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

دليل الأمان الرّقميّ والخصوصيّة في الاحتجاجات السِّلميّة

كانون الأوّل 2021

حملة - المركز العربيّ لتطوير الإعلام الاجتماعيّ
دليل الأمان الرّقمي والخصوصيّة في الاحتجاجات السّلميّة

باحث رئيسيّ: فراس طويل
باحثة مساعدة: بثينة سفاريني
مراجعة قانونيّة: عبير بكر
نقله إلى الإنجليزيّة: شركة رتاج للحلول الإداريّة
تصميم: أمل شوفاني

تمّ إنجاز هذا الدّليل بالشّراكة مع مؤسّسة برايفسي إنترناشونال
ضمن مشروع مواءمة دليل "الحرّيّة بالاحتجاج" (Free To Protest)، الخاصّ بالمؤسّسة الشّريكة.

ملاحظة مهمّة: المعلومات الواردة في هذا الدّليل ليست شاملة، ولا يمكن اعتبارها نصائح ذات صِبغة قانونيّة.

نتطلّع لتواصلكنّ وتواصلكم معنا عبر القنوات التالية:
البريد الإلكتروني: info@7amleh.org
الموقع الإلكتروني: www.7amleh.org
الهاتف: 0774020670 972+
تابعونا عبر صفحاتنا على منصات الإعلام الاجتماعيّة: **7amleh**

مقدمة

في السّنوات الأخيرة، ازدادت وتيرة الاحتجاجات السّلميّة الفلسطينيّة، في الضّفة الغربيّة وقطاع غزّة والقدس والدّاخل، مثل احتجاجات حي الشّيخ جراح في القدس، ضدّ التّهجير القسريّ، واحتجاجات جبل صبيح في قرية بيتا في الضّفة الغربيّة، ضد الاستيطان غير القانونيّ، والاحتجاجات السّلميّة ضدّ قمع الشرّطة وجرائم القتل، في مدن وقرى الدّاخل، واحتجاجات مسيرة العودة في قطاع غزّة. في المقابل ازدادت نسبة الانتهاكات ضدّ المحتجّين، من اعتقالات وقمع بشكل عام، والانتهاكات الرّقميّة كاختراق الهواتف، وانتهاك الخصوصيّة، والوصول للمعلومات الرّقميّة دون إذن، والرّقابة على حرّية التّعبير، عبر الإنترنت، بشكل خاص.

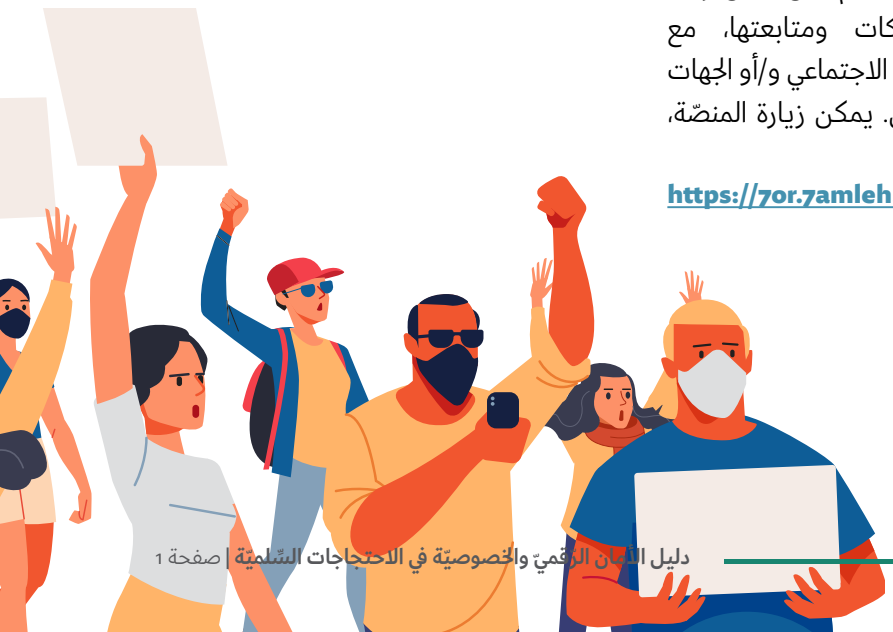
يأتي هذا الدّليل نتيجة شراكة مع مؤسسة برايفسي إنترناشونال (Privacy International)، الّتي عملت خلال السّنوات الماضية على تطوير دليلٍ مُختصرٍ وفعّال، حول الأمان الرّقمي، وحماية الخصوصيّة في الاحتجاجات السّلميّة. بدوره، قام مركز حملة بمواءمة وإعادة صياغة وتصميم الدّليل المذكور، من خلال عمليّة بحث ميدانيّ، تضمّنت خمس مقابلات فرديّة، مع صحفيين/ات وناشطين/ات ومدافعين/ات فلسطينيين/ات عن حقوق الإنسان، ممّن تواجدوا/ن في الاحتجاجات السّلميّة، في كلٍّ من الضّفة الغربيّة وقطاع غزة والقدس والدّاخل، خلال العامين المنصرمين، بالإضافة لثلاث مجموعات تركيز، ضمّت كذلك ناشطين/ات وصحفيين/ات، من الضّفة الغربيّة وقطاع غزّة والقدس ومناطق الدّاخل، كلّ منطقة على حِدَة. يحتوي الدّليل على ثلاثة أقسام: دليل خصوصيّة الهواتف، أثناء الاحتجاجات السّلميّة، ودليل خصوصيّة الوجه والجسد، أثناء الاحتجاجات السّلميّة، ودليل قواعد بيانات الشّرطة والشّرطة التنبؤيّة.

مرصد انتهاكات الحقوق الرقمية (حُـر)

منصّة "حُر"

المرصد الفلسطيني للانتهاكات الرّقميّة في حال التّعرض لأي انتهاك رقميّ، كالاختراق وانتهاك الخصوصيّة والرّقابة على حرّيّة التّعبير، يقدّم مركز حملة، عبر مِنصّة "حُر" الدّعم، من خلال رصد وتوثيق الانتهاكات ومتابعتها، مع شركات التّواصل الاجتماعي و/أو الجهات المختصّة الأخرى. يمكن زيارة المنصّة، من خلال الرّابط:

https://7or.7amleh.org



دليل حماية خصوصيّة أجهزة المحتجّين/ات

ما هي الأساليب والتقنيّات التي قد يتمّ استخدامها، في الضّفة الغربيّة وقطاع غزة والدّاخل، لمراقبة أجهزة المحتجّين/ات؟

مصادرة الأجهزة واختراقها

في السّنوات الأخيرة، بلّغ/ت الكثير/ات من المحتجّين/ات عن تعرّضهم/ن لمصادرة هواتفهم/ن الخاصّة، خلال الاحتجاجات السّلميّة في الضّفة الغربيّة وقطاع غزّة والقدس والدّاخل. من الشّائع استهداف مشاركين/ات، يرفعون/ن هواتفهم/ن للتّصوير أثناء الاحتجاج. قد تتمّ مصادرة الهواتف -أيضًا- في حال التّعرّض للاعتقال. في حال توفّر الوصول المباشر للجهاز- في العادة- تلجأ الجهات المعنيّة إلى اختراق الهواتف من خلال تقنيّات "استخراج البيانات من الهاتف المحمول" (Mobile Phone Extraction)، وهي برامج تتيح القدرة لمن ي/تستخدمها على استخراج البيانات من الهواتف المقفلة، دون إذن صاحب/ة الهاتف، ودون الحاجة لمعرفة الرّمز السّري. تُصنّع شركة Cellebrite الإسرائيلية أحد أشهر برامج استخراج المعلومات من الهاتف المحمول، وتزوّد العديدُ من الحكومات -حول العالم- أجهزةَ الشّرطة الخاصّة بها بهذه البرامج.

يمكن من خلال تقنيات MPE الوصول إلى:

- قائمة الاتصال.
- سجل الاتّصال (الأشخاص الذين اتصّلت بهم/ن ومتى).
- سجل الرّسائل (فحوى الرّسائل ولمن أرسلتها ومتى).
- الملفات المحفوظة (صور، فيديوهات، تسجيلات صوتية، ملفات، إلخ...).
- معلومات التّطبيقات (التّطبيقات على جهازك، والمعلومات المخزّنة فيها).
- سجل موقع الهاتف (المواقع الّتي تواجدت فيها والهاتف بحوزتك).
- سجل اتّصالات الشّبكات اللاسلكيّة Wi-Fi، ما قد يكشف أيّ موقع قمت فيه بالاتّصال بأيّ شبكة لاسلكيّة (Wi-Fi).
- يمكن لبعض تقنيّات استخلاص المعلومات الوصول للبيانات المرفوعة على "الغيمة" أو الـ cloud، أو مواد لا تظهر للمستخدم أو موادّ محذوفة.

لا يمكن استخدام تقنيّات استخراج المعلومات دون وصول مباشر للهاتف، أي أنّه لا يمكن للعمليّة أن تتمّ عن بُعد، أو عبر الاتّصال اللاسلكيّ.

أمور يمكن أخذها بالاعتبار، فيما يتعلّق بتقنيّات MPE:

- تحديث نظام تشغيل الهاتف (Android أو iOS) يضمن توفّر أحدث تقنيات الحمايّة على الجهاز، علمًا أنّ برامج الاختراق تعمل عادةً على استغلال الثّغرات في أنظمة التّشغيل غير المحدّثة.
- يساهم استخدام رمز سرّي قوّي في حماية الهاتف من الاختراق. بينما تستطيع بعض تقنيّات استخراج البيانات تخطّي كلمة السّر، إلّا أنّ القدرة على ذلك تعتمد على نوع الهاتف ونظام التّشغيل.
- توفّر معظم الهواتف الذّكيّة إمكانية عمل نسخة احتياطية (Back-up) ومن ثم حذف البيانات عن الهاتف. علمًا أنّه قد تستطيع بعض البرمجيّات الوصول إلى البيانات المحذوفة.
- تقوم بعض التّطبيقات بتخزين نسخ احتياطيّة، عن بيانات المستخدم (كبيانات الموقع والرّسائل) تلقائيًّا على الغيمة (cloud). في حال الوصول المباشر لهاتف ما ولو كان مقفلًا، يمكن استخدام برمجيّات الاختراق للوصول إلى البيانات المخزّنة على الغيمة، سواء تلك المرفوعة من قبل المستخدم مباشرة أو عن طريق التّطبيقات. يشمل ذلك الرّسائل المتبادلة عبر التطبيقات المشفّرة كـ WhatsApp في حال تمّ تفعيل خاصيّة النّسخ الاحتياطي، من قبل المستخدم. كما يشمل ذلك سجل الموقع Location، على بعض تطبيقات المحادثة أو التّوصيل.

تتبّع موقع الهاتف

خلال العام الماضي، بلّغ/ت العديد من المتظاهرين/ات عن تلقّيهم/ن رسائل قصيرة تحذّرهم/ن من التّواجد في مناطق احتجاج. شمل ذلك مناطق في قطاع غزّة، مثل مسيرة العودة الكبرى، ومناطق في الضّفة الغربية، مثل قرية بيتا ومناطق في أراضي الدّاخل ومدينة القدس.

يمكن تعقّب موقع الهاتف من خلال الشّريحة المتّصل بها، إمّا بشكل مباشر من البيانات لدى شركات الاتّصال، أو بشكل غير مباشر، من خلال عدّة تقنيّات، أبرزها تقنيّة IMSI Catcher، الّتي تعمل على رصد شرائح الهاتف في منطقة معيّنة، من خلال اعتراض اتّصالها مع أبراج الإشارة. كما يمكن تعقّب الهواتف باستخدام خاصيّة الـ GPS، الّتي تستعمل الأقمار الصّناعيّة، لتحديد موقع الهاتف، من خلال رقاقة مثبّتة في الجهاز نفسه.

أمور يمكن أخذها بالاعتبار، فيما يتعلّق بتقنيّات تعقّب موقع الهاتف:

- يمكن إيقاف خاصيّة الـ GPS على الهاتف المحمول يدويًّا، في أيّ وقت. في حال توفّر الوصول المباشر للجهاز، يمكن استخدام تقنيّات الاختراق، للوصول إلى سجلّ بيانات الموقع، الّتي قد تشمل أيّ موقع، تواجد فيه المستخدم سابقًا، دون إيقاف خاصيّة الـ GPS.
- تقوم بعض التّطبيقات بتخزين بيانات الموقع على حساب المستخدم على الإنترنت. يمكن اختراق تلك الحسابات عن بُعد، دون الحاجة للوصول إلى الهاتف مباشرة. يمكن تعطيل خاصيّة تتبّع الموقع على جميع التّطبيقات يدويًّا. لا يتمّ حفظ بيانات المستخدم على الإنترنت، في حال استخدام تلك التّطبيقات كـ "زائر" عوضًا عن إنشاء حساب.
- يصعب على البرمجيّات تعقب الهاتف، في حال تفعيل وضع الطيران أو إغلاق الهاتف أو تعطيل خاصيتيّ الـ Wi-Fi والـ Bluetooth . علمًا أنّ وضع الطّيران لا يعطّل - بالضّرورة- خاصيتيّ الـ GPS والـ Bluetooth.
- بينما يمكن اعتراض إشارة الهاتف، والوصول للرّسائل القصيرة SMS، أو اختراق سجلّات بعض تطبيقات المحادثة، حيث توفّر تطبيقات المحادثة المشفّرة مثل Signal أو Telegram خصوصيّة أعلى.

مراقبة منصّات التواصل الاجتماعي

في السنوات الأخيرة، كان تتبّع منصّات التّواصل الاجتماعي ومراقبتها أحد أكثر التّقنيّات ذات الأثر المحسوس على المحتجّين/ات، في الضّفة الغربيّة وقطاع غزة والدّاخل والقدس. من خلال مسح منصّات التّواصل الاجتماعي، وجمع المعلومات والمواد المنشورة، من قِبل أو عن أشخاص محدّدين أو أحداث معيّنة، وتخزين وتحليل تلك البيانات، ومقارنتها ببيانات مخزّنة مسبقًا، تصبح الجّهات المعنيّة قادرة على بناء ملفّات وسجلّات عن أشخاص و/أو مجموعات و/أو أحداث، تساعدهم/ن في تعقّب الناشطين/ات، وتوقّع الاحتجاجات، وكشف هويّات المتواجدين/ات فيها، ما قد ينتهي - في عديد من الحالات- بالاعتقال قبل أو أثناء أو بعد الاحتجاج، أو في إحباط الاحتجاجات، ومنعها من الحدوث من الأساس.

كيف يمكن مراقبة التّواصل الاجتماعي، فيما يتعلّق بالاحتجاجات السّلميّة؟

- يستخدم منظّمو/ات الاحتجاجات -عادة- منصّات التّواصل الاجتماعي، لتنظيم الفعاليات والدّعوة إليها، أو لنشر توثيق (صور أو فيديو) من الموقع. يمكن لأي جهة معنيّة تجميع وتحليل هذه المنشورات، للتّوصل لمواقع ومواعيد الاحتجاجات وتعقّب هويّات المنظمين/ات والمشاركين/ات وانتماءاتهم/ن.
- قد ينشر بعض المشاركين/ات صورًا وفيديوهات من الاحتجاج، بعد فترات طويلة. قد يتم استخدام جميع تلك المنشورات، سواء كانت قديمة أو متعلّقة بفعاليّة في المستقبل، لتحديد هويّات المتواجدين/ات.
- من الممكن استخدام تقنيّات تحديد الوجوه؛ لمعرفة هويّات أشخاص يظهرون/ن في صورة أو فيديو.

أمور يمكن أخذها بالاعتبار، فيما يتعلّق بتقنيّات مراقبة منصّات التّواصل الاجتماعي:

- يمكن تعقّب هويّات الأشخاص الظّاهرين/ات في صور وفيديوهات، من خلال تقنيّات تحديد الوجوه، أو خاصية الـ tag أو الإشارة التي تدلّ على حساب المستخدم/ة الإلكتروني وغيرها من التّقنيات.
- في حال النّشر عبر إحدى منصّات التّواصل الاجتماعي دون تعطيل خاصيّة "تعقّب الموقع" على التّطبيق المُستخدم، تستطيع بعض برمجيّات التعقّب رصد المنشورات التي تتم مشاركتها في منطقة وزمن محدّدين، كموقع وزمن الاحتجاج مثلًا.
- يقوم تطبيق الكاميرا، في معظم الهواتف الذّكية، بتخزين موقع التقاط الصّورة. يمكن تعطيل تلك الخاصيّة يدويًا من الإعدادات.
- يتمّ تخزين بيانات، مثل موقع وتاريخ ووقت التقاط الصّورة، والجهاز المستخدم لذلك، في معلومات الـ EXIF المرتبطة بالصّورة. يمكن مسح معلومات الـ EXIF قبل نشر أي صورة على منصات التّواصل الاجتماعي من خلال "خصائص" الصّورة.

اختراق الهواتف عن بُعد

تعتمد برمجيّات اختراق الهواتف (hacking) على استغلال ثغرات في أنظمة الهواتف، للوصول للبيانات المخزّنة عليها. يمكن استخدام تقنيّات متنوعة لاختراق الهواتف، قد يعتمد بعضها على الاحتيال على صاحب الهاتف عن بُعد، من خلال الضّغط على روابط خبيثة (phishing) وغيرها من التّقنيات.

أمور يمكن أخذها بالاعتبار، فيما يتعلق باختراق الهواتف:

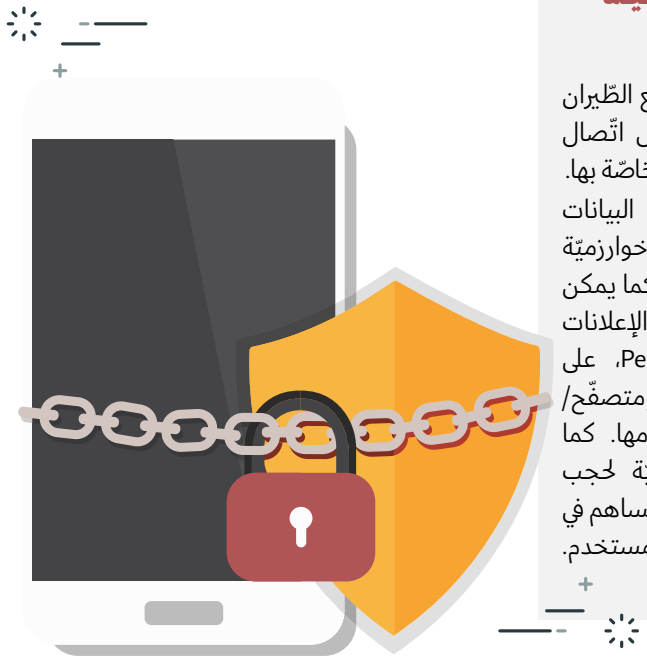
- كلّما كانت النّسخة المستخدمة لنظام تشغيل الهاتف أحدث، تمتّع الجهاز بنسبة خصوصيّة وأمان أعلى.
- كلّما كانت النّسخة المستخدمة -لأي تطبيق على الهاتف- أحدث، زادت نسبة الحماية والخصوصيّة خلال استعمال التّطبيق.
- تُعدّ الرّوابط الخبيثة (phishing) واحدة من أكثر الطّرق شيوعًا لاختراق الهواتف عن بُعد. قد تظهر تلك الرّوابط على شكل نوافذ pop-up أو ضمن رسائل قصيرة، أو رسائل البريد الإلكتروني وغيرها. عادة ما تحتوي تلك الرّسائل على عروض مُغرية، تهدف لحمل المستخدم على النّقر على الرّابط بسرعة، مثل إعلانات عن جوائز ماليّة و/أو مسابقات ضخمة. يتمّ نشر الرّسائل عبر حسابات وهميّة، أو من حسابات تمّ اختراقها، الأمر الّذي قد يدفع البعض على النّقر على روابط قد تصلهم/ن من أصدقائهم/ن ومعارفهم/ن المقرّبين.
- يمكن التأكّد من هوية المُرسل/ة على تطبيق معيّن، أو من جديّة رسالته/ا، من خلال مراسلتهم/ن عبر تطبيق آخر.

تحديد الهُويّة من خلال "معرّفات الهاتف"

لدى كلّ هاتف معرّفات مميزّة، يمكن من خلالها تحديد الهاتف وهُويّة صاحب/ته. يشمل ذلك وحدة تعريف المشترك أو "شريحة الهاتف" (SIM Card)، الّتي تحمل بيانات عن هُويّة المستخدم/ة، ورقم الهوية الدّولية لمشترك الجوّال (IMSI)، وهو رقم دوليّ، مرتبط بـ "الشّريحة"، ولا يتغيّر في حال نقل الشّريحة إلى جهاز آخر، ويكون مرتبطًا باسم المستخدم/ة وأحيانًا عنوانه/ا، بالإضافة لرمز الهويّة الدّوليّة للأجهزة المتنقّلة (IMEI)، وهو رمز مرتبط بالجهاز نفسه، يتغيّر من جهاز إلى آخر، وقد يحمل بيانات عن اسم وعنوان صاحب الجهاز أو طراز الجهاز. كما قد تشمل تلك المحدّدات سجلّ بيانات الإعلانات (Advertising ID)، وهو ملف ينتجه نظام تشغيل الهاتف لعرض إعلانات مخصصة للمستخدم/ة، وقد يرتبط ببيانات شخصيّة عن المستخدم، مثل الاسم وسجل الموقع والمواقع الإلكترونية، الّتي ت/يزورها. يمكن مسح وتحديث الـ Advertising ID يدويّا من خلال إعدادات الهاتف.

أمور يمكن أخذها بالاعتبار، فيما يتعلّق بمعرّفات الهاتف:

- إغلاق الهاتف أو وضعه في وضع الطّيران يحدّ من قدرة تقنيّات اعتراض اتّصال "الشّريحة"، والوصول للبيانات الخاصّة بها.
- بإمكان المستخدم/ة مسح البيانات المخزّنة على هاتفه/ا، لتغذيّة خوارزميّة الإعلانات يدويًّا، وفي أيّ وقت. كما يمكن للمستخدم/ة تعطيل خاصيّة الإعلانات المخصّصة Personalized Ads، على الهاتف عامةً وعلى التّطبيقات ومتصفّح/ات الإنترنت، الّتي ي/تستخدمها. كما تتوفّر تقنيّات خاصّة ومجّانيّة لحجب الإعلانات Ad blocker، التي قد تساهم في الحفاظ على خصوصيّة بيانات المستخدم.



دليل حماية خصوصيّة وجوه وأجساد المحتجّين/ات

ما هي الأساليب والتقنيّات التي قد يتمّ استخدامها، في الضّفة الغربيّة وقطاع غزة والدّاخل، لتعقّب وجوه وأجساد المحتجّين/ات؟

تقنيّات تعقّب الوجه والجسد

تعمل تقنيّات تحديد الوجوه (Facial recognition technology) على جمع وتحليل بيانات مرتبطة بوجوه الأفراد، من خلال التقاط صور لوجوههم/ن ومقارنتها بقوائم وقواعد بيانات جاهزة. مثلًا، تستعمل السلطات الإسرائيلية كاميرات المراقبة، في الأراضي الفلسطينية المحتلة والدّاخل ومدينة القدس، لتحديد هويات المحتجّين/ات. تنتشر هذه الكاميرات بكثافة في الأحياء الفلسطينيّة في القدس وفي مناطق "التّماس" والحواجز العسكريّة في الضّفة الغربية، وعلى السّياج الفاصل على حدود قطاع غزّة الشّمالية. تستخدم تلك الكاميرات في تحديد هويّات المتواجدين/ات في تلك المناطق، من خلال مقارنة الصّور الملتقطة مع قواعد بيانات جاهزة، تحتوي على بيانات وجوه و/أو بصمات عين الفلسطينيين/ات. علمًا أن العديد من الفلسطينيين/ات يقدمون/ن بيانات بصمة العين والإصبع الخاصة بهم/ن سنويًّا للسّلطات المختلفة. في الضّفة الغربيّة يُطلب - في معظم الأحيان- من الفلسطينيين/ات الراغبين/ات بالحصول على تصريح للعمل أو الزيّارة، في أراضي الدّاخل تزويد السلطات ببصمة العين والإصبع، وفي قطاع غزّة يقدّم العديد من المواطنين معلوماتهم/ن تلك بهدف الحصول على المنحة القطريّة. قد تستخدم هذه التّقنيّات لتحليل صور وفيديوهات مباشرة أثناء التقاطها أو مواد قديمة.

أمور يمكن أخذها بالاعتبار، فيما يتعلّق بتقنيّات تعقّب الوجه والجسد:

- تستطيع تقنيّات تحديد الوجه تمييز هويّات الأشخاص، من خلال التقاط مجموعة من الملامح المميّزة لوجوههم/ن. عادةً ما تكون تلك التّقنيّات أقلّ قدرةً على تحديد الهويّات، في حال عدم قدرتها على تحديد ملامح الوجه، بسبب ارتداء الأفراد للنّظارات أو الأقنعة الطّبيّة أو الاثنين معًا.
- يحقّ للشّرطي أن يطلب من أيّ مواطن نزع أيّ غطاء للوجه، لكن قد تتغيّر تلك القواعد، في سياق جائحة كورونا.
- تتيح بعض أدوات تعديل الصور والفيديوهات القدرة على تخفيض جودة تلك المواد و/أو تغبيش أجزاء معينة منها. علمًا أنّ أيّ صور أو فيديوهات، يتمّ نشرها على مواقع التواصل الاجتماعي، أو المواقع الإعلامية، قابلة للرّصد من قبل السّلطات المختلفة.

كاميرات الجسد وتصوير المحتجّين/ات

في السّنوات الأخيرة، بلّغ/ت العديد من الناشطين/ات الفلسطينيين/ات عن استخدام كاميرات الجسد، من قبل السّلطات المختلفة خاصّةً في الدّاخل والقدس، وهي كاميرا تصلّت-عادةً-على الملابس، في منطقة الصّدر أو الكتف أو على مستوى الرأس. كما قد تستخدم السلطات – تحديدًا- في الضفة الغربيّة وقطاع غزة الكاميرات اليدويّة أو كاميرا الهاتف المحمول. قد تستخدم تلك الكاميرات في تعقّب هويّات المشاركين/ات في الاحتجاجات السّلميّة، وقد يتم استخدامها من قبل أجهزة الشّرطة أو عناصر أمن بلباس مدني.

أمور يمكن أخذها بالاعتبار، فيما يتعلّق بكاميرات الجسد والتّصوير:

- تعدّ بعض الأنظمة كاميرات الجسد بمثابة شاهد، مع العلم أن صاحب/ة الكاميرا ي/تتحكم بتشغيل و/أو إيقاف التّصوير ما يجعله/ا قادرا/ة على التحكم بمحتوى التوثيق. كما أن الكاميرات لا توثّق أفعال صاحب/ة الكاميرا نفسه/ا، في كثير من الأحيان.
- يمكن استعمال تقنيّات تحديد الوجه لتعقّب هويّات المتواجدين/ات في تسجيلات كاميرات الجسد وغيرها، التي تعتمد على تجميع ملامح مميزة لوجوه وأجساد الأشخاص، وتصبح أقل قدرة على العمل في حال عدم توفّر مقاطع واضحة لتلك الملامح.
- يحقّ لأيّ فرد، طلب حذف أيّ صورة أو فيديو ت/يظهر فيه/ا بشكل واضح، سواء في لحظة التقاط الصّورة، أو في حال انتشار الصّورة على الإنترنت، أو في الإعلام، حتى لو التقطت في مكان عام.

الطّائرات بلا طيّار

في السّنوات الأخيرة، تصاعد استخدام الطّائـرات بلا طّـيار (drone)، مـن قبل السّلطات المختلفة في الاحتجاجات في فلسطين، خاصّة في قطاع غزة في مسيرات العودة، وفي المسيرات والمظاهرات في الضّفة الغربيّة والقدس والدّاخل. يمكن أن يتم تزويد الطّائرات بلا طيّار بكاميرات عاديّة أو كاميرات مع تقنيّة تحديد الوجوه. كما يمكن تزويد الطائرة بلا طيّار بتقنيّات تعقّب رقم الـ IMSI الخاص بشرائح الهواتف.

أمور يمكن أخذها بالاعتبار، فيما يتعلق بالطائرات بلا طيّار:

- تعتمد قدرة الطّائرة بلا طيّار على تعقّب هويات الأفراد، على طراز الطّائرة، فلا تمتلك كلّ الطائرات القدرات نفسها.
- تعتمد تقنيّات الوجـوه على مقاطـع واضحة لملامح مميّزة لوجوه الأفراد، وقد تكون أقلّ قدرةً على العمل، في حال ارتداء الأفراد نظّارات شمسيّة أو أقنعة طبيّة أو كليهما معًا.
- تعتمد تقنيّات تعقب إشارة "شريحة" الهاتف على اعتراض اتّصالها مع أبراج الإشارة. في حال إغلاق الهاتف أو استخدام وضع الطيران قد تكون تلك التّقنيّات أقل قدرة على العمل.

دليـــل قـــواعد بيـانات الشّـرطة والشّرطة التنبؤيّة

تعتمد تقنيّات الشرطة التنبؤية على تحليل البيانات، على صفحات التّواصل الاجتماعي، وفي قواعد بيانات جاهزة، لدى السّلطات (سجلات عن أحداث سابقة أو ملفّات عن أشخاص أو بيانات بيوميتريّة، أو بيانات تحديد الوجه أو بيانات شرائح الهواتف وغيرها) لتنبؤ أو توقّع "أحداث أمنيّة" مستقبليّة، وبناء عليه، تبرير اعتقال و/أو استدعاءات للتّحقيق. وفق تقارير عدّة، بدأت السلطات الإسرائيلية باستعمال تقنيّات الشرطة التنبؤية بكثافة منذ عام 2015.

تستطيـع السّـلطات استـخدام الصـور والفيديوهات من الاحـتجاجات السّـلميّة في تغذيّة تلك التقنيّات، وتعقّب هويات المشاركين/ات و/أو إدراجهم/ن على قوائم خاصّة. في حال إدراج شخص ما على إحدى تلك القوائم، قد يؤدي ذلك إلى الاعتقال أو الاستجواب أو الإيقاف والتفتيش، في المستقبل. صفي كثير من الأحيان، قد تكون نتائج خوارزميّات الشرطة التنبؤية غير دقيقة ومنحازة، بسبب تواجد فجوة في البيانات

المـدخلة إليها، ما قـد يؤدي - في بعض الحالات- إلى تكثيف العنف على المجتمعات الأكثر عرضة لذلك أصلًا.

أمور يمكن أخذها بالاعتبار، فيما يتعلق بالشرطة التنبؤية:

- يمكن استخدام أيّ صور أو فيديوهات، على منصّات التّواصل الاجتماعي، أو تسجيلات كاميرات المراقبة، وخصوصًا تلك المتعلّقة بالاحتجاجات، في تغذية قواعد بيانات الشّرطة التنبؤيّة.
- يلجأ بعـض المستخدمين/ات على مـنصّات التّواصـل الاجتماعي إلى تشفير "كلمات مفتاحيّة"، قد تؤدي إلى إدراجهم/ن على قوائم الشّرطة التنبؤية، من خلال استخدام الأرقام والرّموز، أو حروف من لغات مخـتلفة في كتابة الكلمات.

مرصد انتهاكات الحقوق الرقمية (حُـر)

منصّة حُر: المرصد الفلسطينيّ للانتهاكات الرّقميّة

في حال التّعرض لأي انتهاك رقميّ، كالاختراق وانتهاك الخصوصيّة، والرّقابة على حريّة التعبير، يقدّم مركز حملة، من خلال منصّة "حُر" الدّعم من خلال رصد وتوثيق الانتهاكات ومتابعتها، مع شركات التّواصل الاجتماعي و/أو الجهات المختصّة الأخرى. يمكن زيارة المنصّة من خلال الرّابط https://7or.7amleh.org.

www.7amleh.org

/7amleh