدام المشترك للخدمة، وهي ساعات الاستخدام للإنترنت.

أحد مبادئ الشركة الحفاظ على سرّية البيانات الشخصيّة للمستخدمين، والجهة الوحيدة التي قد تطلب معلومات من الشركة، ويتمّ الإفصاح لها هي النيابة العامة بقرار قضائي، وبالعادة يتم طلب "IP" لشخص ما في ساعة معينة، ومن الذي كان يستخدمه، حيث يجبر القانون الشركة الاحتفاظ ببيانات الاستخدام لمدة 3 سنوات، عدا ذلك لا يوجد أيّ جهة يمكن تبادل بيانات الخصوصيّة معهم. علمًا أنه لا يوجد خوارزميات لتحليل سلوك الأشخاص، ولا تعلم الشركة طبيعة الاستخدام بل فقط كمية الاستخدام، فمثلًا، يمكن معرفة أنّ أحد المشتركين استهلك 15 جيجا لكن ماذا يوجد بداخلها لا تعلم الشركة ذلك.[88]

85. المصدر السابق.

86. المصدر السابق.

87. عليان، رائد. مقابلة شخصيّة. نيسان، 2021.

88. المصدر السابق.

بيانات المستخدمين موجودة فقط لدى موظف واحد داخل الشركة، ولا يستطيع أيّ أحد الاطلاع عليها، وهذا الموظف لديه تعليمات صارمة وإجراءات حول حماية البيانات، كذلك يستحيل رؤية شاشة حاسوب للشركة تتوفّر فيها معلومات كاملة عن المشتركين، فيتم ترميزها حتى لا يعرف الموظف اسم المشترك وإنما بعض أرقام هاتفه ليميّزه، حتّى عندما يتم إرسال رسالة تهنئة بالعيد للمشتركين يعمل النظام على انشائها وإرسالها SMS دون الاطّلاع على الأرقام والأسماء بطريقة أوتوماتيكية. كما تنفي الشركة استفادتها من البيانات ببيعها أو تبادلها مع أطراف ثالثة بتاتًا، وتقتصر الاستفادة من بيانات المستخدمين على ضبط الجودة، وخدمة المشتركين، كمعرفة توفّر الخدمة لدى بعض المشتركين. وتشير إلى دور الوزارة المحدود في متابعة قضيّة الخصوصيّة، الذي- أحيانًا- يقتصر على طلب الاطّلاع على بيانات المشتركين.[89]

نحو قانون خصوصيّة وحماية بيانات فلسطينيّ

تكمن أهمية وجود قانون فلسطينيّ، ناظم وشامل للخصوصيّة وحماية البيانات، في فرض تنظيم كامل للتعامل مع الخصوصيّة والبيانات الشخصيّة بشكل مفصّل، وتوفير رقابة وحماية كاملة، وتوزيع مهام ومسؤوليات واضحة، وهو ما يتّفق مع التزام فلسطين بالاتفاقيات الدولية، مثل "العهد الدولي الخاص بالحقوق المدنية". من جهة أخرى، أصبح من غير الممكن معالجة حقٍّ أساسي للفرد بهذا الحجم، من خلال نصوص عامة وتشريعات فضفاضة، فوجود قانون خصوصيّة منسجم بالكامل مع المعايير الدولية لبنة أساسية في المأسسة لنظام نزاهة وطني.[90]

ولا شك أن الحالة العصرية والتطورات التكنولوجيّة الهائلة، وقصور القوانين والتشريعات السابقة تستدعي ضرورة سنٍّ مثل هكذا قانون، وهو بدوره ما يعمل على حماية المواطنين من الجريمة وتقليل مستواها في المجتمع وسدّ ثغرة قانونية كانت تستبيح بيانات الفرد الشخصيّة، وتشجع انتهاكها واختراقها دون خشية من العقاب.[91] من جهة أخرى، فإنّ وجود قانون خصوصيّة وحماية بيانات يشكّل حماية للجهات، التي تمتلك المعلومات (قطاع خاص، أهلي، حكومي) وليس فقط للأفراد، حتى تعرف حدودها وما المسموح به وما الممنوع؛ للعمل بناء عليه، ولكن في غيابه قد تخترق الشّركة خصوصيّة الأفراد، وهي لا تعلم ما يقود لمشاكل قضائية وغيرها.[92]

وفيما يتعلّق بقرار مجلس الوزراء رقم (3) لسنة 2019 المتعلق بحماية البيانات الشخصيّة للمواطنين، لا يمكن اعتباره بمكانة "القانون"، فمن حيث قوة القوانين والتشريعات، يأتي أولًا الدستور، ثمّ القانون، ثمّ النظام، وأخيرًا القرارات، وهذا القرار لا يمكنه أن يلغي ما هو منصوص عليه في المستويات السابقة الأعلى منه، فقانون الجرائم الإلكترونيّة أقوى وأعلى منه، كما لا يمكن وضع عقوبات من خلال قرار مجلس وزراء ومعاقبة الأفراد، بناء على قرار مجلس الوزراء، فالعقوبة لا تفرض إلا بقانون، حسب المادة (15) في الدستور الفلسطينيّ، علمًا أنّ العقوبة غير واضحة وغير محدّدة، والأهم لا يمكن معالجة حقّ أساسي من خلال قرار؛ فلا بدّ من مأسسة الحق، كإصدار قانون لحماية البيانات، يعرف من هي الجهة المختصة لمتابعة الخصوصيّة، وهل لديها استقلال مالي وإداري، أم هي جزء من الهيكل الرسمي للحكومة، وما هي المهام والصلاحيات الموكلة لها، في تعاملها مع القطاعين العام والخاص، وما هي آليات الرقابة، التي تكفل إنفاذ هذا الحق، وماذا عن نظام الشكاوى، ومَن الذي يتابع نظام الشكاوى، ومدى فعالية نظام الشكاوى وموافقة كلّ ذلك للمعايير الدولية.[93][94]

89. المصدر السابق.

90. عابدين، عصام. مصدر سابق.

91. جبارين، شعوان. مصدر سابق.

92. أبو شملة، محمود. مصدر سابق.

93. جاموس، عمّار. مصدر سابق.

94. عابدين، عصام. مصدر سابق.

في حال السعي لمواءمة واستنساخ القانون الأوروبيّ؛ لحماية البيانات الشخصيّة في فلسطين، فإنّ هناك خطوتين مهمّتين، وأيضًا يمكن اعتبارهما عقبتين أساسيتين، أولاً: بحاجة لتعديل القوانين الفلسطينيّة المحلية، كقانون الجرائم الإلكترونية، وتعديل المواد التي قد تمسّ بالحقّ بالخصوصيّة، وهي بالأساس تتعارض مع اتفاقيات دولية وقّعت عليها السلطة الفلسطينيّة. ثانيا: محاولة رفع سيطرة الاحتلال على البنية التحتية بشكل كامل، وفرض سيادة فعلية للسلطة الفلسطينيّة، وهو الأمر المعقّد والمتّفق عليه في اتفاقيات مثل أوسلو، كما أن الاحتلال يفرض على الفلسطينيّين استخدام تطبيقات معينة، تخترق خصوصيتهم مثل فرض تطبيق "المنسق" على أكثر من 50 ألف عامل فلسطينيّ، يعملون في الداخل المحتل.[95]

يظهر مما ذكر سابقًا، بأنه لا يوجد جهة رقابية متخصّصة في فرض رقابة قانونية، على شركات القطاع الخاص و/أو مؤسّسات القطاع العام، كقانون تنظيمي كامل، يفصل المراحل التي يفترض أن يتم العمل بها ومن خلالها، بمعنى أنّ الاكتفاء بنصّ عقابي، تتحرّك بموجبه الجهات القضائية فقط إذا كانت ثمّة شكوى، يعدّ قصورًا في تطبيق مفهوم الخصوصيّة وحماية البيانات.[96] ويعتبر جبارين[97] وحماد [98] أنّ مستوى الرقابة على البيانات الشخصيّة للمستخدمين نادرًا، ولا يحوز على الاهتمام الكافي، وهذا ما ينطبق على واقع الضفة الغربية وقطاع غزة وعلى المؤسسات الحكوميّة والخاصة، كما أنّ الرقابة لا يجب أن تكون فقط حكوميّة، وإنما يجب توفير الرقابة الأهلية لحماية بيانات المواطنين.

أيضًا أصبح ضروريًّا تشريعُ قانون شامل، يساهم في تغيير الثقافة المجتمعية السائدة، حول الاعتياد على انتهاك الخصوصيّة، في المجتمع الفلسطينيّ، لذلك يجب أن تسبق عملية تشريع القانون عملية توعية مجتمعية بالخصوصيّة وحماية البيانات الشخصيّة، وأهميتها وضرورتها وأخلاقياتها، ثم يأتي القانون ليؤطّرها وينظّمها ويعمّق المعرفة بها، فلا يمكن تشريع قانون، لا يعلم المجتمع عنه شيئًا ويمارس عكسه تمامًا.[99] لذلك، أيضًا يجب إصدار القانون من خلال الإجراءات والقنوات القانونية المعتمدة في سن القوانين والتشريعات، ومن خلال مجلس تشريعي، دون تفرّد جهة حكوميّة أو سياسية، في صياغته وتحديد مضمونه، وبعد إجراء مشاورات كبيرة، مع المجتمع المدني، وشركات القطاع الخاص المعنية، حيث يحتاج مثل هذا القانون إلى إشراك كافة أطراف المجتمع الفلسطينيّ فيه.[100]

على المجتمع المدني الفلسطينيّ الضغط تجاه استقلال القضاء، والعمل على بناء القدرات والمهارات، واستقطاب النشطاء والفاعلين، وتدريبهم بحيث يكونون قادرين على قيادة المجتمع المدني، والضغط على الجهات الحكوميّة؛ للمساهمة في تخطي العقبات، التي تحول بين تشريع قانون شامل للخصوصيّة وتطبيقه واقعيًّا، ورفع الوعي بقضيّة الخصوصيّة وحماية البيانات مجتمعيًّا، وتنفيذ الحملات الإعلامية وحملات الضغط والمناصرة، على المستوى المحلي والدّولي، كتشكيل ائتلاف من منظّمات المجتمع المدني الفلسطينيّ، لخلق وزيادة الوعي الشعبي والمؤسّسات بأهميّة قضيّة الخصوصيّة للفلسطينيّين، بشكل خاص وفي سياق الواقع الاحتلالي، الذي يحاول السيطرة على كافة بيانات الفلسطينيّين بشكل عام.[101]

95. سمارو، ديما. مصدر سابق.
96. عابدين، عصام. مصدر سابق.
97. جبارين، شعوان. مصدر سابق.
98. حماد، حسين. مصدر سابق.
99. عليان، رائد. مصدر سابق.
100. جاموس، عمّار. مصدر سابق.
101. سمارو، ديما. مصدر سابق.

ملامح قانون الخصوصيّة وحماية البيانات المنشود فلسطينيًّا

ويمكن إجمال بعض النقاط الأساسيّة، التي أشارت إليه عيّنة الدراسة بطريقة مباشرة أو غير مباشرة، للاعتماد عليها وإرشادات أساسية للمساهمة في تحديد معالم قانون خصوصيّة، وحماية بيانات فلسطينيّ شامل، علمًا أن هذه النقاط لا تلغي دور الجهات القضائية وجهات الاختصاص وتفصيلاتها، وإنّما هي لتسليط الضوء على أبرز محاور القانون:

- التزام كامل بكلّ ما ورد في الإعلان العالمي لحقوق الإنسان، العهد الدولي الخاص بالحقوق المدنية والسياسية، ومواءمة كل من التشريعات والسياسات العامة والتطبيقات القضائية الفلسطينيّة معها ومع قانون الخصوصيّة وحماية البيانات الأوروبي (GDPR).
- فهم والمطالبة بتحقيق مبدأ الحق في النسيان الرقميّ وإتاحة خيار حذف البيانات الشخصيّة بعد الانتهاء منها، أو في حال لا يوجد ضرورة لوجودها. يجب أن تكون ثمة ضوابط تمنع إساءة استخدام البيانات التي لا يمكن محوها من الأرشيف الرقمي، لمؤسسات وشركات ومواقع، وفرض عقوبة على مَن يخالف ذلك، ويستخدم بيانات شخصيّة، ولو بعد مئة عام، فبيانات المستخدمين، لدى شركات الاتصال الفلسطينيّة لا يتم حذفها ولا نستطيع إجبارهم على حذفها دون قانون، حيث إنّ القانون الحالي يجبرها على الاحتفاظ ببيانات المستخدمين بعد انتهاء الخدمة.
- إعطاء تعريفات واضحة حول الجهة المختصة المستقلة المعنية بمتابعة ملف الخصوصيّة والبيانات الشخصيّة في الدولة، هل لديها استقلال مالي وإداري، أم هي جزء من الهيكل الرسمي للحكومة، ما هي مهامها ومسؤولياتها تجاه القطاعين العام والخاص، ما هي آليات الرقابة الفعالة لضمان احترام هذا الحقّ، كيف ستعمل على نظام شكاوى وعقوبات فعال.
- عدم استخدام مصطلحات عامة وفضفاضة، يجب أن يكون القانون واضحًا ومحدّدًا، وتحديد طبيعة الجرائم، التي يمكن ارتكابها في سياق الخصوصيّة والبيانات الشخصيّة وتحديد طبيعة التعامل معها.
- من أهم العناصر، التي يجب أن يقوم عليها القانون نظام عقوبات واضح لكافة الجرائم، التي قد ترتكب مع تنوّع العقوبات وتشديدها، بحيث لا تكون فقط مادية، وكذلك توفير نظام للمساءلة الجنائية حول انتهاك الحق في الخصوصيّة، من قبل موظفي الدولة أو شركات القطاع الخاص.
- وضع معايير صارمة ومحددة بالقانون للجهات، التي لديها الإذن بحفظ البيانات للمستخدمين ومعالجتها وحفظها.
- احترام حقوق الإنسان بشكل عام، احترام الحقّ في حرية الرّأي والتعبير، والحق في الوصول إلى المعلومات، واحترام الحريات الخاصة والثقافات الخاصة.
- تحديد مسؤوليات ومهام وشروط للأشخاص، الذين يفترض أن يكون لديهم وصول لبيانات المستخدمين والمشتركين، ومواصفات الأشخاص القادرين على الوصول لهذه البيانات، وكيف يجب أن يتعامل الموظفون مع هذه البيانات الشخصيّة.
- تحديد مسؤولية الإشراف على الالتزام بخصوصيّة البيانات، وكيف يتم التعامل مع البيانات الشخصيّة داخل الجهات الحكوميّة والقطاع الخاص، وكيف يتم استخدامها، ومتابعة دائمة لأي حالات انتهاك للخصوصيّة، والأفضل عادة ألا يتم إعطاء صلاحيات واسعة في التعامل مع البيانات الخاصة.
- يجب تنظيم عملية التصريح بالبيانات لأي طرف ثالث، وفق القانون وأن تكون بإذن واضح وصريح من صاحب البيانات نفسه، وبحاجة لضبط ما يمكن الطلب من صاحب البيانات التصريح به، ولأي

غرض، فهناك أغراض لا يجب أن يطلب من مالك البيانات التصريح بها، لعدم إدراكه بأضرارها على خصوصيته.

يجب أن يضمن القانون الفلسطيني المنشود، على غرار نظيره الأوروبي، مجموعة من الحقوق مثل: الحق في النفاذ إلى البيانات، وهو ضمان حقّ المستخدمين بالحصول على تأكيد إذا جُمعت بياناتهم أو أُستخدمت، ولأي غرض إلى جانب معرفة هويّة المُنفّذ. والحقّ في الاعتراض، وضمان حقّ المستخدمين بالاعتراض على جمع ومعالجة بياناتهم. والحقّ في المحو والنسيان، لضمان حق المستخدمين بطلب حذف بياناتهم الشخصيّة، عند مغادرتهم الخدمة أو التطبيق. والحق في التصحيح والتعديل، ضمان حقّ المستخدمين بطلب تعديل بياناتهم الشخصيّة وتحديثها، والتأكد من دقّتها. والحقّ في المعلومة، وضمان حق المستخدمين بتلقي معلومات واضحة ومفهومة، حول نشاط وطبيعة استخدام بياناتهم، من الجهات التي تملكها. والحقّ في الاستفسار، وضمان حق المستخدمين بالاستفسار عن أهداف جمع ومعالجة البيانات، وحقّهم بمعرفة النتائج، التي توصلت إليها الجهات التي عملت على تحليل البيانات، من خلال الخوارزميات وغيرها، إلى جانب معرفة القرارات التي ترتبت عليها.

التوصيات

بعد التعمّق في قضيّة الخصوصيّة وحماية البيانات الشخصيّة في فلسطين وواقعها، وما هو المأمون منها، تقدّم هذه الدراسة بعض التوصيات المهمة، المستوحاة من نقاشات الأشخاص، ذوي العلاقة وتحليل عينة الدراسة، ويمكن إيجازها على النحو التالي:

- **تشكيل هيئة فلسطينيّة لحماية وتنظيم الخصوصيّة والبيانات الشخصيّة**

ضرورة إيجاد جهة تكون أقرب إلى صفة المراقب العام للخصوصيّة، وحماية البيانات في فلسطين تتمتّع بموثوقية عالية، تكون مرجعيتها المجلس التشريعي الفلسطينيّ، تعمل على تطبيق وإنفاذ القانون، الذي يفترض أن ينظّم ويحمي خصوصيّة الفلسطينيّين، وجمع ومعالجة بياناتهم، فمثلًا على وزارة الاتصالات فرض سياسات خصوصيّة ورقابية مشدّدة، بالتشاور مع هذه الجهة، كما تعمل جهة المراقب العام على الإشراف ومراقبة الالتزام بسياسات الخصوصيّة، خلال أداء الشركات والمواقع الإلكترونية، في القطاعين العام والخاص، وفي السياق المحلي والدولي، ومن أجل مأسسة هذه القضيّة، يجب أن يتمّ تحديد ما هي المهام التي يجب على الجهة المختصة بمتابعة الخصوصيّة والبيانات الشخصيّة أن تقوم بها، وما هي صلاحياتها، وما نظام المراقبة المتّبع، ونظام الشكاوى، الذي يسمح للمواطنين المطالبة بحقوقهم، والتّبليغ عن انتهاكات الخصوصيّة، التي قد يتعرّضون لها.

- **يوصي مركز حملة بضرورة إقرار قانون الخصوصية وحماية البيانات**؛ لحماية المواطنين من الانتهاكات الواقعة عليهم من مختلف الأطراف، بالتّشاور مع المجتمع المدني والجهات المختصة ذات العلاقة، وذلك بعد التعجيل بإجراء الانتخابات التشريعية، بصفة المجلس التشريعي صاحب الاختصاص الأصيل بالتشريع. إلى ذلك الحين، يطالب مركز حملة بتطبيق القاعدة الدستورية الواردة في نصّ المادة رقم (32) على كل انتهاك للخصوصية الإلكترونية وللبيانات الشخصية، التي تعتبر أي اعتداء على حرمة الحياة الخاصة للإنسان جريمة، لا تسقط الدعوى الجنائية ولا المدنية عنها بالتقادم.

- **التوعية بقضيّة الخصوصيّة وحماية البيانات في فلسطين شعبيًّا ورسميًّا**

على كافة الجهات المعنية، ابتداءً من مؤسسات المجتمع المدني والجهات الحكوميّة المعنية، وحتى المؤسسات الدولية العاملة في فلسطين العمل على توعية الجمهور الفلسطينيّ بقضيّة الخصوصيّة وحماية البيانات، وأهميتها وخطورتها وتأثيراتها وأبعادها، وعقد الندوات والدورات والتدريبات، واستدعاء

الخبراء والفنيين لمناقشة القضيّة، من زوايا أكثر تقنية، وأن يتم مأسسة ذلك، من خلال الدراسات والأبحاث والإنتاج العلمي، وكذلك إدخال بعض المواضيع والمساقات إلى طلبة الجامعات وخاصة كليات الإعلام والاتصال والقانون وعلوم الحاسوب، والدعوة لعمل الأبحاث والدراسات بهذا الجانب، والتعمق فيه ودراسة كافة جوانبه وتطوراته وتقنياته ومقارنة الواقع الفلسطينيّ بالسياق العالمي في قضيّة الخصوصيّة.

من جهة أخرى، وتتفق توصيات هذه الدراسة بشكل خاص مع ما أوصت به الدراسات السابقة، من حيث ضرورة قيام المنظمات الدولية بواجبها تجاه هذه القضيّة وتوعية الجمهور والمستخدمين بأبعاد القضيّة، وكيفية حماية خصوصيتهم الرقمية وطرق ذلك، من خلال حثّ الدول على العمل على مشاريع مشتركة، والضغط على الدول لسنّ مثل هذه القوانين، كما طالبتها بفرض عقوبات دولية تنفذ على كافة المخالفين لقانون الخصوصيّة في أي دولة كانت واعتبار ذلك من أساسيات قيام الديمقراطيات في العالم.

ملحق 1:

جدول 2: عينة المقابلات المعمّقة وعلاقتهم بموضوع البحث

الرقم	الاسم	الصفة الاعتبارية
1	إياد الزيتاوي	المدير التنفيذي لمجموعة الاستقرار المالي، ومدير مكتب إدارة المخاطر في سلطة النقد الفلسطينيّة.
2	عبد المنعم فطافطة	خبير السوشيال ميديا والتسويق الرقمي.
3	شعوان جبارين	مدير مؤسسة الحق الفلسطينيّة لحقوق الإنسان.
4	إبراهيم أبو بكر	رئيس مركز الاستجابة لطوارئ الحاسوب، في وزارة الاتصالات الفلسطينيّة.
5	حسين حماد	ممثلًا عن مؤسسة الميزان لحقوق الإنسان – غزة.
6	ديما سمارو	محامية وخبيرة في الحقوق الرقمية، في منطقة الشرق الأوسط وشمال إفريقيا. سابقا محللة سياسات ـ الشرق الأوسط وشمال أفريقيا في منظمة أكسس ناو.
7	د. عصام عابدين	أكاديمي وخبير حقوقي.
8	رائد عليان	مدير شركة Call You لخدمات الإنترنت.
9	محمود أبو شملة	المدير التنفيذي لشركة الدفع الإلكتروني Maalchat.
10	عمّار جاموس	ممثلًا عن الهيئة المستقلة لحقوق الإنسان والمتابع لملف الخصوصيّة وحماية البيانات في فلسطين.

ملحق 2:

جدول 3: توزيع عينة المجموعات المركزة

الحيّز الجغرافيّ	عدد الأفراد	مدة الجلسة	ذكر	أنثى
الضفة الغربيّة	16	2	6	10
قطاع غزة	15	2	8	7
شرقيّ القدس	14	2	6	8
المجموع	**45**	**ساعات 6**	**20**	**25**

تواصلوا معنا

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

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