accessnow.org

عُرضة للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال إفريقيا

accessnow

تُدافع أكسس ناو عن الحقوق الرّقميّة للمستخدمين المعرّضين للخطر حول العالم وتُوسّع نطاقها. نحن نُكافح من أجل حقوق الإنسان في العصر الرّقمي من خلال الجمع بين الدّعم التقني المباشر والمشاركة الشاملة في مجال السياسات العامة والمناصرة الدّوليّة وتقديم المنح للقواعد الشعبية وعقد المؤتمرات مثل الرايتسكون.

عُرضة للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال إفريقيا

يناير 2021

جدول المحتويات

تنشر أكسس ناو هذا التقرير وهو من تأليف مروة فطافطة وديما سمارو بالتعاون مع ريما الصغيّر التي قامت بالبحوث اللازمة لدراسات الحالة. وتودّ المؤلفتان التوجّه بشكر خاص إلى كل من مركز حملة – المركز العربي لتطوير الإعلام الاجتماعي و SMEX سمكس و الجمعية الأردنية للمصدر المفتوح وريم المصري، ريما الصغيّر، سايج تشانغ، دونا وانتوورث، وفريق السياسات العامة في أكسس ناو على مساهماتهم في هذا التقرير.

تُدافع أكسس ناو (https://www.accessnow.org**) عن الحقوق الرّقميّة للمستخدمين المعرّضين للخطر حول العالم وتُوسّع نطاقها. نحن نُكافح من أجل حقوق الإنسان في العصر الرّقمي من خلال الجمع بين الدّعم التقني المباشر والمشاركة الشاملة في مجال السياسات العامة والمناصرة الدّوليّة وتقديم المنح للقواعد الشعبية وعقد المؤتمرات مثل الرايتسكون.**

معلومات الاتّصال

للحصول على المزيد من المعلومات حول هذا التقرير، الرجاء الاتّصال بـ :

مروة فطافطة (marwa@accessnow.org)

ديما سمارو (dima@accessnow.org)

١. الملخّص التنفيذي

شهدت سنة 2020 مسارعة الحكومات للتصدي لانتشار فيروس كوفيد-19 من خلال توظيف الحلول التكنولوجية بدءا بتطبيقات تعق مخالطي المرضى وصولا إلى الشهادات الصحية وجوازات السفر البيومترية. وبذلك سلّطت الجائحة الضوء على مدى تهديد وسائل التكنولوجيا الحديثة لحقوق الإنسان، مما يؤكد على ضرورة إرساء حماية البيانات الشخصية كأولوية قصوى للحكومات واعتماد إجراءات مُحكمة تحمي خصوصية المواطنين، وأطر قانونية لحماية بياناتهم الشخصية.

لا تزال قوانين حماية البيانات في دول الشرق الأوسط وشمال إفريقيا في آخر سلم الأولويات للحكومات حيث تبقى مثل هذه القوانين اما غائبة كلياً أو ضعيفة وغير مطبّقة، في حين تسارع هذه الحكومات إلى توظيف تكنولوجيات تستوجب جمع كماً هائلا من البيانات، على غرار برامج الهوية الوطنية البيومتري أو الرقمية، وجوازات السفر البيومترية، والخدمات الصحية الإلكترونية، غير عابئة بإمكانية استغلال هذه التكنولوجيا لانتهاك خصوصية المواطنين أو استغلال بياناتهم الشخصية. وحتى في الدول التي تعتمد قوانين لحماية البيانات، يبقى الإشكال على مستوى إنفاذ وتطبيق هذه القوانين. حيث غالبا ما تحظى الأجهزة الأمنية بحرية الوصول إلى البيانات الشخصية للمواطنين دون قيد أو شرط، وتستغل الشركات الخاصة هذه المعلومات لأهداف ربحية دون علم أصحابها أو موافقتهم على ذلك.

وتلتزم أكسس ناو بحماية حقوق الإنسان في العصر الرقمي من خلال حملات الضغط والمناصرة العالمية والإقليمية والمحلية من أجل حماية الحق في الخصوصية وحماية البيانات الشخصية من الانتهاكات وأوجه الاستغلال العديدة. وفي هذا الإطار، نسلط في هذا التقرير الضوء على تفاقم الانتهاكات من قبل الحكومات والشركات الخاصة وغيرها جراء ضعف الضمانات القانونية المتعلقة بحماية البيانات الشخصية، والتي من شأنها أن تُجبر المنشآت العامة والشركات الخاصة والمنظمات الدولية على احترام مبادئ حماية البيانات وتمكين مستخدمي الوسائل التكنولوجية من التحكم في معلوماتهم الخاصة والسيطرة عليها، واستحداث آليات لتقديم الشكاوى وجبر الضرر في حال وقوع انتهاكات من هذا القبيل.

كما يضم هذا التقرير مجموعة من التوصيات للجهات التي تتولى جمع البيانات الشخصية ومعالجتها: الحكومات والشركات الخاصة والمنظمات الدولية. ويشمل هذا التقرير أمثلة واقعية من **الأردن ولبنان وفلسطين وتونس.** ولا نهدف هنا إلى إدراج قائمة شاملة بكل الحالات المتعلقة بحماية البيانات، بل نستعرض بعض الأمثلة التي تعكس الوضع في كل من هذه البلدان. وليس هذا التقرير إلا غيضا من فيض، وبذلك نرحب بأي مساهمات أو أمثلة أو تحقيقات أجراها مواطنون أو نشطاء أو صحفيون أو منظمات المجتمع المدني.

II. المقدمة

كانت إحدى النساء في بيروت تقود سيارتها محاولة تجاهل رجل يضايقها من سيارته. بعد بضع دقائق، تلقت مكالمة منه. وقبل أن تغلق الخط أخبرها الرجل بأنه يعرف عنوان بيتها. من أين حصل على هذه المعلومات؟ استخدم الرقم المكتوب على لوحة تسجيل سيارتها. في سنة 2014 في لبنان، كان بمقدور أي شخص أن يحصل على اسمك وعنوان بيتك ورقم هاتفك ومعطيات شخصية أخرى، مثل فصيلة دمك، بمجرد أن يُدرج رقم تسجيل سيارتك في تطبيق متوفر على الهواتف الجوالة.[1]

وللأسف، كثيرة هي الحالات المشابهة في دول منطقة الشرق الأوسط وشمال إفريقيا والتي تعكس مدى التدخل في حياتنا الخاصة ومعلوماتنا الشخصية على نحو يبعث على الخوف. وتختلف الحالات وتتنوع، على غرار شركة الاتصالات أورانج (Orange) في تونس التي ألقت ما يقارب 1500 عقد خدمات، بما فيها بطاقات هوية المواطنين التونسيين وجوازات سفرهم، على قارعة الطريق، [2] وبين استغلال تطبيقات المواعدة بين أفراد مجتمع الميم في المغرب أثناء فترة الحجر الصحي من أجل إفشاء ميولاتهم الجنسية والتشهير بهم، ونشر صورهم على وسائل التواصل الاجتماعي دون موافقتهم.[3] والأمثلة على ذلك لا تحصى ولا تعد لمستخدمي الإنترنت في المنطقة ممن تعرضوا لانتهاك

[1] محمد نجم (2014، 15 مايو). *في لبنان، تطبيقات تمكنك بسهولة من الحصول على معطيات الآخرين*. وقع الاطلاع عليه يوم 8 جانفي 2021 من موقع https://slate.com/technology/2014/05/in-lebanon-apps-let-you-get-someone-else-s-personal-info-with-ease.html

[2] اكسس ناو (2018، 6 نوفمبر). *تونس: شركة اورونج للاتصالات تنتهك حق حرفائها في حماية المعطيات الشخصية (بالعربية)*. وقع الاطلاع عليه يوم 8 جانفي 2021 على الرابط التالي https://www.accessnow.org/%D8%AA%D9%88%D9%86%D8%B3-%D9%81%D8%B6%D9%8A%D8%AD%D8%A9-%D8%B4%D8%B1%D9%83%D8%A9-%D8%A3%D9%88%D8%B1%D9%88%D9%86%D8%AC-%D9%84%D9%84%D8%A5%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA%D8%8C-%D8%A7%D9%84%D8%A5/

[3] هيومن رايتس وانتش (2020، 28 أكتوبر). *المغرب: هجمات عبر الإنترنت على المثليين*. وقع الاطلاع عليه يوم 8 جانفي 2021 على الرابط التالي https://www.hrw.org/news/2020/04/27/morocco-online-attacks-over-same-sex-relations

خصوصيتهم على الشبكة الإلكترونية, والتي أدت في بعض الحالات إلى الأذى الجسدي وانتهاكات أخرى على أرض الواقع دون توفير حماية لهم أو جبر ضررهم.

ويعتبر الحق في الخصوصية, وهو مرتبط بالحق في حماية البيانات, من حقوق الإنسان الأساسية. ولكن, كما أشرنا آنفا, تسارع الحكومات في المنطقة لاعتماد وسائل تكنولوجية جديدة تجمع المعطيات الشخصية للملايين من مواطنيها وتعالجها, على غرار بطاقات الهوية الرقمية وجوازات السفر البيومترية الإلكترونية ورخص القيادة والخدمات الحكومية الإلكترونية, ولكنها في ذات الوقت فشلت في إعطاء الأولوية لحماية معطيات مواطنيها. وعوضا عن ذلك, ذهب المشرّعون وواضعي السياسات على الصعيد الوطني في الاتجاه المعاكس, حيث قاموا ببلورة تشريعات وسياسات قمعية, من بينها مشاريع قوانين تتعلق بالجرائم الإلكترونية وقوانين مكافحة الإرهاب, سعياً منهم إلى تجريم حرية التعبير على الشبكة الإلكترونية وتحويل الإنترنت إلى منصة تخضع للرقابة والمراقبة.

وفي سنة 2012, أصدرت لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا) عدداً من التوجيهات بشأن التشريعات المتعلقة بالإنترنت, بما في ذلك توجيهات بشأن حماية المعطيات الشخصية, في محاولة منها لتحقيق التجانس بين هذه التشريعات في العالم العربي. [4] واستندت التوجيهات المتعلقة بحماية البيانات بشكل كبير إلى توجيهات الاتحاد الأوروبي المتعلقة بحماية البيانات والصادرة سنة 1995, والتوجيه رقم EC/95/46 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة المعطيات الشخصية وحرية تناقل هذه المعطيات (التوجيه EC/95/46) كما استندت إلى توجيهات منظمة التعاون والتنمية الاقتصادية المتعلقة بحماية الخصوصية وتدفق البيانات الشخصية عبر الحدود (1980).

وكانت التوجيهات التي قدمتها اللجنة بشأن حماية البيانات واعدة حيث طرحت المبادئ الأساسية التي تمنح الأفراد والجهات صاحبة البيانات الحق في إبداء موافقتها على جمع معطياته الشخصية

[4] لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (2017، 08 مارس). *التنسيق الإقليمي للتشريعات السيبرانية من أجل تعزيز مجتمع المعرفة في العالم العربي*. وقع الاطلاع عليه بتاريخ 8 جانفي 2021 على الرابط التالي https://www.unescwa.org/publications/brochure-cyberlegislation-arab-world

ومعالجتها ومشاركتها, وهو ما يفرض على جامعي البيانات ومعالجيها واجبات محددة, ويمكن من إرساء هيئات مستقلة لتراقب مدى حماية البيانات إلى جانب مسائل أخرى.

وللأسف, لا تزال الأطر التشريعية والتنظيمية المعمول بها في المنطقة تعاني من نقائص. حيث لم يقم سوى نصف البلدان العربية بسنّ قوانين وطنية لحماية البيانات. أما البلدان التي تحظى بمثل هذه القوانين, على غرار تونس ولبنان والمغرب, فهي تعاني من أطر قانونية هشّة وقديمة وتواجهها صعوبات كبرى في تفعيل القانون وتنفيذه. ونتيجة لذلك تتعرض المعطيات الشخصية لملايين المواطنين للاستغلال المستمر على يد الشركات الخاصة الرامية لتحقيق الأرباح والحكومات التي تستخدمها لأغراض الرقابة وقمع حرية التعبير والمعارضة السياسية تحت ذريعة مكافحة الإرهاب والجريمة أو باسم المحافظة على الأمن القومي.

بل الأدهى والأمرّ أنه في بعض الحالات قد لا يكون الدافع وراء التقدم بمقترحات قوانين وطنية لحماية البيانات هو حماية الحقوق الأساسية للمواطنين, بل فسح المجال أمام الاستثمار المالي في قطاع البيانات الضخمة.

وفي هذا التقرير نسعى إلى تقديم لمحة عن الوضع الحالي لحماية البيانات في منطقة الشرق الأوسط وشمال إفريقيا عن طريق تسليط الضوء على الوضع في البلدان الأربعة: الأردن, لبنان, المغرب, فلسطين, تونس .حيث نقدّم تحليلاً للأطر القانونية والتنظيمية المتعلقة بالخصوصية وحماية البيانات المعمول بها حاليا في كل بلد من البلدان الأربعة.

كما نُعاين حالات شهدتها هذه البلدان مؤخرا في علاقة باختراق الحكومات والشركات الخاصة للبيانات وانتهاك خصوصية المواطنين. وفي العديد من الحالات يصعب الحصول على المعلومات اللازمة لتحديد كيفية جمع معطيات المواطنين ومعالجتها في مختلف أنحاء المنطقة. وفي ظل ضعف الشفافية والنفاذ إلى المعلومة في العديد من بلدان منطقة الشرق الأوسط وشمال إفريقيا, بات من الشاق على الصحفيين والنشطاء ومنظمات المجتمع المدني, على غرار منظمتنا, أن تؤدي عملها. فحتى في البلدان التي تعتمد قوانين للنفاذ إلى المعلومة, غالبا ما يكون مصير طلبات النفاذ إلى المعلومة

التجاهل كما هو الحال بالنسبة لمطلب النفاذ إلى المعلومة الذي تقدمنا به إلى وزارة الصحة في تونس من أجل تمكيننا من الإطلاع على المعلومات المتعلقة بتطبيق تعقب مخالطي المرضى التي استخدمتها الحكومة في يونيو 2020.[5]

ومما يزيد الوضع تعقيداً هو أن مستوى الوعي لدى العديد من مستخدمي الإنترنت في المنطقة لايزال متواضعاً حين يتعلق الأمر بقوانين الخصوصية على الإنترنت وحماية البيانات الشخصية. وكما ورد في أبحاث منظمة سمكس (SMEX), فإن العديد من المواطنين على قناعة واستسلام بأنهم دائما تحت أعين رقابة حكوماتهم, في حين يرى آخرون أنه يتعين التركيز على انتهاكات أخرى لحقوق الإنسان أشد فظاعة من هذه, إلى جانب المشاكل التي تشوب المجتمع والمشهد السياسي التي يعتبرونها على قدر أكبر من الأهمية مثل تفشي الفساد والفقر والبطالة. [6]

ومن المهم هنا التأكيد على أن منطقة الشرق الأوسط وشمال إفريقيا ليست قالبا واحدا متجانسا, وأن التهديدات والمخاطر التي يواجهها الأفراد والجماعات تعتمد وتتشكل وفقا للسياقات السياسية والقانونية والاجتماعية والثقافية الخاصة بالمكان الذي يعيشون فيه. ولنا على ذلك أمثلة مفزعة حيث باتت الفئات المستضعفة أكثر عرضة للمخاطر والأضرار بدءا من جمع كميات مهولة من البيانات البيومترية, مثل بصمة العين وبصمات الأصابع, لـ 2.5 مليون لاجئ, وصولا إلى اختراق خصوصية النساء ومجتمع الميم على شبكة الإنترنت كما حدث مع أفراد من مجتمع الميم في المغرب الذين وقع "فضحهم" على وسائل التواصل الاجتماعي ليصبحوا هدفا للهجمات الإلكترونية الشرسة وتم نبذهم من أهاليهم في فترة انتشار جائحة الكورونا. وعليه, تعتبر الخصوصية وحماية البيانات أمرا أساسيا لضمان سلامة الغير, كما تبين من هذه الحالات وحالات عديدة أخرى.

[5] أكسس ناو (2020، 17 سبتمبر). *تعزيز الشفافية في تونس: تطبيق تعقب مخالطي المصابين بفيروس كوفيد-19*. وقع الاطلاع عليه يوم 22 جانفي 2021 على الرابط التالي https://www.accessnow.org/to-safeguard-privacy-tunisia-must-be-transparent-on-tech-used-to-fight-covid-19/

[6] سمكس (2020، 16 يناير). *A Snapshot of Digital Rights Coverage in the MENA Region*. وقع الاطلاع عليه يوم 08 جانفي 2021 على الرابط التالي https://smex.org/a-snapshot-of-digital-rights-coverage-in-the-mena-region/

وتحث أكسس ناو الحكومات على اعتماد قوانين وسياسات صارمة وكافية لحماية البيانات الشخصية على الشبكة الإلكترونية. كما نحث الشركات الخاصة على تحمل مسؤوليتها إزاء احترام حقوق الإنسان عوضا عن تحقيق الأرباح من وراء هذه الانتهاكات.

III. حماية البيانات في منطقة الشرق الأوسط

الأردن

1- الإطار القانوني لاحترام الخصوصية وحماية البيانات

على غرار العديد من السلطات القضائية المحلية في منطقة الشرق الأوسط وشمال إفريقيا, لا يوجد في الأردن حتى الآن قانون مختص لحماية البيانات الشخصية. في عام ٢٠١٤, قامت وزارة الاقتصاد الرقمي والريادة (المعروفة سابقاً بوزارة الاتصالات وتكنولوجيا المعلومات) بتقديم مشروع قانون يتعلق بحماية البيانات الشخصية. ولكن بعد مرور سنة ونصف من المشاورات العامة مع الأطراف المعنية من القطاعين الخاص والعام, لا يزال مشروع القانون في نسخته الخامسة والنهائية قيد النظر إلى هذا اليوم.

حيث تلى المقترح الأوليّ تشكيل لجنة لمناقشة القانون, وضمت كل من وزير الداخلية ووزير العمل ووزير الاتصالات وهيئة تنظيم قطاع الاتصالات, والمصرف المركزي, وجمعية شركات تقنية المعلومات والاتصالات في الأردن. أما مشاركة المجتمع المدني ومؤسسات حقوق الإنسان في هذه النقاشات فقد كانت متواضعة, واقتصرت على إبداء الملاحظات على مشروع القانون من خلال المشاورات العامة التي أجرتها وزارة الاتصالات وتكنولوجيا المعلومات.

وفي سنة 2018, اقترحت وزارة الاتصالات وتكنولوجيا المعلومات النسخة الرابعة من نص القانون بحيث يتماشى مع القانون العام لحماية البيانات الصادر عن الاتحاد الأوروبي.[7] وبالفعل, عند النظر للوهلة الأولى إلى مشروع القانون المتعلق بحماية البيانات الشخصية يتبين أنه يعكس المبادئ الأساسية للقانون العام لحماية البيانات, مثل الشفافية والدقة والحد الأقصى لحفظ البيانات والتقليل إلى الحد الأدنى من البيانات. كما يوسّع مشروع القانون نطاق تطبيقه ليشمل جميع المؤسسات العامة والخاصة في الأردن بما فيها الوكالات والمنظمات الدولية المسجلة محلياً.

ولكن القانون بصيغته الحالية يبعث على القلق بشكل كبير, خاصة فيما يتعلق بالهيكلة المقترحة للهيئة المعنية بحماية البيانات وإنشائها مستقبلا. فعلى سبيل المثال, تقترح المادة 4 من مشروع القانون أن يترأس لجنة حماية البيانات: وزير الاتصالات وتكنولوجيا المعلومات, وهو ما من شأنه أن ينال من استقلالية اللجنة بصفتها هيئة رقابية. وكما أشارت المؤسسة الإعلامية حبر, الهيكلية المقترحة بحسب القانون تضم في جوهرها تضارب في المصالح على المستوى الهيكلي, وخاصة بأن لوزارة الاتصالات وتكنولوجيا المعلومات "مصلحة كبرى في تطوير قطاع التكنولوجيا, إذ تمثّل مصلحة الشركات التي من شأنها أن تستفيد من جمع أكبر عدد من البيانات الشخصية دون أن تحمي حقوق أصحابها بالضرورة".[8] كما ستشمل اللجنة عضوين من قوات الأمن ليتوليا ضمن مهامهما صياغة السياسات والاستراتيجيات فيما يتعلق بحماية البيانات الشخصية والموافقة عليها. وبالتالي, هناك شكوك حول إذا ما كانت لجنة حماية البيانات في هيكلتها المقترحة حاليا ستتمكن من التحقيق في الشكاوى المتعلقة بانتهاك الخصوصية إذا كان مرتكبوها من السلطة التنفيذية.

علاوة على ذلك, تتسم صياغة مشروع القانون بلغة فضفاضة وعامة من شأنها أن تسمح بمعالجة البيانات الشخصية دون الحصول مسبقا على موافقة أصحابها حين يقتضي الأمر ذلك "لدواعي أمنية" أو "للصالح العام" (المادة 15).[9] ويبعث ذلك على القلق الشديد باعتبار أن الجهات والدوائر الحكومية تتعامل مع كم هائل من البيانات, ولا يجب إعفائها من شرط الحصول على موافقة صريحة قبل جمع البيانات

[7] زاد الاردن (2020، 15 يناير). *مشروع قانون حماية البيانات في الأردن (بالعربية)*. وقع الاطلاع عليه يوم 08 جانفي 2021 على الرابط التالي http://www.jordanzad.com/index.php?page=article&id=360987

[8] حبر (2017، 13 سبتمبر). *قانون حماية البيانات: دعوة للدفاع عن حماية حقّنا في الخُصوصيّة*. وقع الاطلاع عليه يوم 08 جانفي 2021 على الرابط التالي https://www.7iber.com/technology/data-protection-law-invitation-to-protect-our-privacy/

[9] المرجع السابق.

الشخصية للناس ومشاركتها فيما بينها. أو على الأقل, ينبغي تفعيل الحقوق الأساسية في مجال حماية البيانات, بما في ذلك الحق في الحصول على المعلومة وجبر الضرر. وفي غياب الضمانات المناسبة, يشكّل المقترح الحالي انتهاكاً للحق الأساسي والغاية من قانون حماية الخصوصية, الذي يرمي إلى حماية البيانات الشخصية للمواطنين من أي اختراق محتمل.

ولم يتضح بعد متى يعتزم مجلس النواب الاردني سن هذا القانون. وفي الأثناء, تشمل القوانين والأحكام الأخرى ذات الصلة بالحق في الخصوصية في الأردن ما يلي:

- **الدستور:** بينما يضمّن الدستور بموجب مادته رقم 18 الحق في الخصوصية, تسمح التعديلات الدستورية التي أُدرجت سنة 2011 بمراقبة الاتصالات الخاصة لدى الحصول على إذن قضائي بذلك, وذلك كشرط أساسي للحجب أو المصادرة أو الاطلاع على الاتصالات الخاصة. [10]
- **مشروع قانون مكافحة الجرائم الإلكترونية:** اقترحت الحكومة في ديسمبر 2018 تعديلات على قانون مكافحة الجرائم الإلكترونية والذي أُجري سحبه منذ ذلك الوقت. وأضافت التعديلات المقترحة عبارة "التطبيقات" لتعريف "منظومة المعلومات", والمقصود هو أن تطبيقات الهواتف الذكية ستصبح معرضة للرقابة المكثّفة. علاوة على ذلك, تُجرّم المادتان 11 و13 من القانون الذي وقع سحبه التشهير على المنصّات الإلكترونية وهو ما يعطي الحكومة صلاحية مصادرة الحواسيب الشخصية ونُظم المعلومات وإيقافها وتفتيشها, وهو ما يعد انتهاكا لحق الأفراد في الخصوصية.[11]
- **قانون الاتصالات رقم 13 لسنة 1995**: تشير المادة 56 إلى أنه "تعتبر المكالمات الهاتفية والاتصالات الخاصة من الأمور السرية التي لا يجوز انتهاك حرمتها وذلك تحت طائلة المسؤولية القانونية" وعلى الرغم من أن القانون ينطبق على وسائل الاتصال التقليدية, لا يرد أي إشارة واضحة لوسائل الاتصال الرقمية والإلكترونية. كما يسمح قانون الاتصالات بمراقبة الاتصال بموجب طلب قضائي أو إداري. وتنص المادة 29 من القانون على "التزام المرخص له بتقديم

[10] الدستور الأردني، وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي
https://www.constituteproject.org/constitution/Jordan_2016.pdf?lang=en

[11] اكسس ناو (2019، 19 فبراير). Cybercrime law in Jordan: pushing back on new amendments that could harm free expression and violate privacy. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي
https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/

التسهيلات اللازمة للجهات المختصة لتنفيذ الأوامر القضائية والإدارية المتعلقة بتتبع الاتصالات المحددة بتلك الأوامر."

- **قانون العقوبات رقم (16) لسنة 1960:** يعاقب قانون العقوبات على نشر الرسائل الخاصة بالسجن لمدة تصل إلى 3 أشهر، وتتراوح مدة العقوبة المنصوص عليها في قانون الاتصالات عند إجراء عملية مراقبة دون رخصة بين شهر إلى سنة في السجن أو غرامة تتراوح قيمتها بين 100 إلى 300 دينار أردني. وتنص المادة 356 من قانون العقوبات على ما يلي: "يعاقب بالحبس مدة ستة أشهر أو بالغرامة حتى عشرين ديناراً من كان ملحقاً بمصلحة الهاتف وأفشى مخابرة هاتفية اطلع عليها بحكم وظيفته أو عمله". بالإضافة إلى ذلك تنص المادة 348 على ما يلي: "بناء على شكوى المتضرر بالحبس مدة لا تقل عن ستة أشهر وبالغرامة مائتي دينار كل من خرق الحياة الخاصة للآخرين باستراق السمع أو البصر بأي وسيلة كانت بما في ذلك التسجيل الصوتي أو التقاط الصور أو استخدام المنظار، وتضاعف العقوبة في حال التكرار".[12]
- **قانون منع الارهاب رقم 55 لسنة 2006:** تنص المادة 4 على أنه "إذا وردت للمدعي العام معلومة ذات أساس بأن لأحد الاشخاص أو مجموعة من أشخاص علاقة بنشاط ارهابي فيجوز للمدعي العام أن يصدر... فرض الرقابة على محل إقامة المشتبه به وتحركاته ووسائل اتصالات". ومن الجدير بالذكر أن القانون يحتوي على تعريفات ومفاهيم فضفاضة على غرار "معلومة ذات أساس" و"نشاط إرهابي" مما يسهّل استخدامه لتبرير مراقبة المواطنين. [13]
- **قانون المعلومات الائتمانية المؤقت رقم (15) لسنة 2010:** تنص المادة 8 من القانون على ضرورة الحصول على الموافقة الخطية المسبقة للعميل قبل الكشف عن أي معلومات ائتمانية تتعلق به. كما تحظر الشركات من أن تقدم "أي معلومات ائتمانية أو أن تصدر أي تقرير ائتماني يخصّ العميل إلا بعد التحقق من وجود تصريح اطلاع صادر عنه لمقدم الائتمان". لكن المادة تستثني من هذه الحالة تقديم المعلومات المتعلقة بالعميل "إذا كانت الجهة التي

[12] قانون العقوبات الأردني رقم 16 لسنة 1960. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=79914&p_country=JOR&p_count=179&p_classification=01.04&p_classcount=6

[13] CYRILLA. *قانون منع الإرهاب رقم 55/2006*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي ++https://cyrilla.org/en/entity/xc3gtsd647yr0iepk3o50cnmi?searchTerm=anti+jordan

تلتمس المعلومات بنكا أو شركة تأمين أي جهة أخرى يوافق عليها المحافظ".كما تجيز المادة 18 بتبادل المعلومات بين الشركات المرخص لها بموافقة المحافظ.[14]

- **قانون ضمان حق الحصول على المعلومات لسنة 2007**: تنص المادة 13 من القانون على عدم الكشف عن "المراسلات ذات الطبيعة الشخصية والسرية سواء كانت بريدية أو برقية او هاتفية او عبر اي وسيلة تقنية أخرى مع الدوائر الحكومية والإجابات عليها". ولكن, لا يوضح القانون ما إذا كان يجوز الكشف عن المراسلات بين المواطنين.[16]

وفي غياب ضمانات كافية ومناسبة لحماية المعطيات الشخصية, سيبقى الأردنيون معرضين لخطر انتهاك حقهم في الخصوصية. وهو ما أُقر به في نوفمبر 2018 خلال الاستعراض الدوري الشامل في الدورة الحادية والثلاثين لمجلس حقوق الإنسان التابع للأمم المتحدة, حيث تلقّى الأردن للمرة الأولى في تاريخه توصيتين من دولتي إستونيا والبرازيل بشأن احترام الخصوصية.[16] وأوصت الجمعية الأردنية للمصدر المفتوح سابقا خلال الاستعراض الدوري الشامل بأن "تجري الحكومة الأردنية عمليات الرقابة الإلكترونية في كنف احترام حقوق الإنسان والحق في الخصوصية امتثالاً للدستور الأردني والمعايير الدولية لحقوق الإنسان".[17]

ويبقى إقرار قانون حماية البيانات الشخصية في بالغ الأهمية خاصة في ضوء ما تقوم به الحكومة من رقمنة للخدمات والوثائق الحكومية. حيث طرحت وزارة الداخلية ووزارة الاتصالات وتكنولوجيا المعلومات في عام ٢٠١٧ بطاقة الهوية الوطنية الذكية بشكل إجباري لتعويض وثائق الهوية الوطنية الورقية

[14] حبر. *قانون المعلومات الائتمانية رقم 15 لسنة 2010*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.7iber.com/wp-content/uploads/2016/06/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%A7%D9%8A%D9%94%D8%AA%D9%85%D8%A7%D9%86%D9%8A%D8%A9.pdf

[15] CYRILLA. قانون ضمان حق الحصول على المعلومات، رقم 47 لسنة 2007. وقع الاطلاع عليه يوم 8 يناير 2021 على الرابط التالي https://cyrilla.org/en/entity/si4p74r2ylf2jfiequcqy3nmi?searchTerm=access+to+info

[16] المفوضية السامية لحقوق الإنسان. *الاستعراض الدوري الشامل - الأردن*. وقع الاطلاع عليه بتاريخ 8 يناير 2021 على الرابط التالي https://www.ohchr.org/EN/HRBodies/UPR/Pages/JOindex.aspx

[17] الجمعية الأردنية للمصدر المفتوح (2020، 13 يوليو). *تقرير مشترك حول الحق في الخصوصية في الأردن ضمن الاستعراض الدوري الشامل لحقوق الإنسان - الدورة*. ٣١ وقع الاطلاع عليه يوم 8 يناير 2021 على الرابط التالي https://jordanopensource.org/publications/1/cosubmission-to-the-universal-periodic-review-31st-session--jordan-on-the-right-to-privacy

السابقة وإدراج المزيد من البيانات المتعلقة بصاحب البطاقة.[18] وتحتوي هذه البطاقة على شريحة إلكترونية (بسعة تخزينية مقدارها 144 كيلو بايت) لحفظ البيانات البيومترية بما في ذلك بصمات العين وبصمات صاحب البطاقة إلى جانب الاسم والجنس ومكان الولادة ومقر السكن وفصيلة الدم. وفي مراحل لاحقة، ستحتوي بطاقة الهوية الوطنية على معلومات إضافية بشأن التأمين الصحي ورقم الضمان الاجتماعي والإمضاء الإلكتروني للمواطن والنشاط الانتخابي وغيرها بعد مضي سنتين، أعلنت لجنة تنظيم قطاع الاتصالات أنها ستضع قواعد جديدة تستوجب أن يقدم كل من يملك بطاقة هاتفية جديدة بصماته للتحقق من رقمه.

2ـ دراسات الحالة

1) استغلال مزودي خدمات الإنترنت وشركات الاتصالات للمعطيات الشخصية في الأردن

نشرت أكسس ناو في عام 2019، بالاشتراك مع مركز إمباكت الدولية لسياسات حقوق الإنسان، تقريراً سلّط الضوء على ممارسات مزودي خدمات الإنترنت الخمسة الموجودين في الأردن، وهم شركة زين، أورانج، أمنية، TE Data، وشركة الحداثة للاتصالات والتكنولوجيا (داماماكس)، حيث تقوم هذه الشركات بجمع البيانات الشخصية لعملائها على نحو روتيني دون إخطارهم بذلك أو الكشف عن أوجه استخدامات هذه البيانات وكيفية مشاركتها.[20] ولم يتفاعل مع ما توصل إليه التقرير سوى شركة أورونج، مكتفية بالتأكيد مجدداً على "امتثالها الكامل لجميع الشروط القانونية والتعاقدية للحفاظ على خصوصية معلومات العملاء"،[21] دون التطرق لأي من الأسئلة والمخاوف التي أثرناها في التقرير.

---

[18] الحكومة الإلكترونية المملكة الأردنية الهاشمية، *البطاقة الذكية الاردنية (باللغة العربية)*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://portal.jordan.gov.jo/wps/portal/Home/SmartCard?lang=ar&isFromLangChange=yes

[19] اكسس ناو (2019, 03 ديسمبر). *دراسة جديدة: انتهاك مزودي خدمات الإنترنت في الاردن لخصوصية العملاء* وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.accessnow.org/new-study-jordanian-isps-violate-customers-privacy/

[20] مرصد الأعمال وحقوق الإنسان (2019, 9 ديسمبر). *Orange responds to ImpACT International for Human Rights Policies and Access Now report*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.business-humanrights.org/en/latest-news/orange-responds-to-impact-international-for-human-rights-policies-and-access-now-report/

ومن جهة أخرى، أكدّت هيئة تنظيم قطاع الاتصالات في بيان لها على أنها ستحقق في الأمر وتتخذ كافة التدابير اللازمة للتصدي لانتهاكات خصوصية عملاء شركات الاتصالات في الأردن. [21] وعلى الرغم من ذلك، ليس هناك إلى الآن ما يثبت تطبيق قانون الاتصالات (رقم 13 لسنة 1995) على مزودي خدمات الإنترنت لارتكابها هذه الانتهاكات في حق خصوصية العملاء.

ووفقا لريم المصري، وهي باحثة صحفية متخصصة في التكنولوجيا في المؤسسة الإعلامية الأردنية المستقلة "حبر"، تُجبر السياسات الضعيفة المتعلقة بالخصوصية لدى شركات الاتصالات الأردنية "مستعملي الخدمة على الموافقة عملياً على مشاركة بياناتهم مع أطراف ثالثة وعدم إخطارهم في كل مرة تشارك فيها هذه المعطيات". فعلى سبيل المثال، أخبرنا مصدر من الأردن أنهم تمكنوا سنة 2019 من شراء خدمة من شركة الاتصالات أمنية تخوّل لهم إرسال رسائل ترويجية قصيرة (رسائل نصية قصيرة) إلى عملائهم في إحدى المدن الأردنية. وللأسف، يعتقد بعض المستخدمين أن هذه الممارسة مشروعة بأنها أصبحت مألوفة، وفقا لمصدرنا: "أرقام هواتفنا هي ملك للشركة وبذلك نكون قد قبلنا بشكل تلقائي تلقّي الإعلانات. وإذا أردنا الانسحاب من هذه الخدمة، يمكن لنا أن نتصل بالشركة"

وفي أغلب الأحيان، يكون المنتفع الأول من بيانات مشتركي الاتصالات هم وكالات الإعلانات والشركات الخاصة التي تسعى إلى الترويج لمنتجاتها أو خدمات معينة، أو ترغب في الإعلان عن عروض خاصة أو التخفيضات الموسمية. ولكن في بعض الحالات، يتم استغلال هذه البيانات لأغراض سياسية. فخلال احتجاجات النقابات سنة 2018، تلقى المواطنون في الأردن رسالة نصية قصيرة في الليلة التي سبقت الاحتجاجات المقررة. وفي هذه الرسالة الواردة من رقم غير معروف دعوة ضمنية بعدم المشاركة في هذه الاحتجاجات. ولم يتبين إلى الآن من هو مرسل الرسالة، ولكن تشير الترجيحات إلى مشاركة أرقام هواتف مستخدمي خدمة الاتصالات مع طرف ثالث والتي يرجح أن تكون جهة تابعة للحكومة الأردنية.

[21] هيئة تنظيم قطاع الاتصالات (2019، 13 نوفمبر). *تأكيد على إجراءات ضد أي انتهاك لخصوصية المشتركين*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.almamlakatv.com/news/%D8%AA%D8%A3%D9%83%D9%8A%D8%AF-%D8%B9%D9%84%D9%89-%D8%A5%D8%AC%D8%B1%D8%A7%D8%A1%D8%A7%D8%AA-%D8%B6%D8%AF-%D8%A3%D9%8A-%D8%A7%D9%86%D8%AA%D9%87%D8%A7%D9%83-%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B4%D8%AA%D8%B1%D9%83%D9%8A%D9%86-29064

الصورة 1: صورة عن شاشة الهاتف تُبين الرسالة النصية القصيرة التي تلقاها المواطنون في الأردن في يونيو 2018. [22]

2) جمع البيانات البيومترية للاجئين من قبل المنظمات الدولية

يعتبر الأردن هو البلد الأول في العالم الذي يُستخدم فيه تقنية مسح القزحية لأغراض المساعدة الإنسانية.[23] حيث بدأ برنامج الأغذية العالمي في سنة 2016, وبالاشتراك مع المفوضية السامية للأمم المتحدة لشؤون اللاجئين, بالعمل باستخدام تقنية الدفع عبر مسح القزحية في مخيمي الزعتري والأزرق في الأردن, ثم توسع نطاق المسح ليشمل مخيمات أخرى ومراكز متنقلة, وذلك في إطار برنامج يمكن اللاجئين من شراء البقالة من المحلات. [24]

وتعتمد منظومة برنامج الأغذية العالمي على قاعدة بيانات تسجيل اللاجئين البيومترية التابعة لمفوضية شؤون اللاجئين, واسمها EyeBank [25] حيث تستخدم المفوضية مسوح القزحية أولا لتسجيل اللاجئين الذين تفوق أعمارهم 3 سنوات, وتستخدمها في مرحلة لاحقة للتحقق من هوياتهم. [26] فعلى سبيل المثال, يمكن استخدام مسح القزحية عند شراء المواد الغذائية بدلاً من الدفع نقدا, وذلك

---

[22] مدّتنا بها مشكورة السيدة ريم المصري.

[23] Privacy International. (يناير ٢٠١٩). *State of Privacy Jordan*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

[24] برنامج الأغذية العالمي (2016 , 6 أكتوبر). *WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.wfp.org/news/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu

[25] IrisGuard. *Refugee Cash Assistance*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.irisguard.com/where-we-work/humanitarian-assistance/refugee-cash-assistance/

[26] Die Zeit.(2017,December 17). *Iris Scan Technology Tested on millions of Non-volunteers*. (مترجم للغة الإنجليزية على مدونة المفوضية السامية لشؤون اللاجئين). وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/01/article_1.pdf

للتحقق من هوية اللاجئ وخصم المبلغ من حسابه البنكي المتصل بالمنظومة. وقد اعتمد برنامج الأغذية العالمي تقنية الدفع بمسح القزحية هذه في 206 موقعا تجارياً في الأردن. [27]

وتستُخدم نفس العملية للدفع النقدي. حيث يمكن للاجئين أن يسحبوا النقود من الصرافات الآلية التي تعمل بمسح القزحية في الأردن. [28] وتزود شركة خاصة تدعى IrisGuard تقنية مسح القزحية والتي تُستخدم للتحقق من هوية الشخص وتسديد المبالغ ضمن عدد من أطر المساعدة النقدية. ومن بين هذه الأطر إطار المرفق النقدي المشترك، والذي يستند إلى شراكة بين القطاعين العام والخاص، أي بين بنك القاهرة-عمان، والمفوضية السامية لشؤون اللاجئين وشركة IrisGuard. وفي هذا الإطار يمكن لمختلف المنظمات الإنسانية والوكالات الحكومية أن ترسل أموالاً إلى اللاجئين عن طريق المحفظات الفرعية المرتبطة بقاعدة بيانات الهوية التابعة لمفوضية شؤون اللاجئين. [29] وانطلاقا من سنة 2018، ضم المرفق النقدي المشترك 22 عضوا، بما في ذلك المفوضية السامية لشؤون اللاجئين واليونيسيف ومنظمة والمجلس الدنماركي للاجئين وغيرها. [30]

شركة IrisGuard مسجلة في المملكة المتحدة. [31] واشترك في تأسيسها كل من عماد ملحس الذي استخدم تقنية مسح القزحية "EyeHood" سنة 2001 للمرة الأولى في الإمارات العربية المتحدة لتحديد المهاجرين غير النظاميين لإتاحة ترحيلهم، [32] وكريم قعوار، رجل أعمال وسفير الأردن سابقاً لدى الولايات المتحدة الأمريكية والمكسيك. [33] وقد ضمّ المجلس الاستشاري لشركة IrisGuard مسؤولين سابقين في الاستخبارات الأجنبية: فرانسيس ناونسيند، استشاري مختص في الأمن القومي الأمريكي لدى الرئيس الأمريكي السابق جورج بوش خلال فترة غزو العراق،[43] و ريتشارد ديرلوف الذي ترأّس جهاز

---

[27] المجموعة التشاورية المعنية بمساعدة الفقراء ومجموعة البنك الدولي (2020، أبريل). *Humanitarian Cash Transfers and Financial Inclusion: Lessons from Jordan and Lebanon*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي http://documents1.worldbank.org/curated/en/974621587749884009/pdf/Humanitarian-Cash-Transfers-and-Financial-Inclusion-Lessons-from-Jordan-and-Lebanon.pdf

[28] أنظر المرجع 18.

[29] أنظر المرجع 19.

[30] المرجع السابق.

[31] IrisGuard. وقع الاطلاع عليه بتاريخ 8 يناير 2021 على الرابط التالي https://www.irisguard.com/

[32] أنظر المرجع 18.

[33] أنظر المرجع 19.

[34] السيرة الموجزة لفرانسيس ناونسيند. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://network2020.org/past-benefits/frances-fragos-townsend/

الاستخبارات البريطاني. [35]

أما التقنية التي تُتيحها IrisGuard، والتي أُطلق عليها اسم "EyePay"، فهي مصدر مغلق، وبالتالي لا نعلم كيف تعمل تحديدا وإلى أي مدى يعتبر استعمالها آمنا، وما مدى ضمان احترام خصوصية اللاجئين وحماية بياناتهم الشخصية الحسّاسة و البيومترية. ووفقا لموقع IrisGuard، تستخدم "EyePay" تقنية سلاسل البيانات فيما يطلق عليه برنامج الأغذية العالمي مشروع "لبنات البناء"، عن طريق إدراج العملة المشفرة "إيثريوم". [36]

وبحسب تقرير للبنك الدولي، تحقق IrisGuard أرباحها باقتطاع نسبة عن رسوم المعاملات المالية. في إطار المرفق النقدي المشترك، تحصل IrisGuard على 15% من رسوم كل معاملة مالية لقاء التحقق من الهويات، ويدفع بنك القاهرة-عمان هذه الرسوم. وتتراوح رسوم المعاملات في الأردن بين 1.15-1.32% من مبلغ التحويل. [37]

وتفيد الشركة على موقعها بأن المفوضية السامية لشؤون اللاجئين قد تمكنت "بنجاح وبكل سلاسة" من تسجيل ما يزيد عن 2.5 مليون لاجئ سوري نازح في الأردن، ولبنان، والعراق، ومصر، وسوريا، وتركيا باستخدام هذه التقنية. [38] وليس من الواضح إن كان جميع اللاجئين الذي سجلتهم المفوضية في الأردن (751.901 اعتبارا من 31 أكتوبر 2020) قد خضعوا للتسجيل باستخدام هذه التقنية. [39]

وهذا أمر يبعث على الخوف. إذ يترتب عن استخدام التقنيات البيومترية تداعيات وخيمة على حقوق الإنسان، وقد يتسبب في أخطار جسيمة تهدد فئة مهمشة بالأساس. وكما سبق وشرحنا في وثيقتنا

---

[35] السيرة الذاتية لريتشارد ديرلوف. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي
http://investors.kosmosenergy.com/board-member/sir-richard-dearlove

[36] برنامج الأغذية العالمي. *لبنات بناء سلاسل البيانات للقضاء على الجوع*. وقع الاطلاع عليه بتاريخ 8 يناير 2021 على الرابط التالي
https://innovation.wfp.org/project/building-blocks

[37] أنظر المرجع 19.

[38] المرجع السابق.

[39] المفوضية السامية لشؤون اللاجئين *Operational Portal: Sum based on data from the official public UNHCR database*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://data2.unhcr.org/en/situations

بشأن الهوية الرقمية,[40] فإن محددات الهوية البيومترية على غرار بصمات الأصابع والحمض النووي وأنماط القزحية أو الشبكية, هي بيانات شخصية حساسة, وفي حال تم اختراق هذه البيانات أو الافصاح عنها, فقد يتسبب ذلك في أضرار جسيمة لا يمكن إصلاحها أو تداركها. وكما أشار أحد مؤسسي شركة IrisGuard: "إن قزحيّة عين الإنسان لا تتغير من سن الثالثة إلى حتى الموت... وبالتالي يمكن التعرف على كل من خضع لهذا المسح حتى في سن المائة بالاستناد فقط إلى خصائصه البيومترية" وهذا ما يجعل التعرف على الهوية بالاستناد إلى القزحية طريقة خطيرة للتحقق من هويات الأشخاص, وبالتالي يتعين على الحكومات والمنظمات أن تضع اعتبارات جدية لحماية البيانات والأمن الرقمي, قبل الانطلاق في العمل بهذه النظم. وعادة ما يبّرر أنصار هذه النظم البيومترية للهوية بأنها تساعد بشكل أكثر نجاعة ودقة على تقديم الخدمات والمساعدات, وتحد من الفساد وتمنع الاحتيال وتعزز المساءلة. ولكن استخدام تقنية مسح القزحية للتحقق من الهوية بحجة "تغيير تجربة التسوّق"[41] لدى اللاجئين السوريين هو هدف لا يوفي شرطي الضرورة والتناسب نظراً لمخاطر هذه التكنولوجيا على الحق في الخصوصية.[42]

علاوة على ذلك, يشكل استخدام هذه التقنية لأغراض المساعدة الإنسانية شكلا من أشكال الإكراه الضمني وينفي أحد المبادئ الأساسية لحماية البيانات وهو موافقة الشخص المعني ووكالته. وتشير المقررة الخاصة المعنية بالأشكال المعاصرة للعنصرية والتمييز العنصري وكُره الأجانب وما يتصل بذلك من تعصُّب, تينداي اتشيمي, في تقريرها الأخير حول استخدام التقنيات الرقمية الناشئة في مجال الهجرة وادارة الحدود "إلى أن تقييد الحصول على الغذاء بجمع البيانات يقضي على أي شكل من أشكال حرية الاختيار أو الاستقلالية في صفوف اللاجئين, فلا يمكننا الحديث عن حرية إعطاء الموافقة حين يكون البديل الوحيد أمامك هو الموت جوعا".[43]

---

[40] أكسس ناو (2019، نوفمبر). *برامج الهوية الوطنية الرقمية: ماذا بعد؟* وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.accessnow.org/accessnow-digital-id-paper

[41] أنظر المرجع 16.

[42] المادة 19 ومؤسسة الحدود الإلكترونية (2014، مايو). *Necessary & Proportionate International Principles on the Application of Human Rights Law to Communications Surveillance*. وقع الاطلاع عليه يوم 25 يناير 2021 على الرابط التالي https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf

[43] المفوضية السامية لحقوق الإنسان. *تقرير المقررة الخاصة المعنية بالأشكال المعاصرة للعنصرية والتمييز العنصري وكُره الأجانب وما يتصل بذلك من تعصُّب، A/75/590، 2020*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.ohchr.org/EN/newyork/Documents/A-75-590-AUV.docx

ومن بين الجوانب التي تبعث بشكل كبير على القلق، نقص الشفافية على مستوى كل من المفوضية السامية لشؤون اللاجئين وبرنامج الأغذية العالمي. إذ لا توجد أي معلومة متاحة للعموم بشأن اختيار IrisGuard وإجراء الصفقة معها، وإن كانت المنظمتان تحصلان على موافقة اللاجئين أم لا، وإن كان الأمر كذلك فبأي الطرق، وإن كانت تشارك هذه البيانات مع أطراف ثالثة أو جهات حكومية محلية، وكيف يتم حفظ هذه البيانات، وما هي الضمانات التقنية والقانونية المعمول بها لحماية الكم الهائل من هذه البيانات الحساسة. وبهذا الصدد، بعثت أكسس ناو رسالة إلى مكتبي المفوضية وبرنامج الأغذية العالمي في الأردن ملتمسة معلومات إضافية بشأن هذه الاسئلة. [44]

3) مطالب الحكومة بالحصول على بيانات مستخدمي تطبيقات النقل

دقّت الجمعية الأردنية للمصدر المفتوح، وهي منظمة غير حكومية محلية تعنى بالحقوق الرقمية، ناقوس الخطر إزاء تعديل أُدخل مؤخرا على نظام صدر عن وزارة النقل في مايو 2018 يرخّص لتطبيقات نقل الركاب، بما فيها Uber و Kareem [45] حيث يفرض النظام على هذه الشركات مشاركة البيانات الشخصية لمستخدميها وتفاصيل رحلتهم وموقعهم الجغرافي. ويسمح التعديل الجديد بدوره للوكالات القضائية والأمنية بالوصول مباشرة إلى خوادم هذه الشركات وقواعد بياناتها، وهو من شأنه أن يسهّل الرقابة المكثفة على المواطنين الأردنيين. [46] كما سبق وأشارت الجمعية الأردنية للمصدر المفتوح إلى معالجة هذه البيانات قد تشكّل "انتهاكا لحق المواطنين في الخصوصية في ظل غياب أي شروط ينص عليها القانون حول معالجة السلطة المعنية (النقل البري) لهذه البيانات، كما أن هناك غيابا تاما لأي قيود على نقل البيانات من السلطة المعنية إلى هيئات أخرى". [47]

---

[44] أكسس ناو (21 أكتوبر, 2020). *Letter to UNHCR and WFP Re: Collection of biometric data in refugee camps in Jordan*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://www.accessnow.org/cms/assets/uploads/2020/11/Access-Now-Letter-to-UNHCR-and-WFP-on-Jordan.pdf

[45] الجمعية الأردنية للمصدر المفتوح (2018). *نظام تنظيم نقل الركاب من خلال استخدام التطبيقات الذكية* (باللغة العربية). وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي https://opinions.jordanopensource.org/wp-content/uploads/2018/05/d0001075.pdf

[46] أخبار الأنباط (2020). *الجمعية الأردنية للمصدر المفتوح: "تعديل تعليمات تنظيم تطبيقات النقل يتيح رقابة جماعية على الركاب"*. وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي: https://alanbatnews.net/article/197268

[47] مقابلة مع الجمعية الأردنية للمصدر المفتوح (2020).

لبنان

1- الإطار القانوني لاحترام الخصوصية وحماية البيانات

لا ينص الدستور اللبناني صراحةً على ضمان الحق في الخصوصية. إذ يرد في المادة 14 منه أن "للمنزل حُرمة" ولا ينص إلا على حماية مسكن المواطن.[48] ولكن إحدى التفسيرات القانونية تذهب إلى أن المادة 8، التي تضمن الحرية الفردية، والمادة 13، التي تضمن حرية التعبير، يضمنان على نحو غير مباشر حق الأفراد في الخصوصية وسرية كل أشكال التواصل، بما في ذلك المكالمات الهاتفية والتواصل عن طريق البريد الإلكتروني.[49]

وفي عام 2018، سنّ لبنان قانونا لحماية البيانات، وهو القانون رقم 81 المتعلق بالمعاملات الالكترونية والبيانات ذات الطابع الشخصي. وعلى الرغم من مرور مشروع القانون بعديد الجولات منذ أول نسخة ظهرت له في 2004، فإن النسخة المحينة والمُعتمدة لم تعكس تطور الإنترنت ولم تعالج مسألة الخصوصية وحماية البيانات التي تقترن بظهور واستخدام الوسائل التكنولوجية الجديدة.

ويتسم العديد من أحكام هذا القانون باللبس والغموض. فعلى سبيل المثال، لا يُعرّف القانون معنى الموافقة في المواضيع المتعلقة بالبيانات، ويمنع الأفراد من سحب موافقتهم على جمع بياناتهم الشخصية ومعالجتها إذا سبق وأن وافقوا على ذلك.[50]

---

[48] The Constitute Project. *Lebanon's Constitution of 1926 with Amendments through 2004.* وقع الاطلاع عليه يوم 08 يناير 2021 على الرابط التالي: https://www.constituteproject.org/constitution/Lebanon_2004.pdf?lang=en

[49] Privacy International. SMEX, and the Association for Progressive Communication. (2015, مارس). *الاستعراض الدوري الشامل Stakeholder Report: 23rd Session, Lebanon*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://privacyinternational.org/sites/default/files/2018-02/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf

[50] سمكس (2018، أكتوبر). *القانون رقم 81 المتعلق بالمعاملات الالكترونية والبيانات ذات الطابع الشخصي*. وقع الاطلاع عليه يوم 10 جانفي 2021 على الرابط التالي https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf

ولا ينص القانون على أي حدود زمنية للاحتفاظ بالبيانات, ولا يشير إلى معالجة البيانات الشخصية الحساسة مثل المعلومات البيومترية أو ينظمها. وعوضا عن ذلك, يكتفي القانون بعرض قائمة من الاستثناءات التي لا تستوجب رخصة لجمع البيانات ومعالجتها. إضافة إلى ذلك, لم يضمن القانون حق الأفراد في إخطارهم في حال انتُهكت خصوصيتهم, ومما يبعث أكثر على القلق, أنه لا يحق للأفراد معرفة كيفية معالجة بياناتهم الشخصية لأغراض تتعلق بالأمن القومي.[51]

علاوة على ذلك, لا ينص القانون على إرساء هيئة مستقلة تعنى بحماية البيانات, وهو ما يعد أمرا ضروريا لضمان الإشراف وتطبيق القانون على النحو الواجب. بل يُسند صلاحيات وسلطة أكبر إلى السلطة التنفيذية, لاسيما وزارة الاقتصاد والتجارة, التي تملك صلاحية النظر في مطالب جمع البيانات ومعالجتها. وتمنح المادة 97 من القانون صلاحيات لكل من وزارة الدفاع والداخلية والصحة العامة للنظر في رخص البيانات المتعلقة بالأمن الخارجي وأمن الدولة الداخلي, والجرائم الجنائية, والدعاوى القضائية, إلى جانب الصحة, والهوية الوراثية, والحياة الجنسية تباعاً.

وتبعث السلطة المُسندة لوزارة الداخلية على القلق بشكل خاص. ففي ديسمبر 2012, طلبت قوى الأمن الداخلي اعتراض جميع الرسائل النصية القصيرة التي أرسلت على امتداد شهرين والاحتفاظ بها وذلك على إثر مقتل رئيس استخباراتها في انفجار سيارة مفخّخة في بيروت.[52] وأظهرت وثيقة مسرّبة من وزارة الإعلام أن أنواع البيانات المطلوبة شملت المشتركين في باقات الجيلين الثاني والثالث في لبنان, بما في ذلك رموز الدخول على الشبكة, وعناوين بروتوكول الإنترنت, وأسماء المستخدمين وكلمات مرورهم, وأرقام هواتفهم, والأسماء, والعناوين, والتطبيقات التي استخدمت على هواتف المشتركين.[53] وفي مارس 2014, أعطت الحكومة اللبنانية قوى الأمن الداخلي وغيرها من الأجهزة الأمنية الصلاحية الكاملة -دون أي قيد أو شرط- للحصول على بيانات الاتصالات الإلكترونية لكل

[51] SMEX. يرجى الاطلاع على المادة 103 من القانون. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf

[52] أنظر المرجع 31

[53] مؤسسة الحدود الالكترونية (2013, 07 فبراير). *Data Request from Lebanese Security Agency Sparks Controversy*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://www.eff.org/deeplinks/2012/12/lebanese-security-agency-user-data-request-sparks-controversy

المواطنين اللبنانيين لفترات تتراوح بين 6 أشهر وسنة, وجُددت هذه الصلاحيات لفترة 4 أشهر في أكتوبر 2017. [54]

وفي ظل هذه الانتهاكات الفظيعة للخصوصية وحماية البيانات, يعتبر قانون المعاملات الإلكترونية هشّا وغير قادر على توفير ضمانات مُحكمة, وعليه, كان هذا القانون عرضة للانتقادات من قبل المجتمع المدني والخبراء في المجال القانوني. وكما سبق وأشارت المنظمة اللبنانية المعنية بالحقوق الرقمية, منظمة تبادل الإعلام الاجتماعي (SMEX), فإن الهدف الأساسي من القانون على ما يبدو هو "تسهيل توسيع نطاق التجارة الإلكترونية دون مراعاة تأثير هذا التوسع على حماية البيانات". [55]

وإلى جانب قانون المعاملات الإلكترونية لسنة 2018, يوفر عدد من القوانين المتعلقة بالخصوصية والقوانين والأحكام القطاعية حماية محدودة للبيانات الشخصية, ويشمل ذلك: [56]

- **قانون الحق في الوصول إلى المعلومات (قانون رقم 28 تاريخ 2/ 10/ 2017):** ينص القانون على حماية محدودة للبيانات الشخصية وذلك بمنع المؤسسات العامة من مشاركة المعلومات الشخصية الخاصة بالمواطنين. وتمنح المادة 4 من القانون المواطنين الحق في الحصول على بياناتهم وملفاتهم الشخصية التي حصلت عليها السلطات العامة, وفي بعض الحالات المحدودة يمكنهم الحصول عليها من الشركات الخاصة التي تملكها الدولة أو متعاقدة معها لتقديم خدمة عامة أو لإدارة ملك عام. ويشمل هذا "أي تقرير تقييمي يتعلق بشخص طبيعي مشار إليه بالاسم أو برقم تعريفي او برمز أو بأي وصف تعريفي آخر كبصمات الأصابع او العين او الصوت او الصورة" كما يمنح القانون المواطنين الحق في "تصحيح او اكمال او تحديث او محو المعلومات الشخصية المتعلقة به غير الصحيحة او الناقصة أو الملتبسة او القديمة او التي يكون من الممنوع جمعها او استعمالها او تبادلها أو حفظها". [57]

---

[54] الخصوصية الدولية (2019، 27 يناير). *State of Privacy Lebanon*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

[55] سمكس (2020 , 31 مارس). *القانون الجديد لحماية البيانات في لبنان... "ناقص"* وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://smex.org/an-ugly-new-data-protection-law-in-lebanon/

[56] سمكس (2020 , 12 أكتوبر). *بناء الثقة: نحو إطار قانوني يحمي البيانات الشخصية في لبنان*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://smex.org/building-trust-toward-a-legal-framework-that-protects-personal-data-in-lebanon-report/

[57] CYRILLA. *القانون المتعلق بالحق في الوصول إلى المعلومات 2017*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي https://cyrilla.org/en/entity/s1g1mlpyymh?page=3

- **قانون حماية المستهلك رقم 659:** يفرض هذا القانون على المزودين التجاريين عدم الكشف عن بيانات عملائهم دون موافقتهم, و "اتخاذ كافة التدابير اللازمة للمحافظة على سرية هذه المعلومات".[58]

- **قانون الآداب الطبية رقم 288 لسنة 1994 وتعديلاته لسنة 2012:** تفرض المادة 7 على الأطباء مبدأ السرية المهنية. وعلى الأطباء أن يحرصوا على سرية كل المعلومات التي يطلعهم عليها المرضى, وأي معلومة رآها الطبيب أو علم بها أو اكتشفها أو استنتجها أثناء ممارسته لمهنته أو نتيجة للتحاليل التي أجراها, ما عدا بعض الاستثناءات على غرار التبليغ عن الأمراض المنقولة جنسيا أو أمراض أخرى يجب إبلاغ السلطات بها.[59]

- **قانون العقوبات:** تعاقب المواد 579 و 580 و 581 أي شخص على علم بسر بحكم وضعه أو وظيفته أو مهنته أو فنه, و أفشاه دون سبب شرعي أو استعمله لمنفعته الخاصة أو لمنفعة آخر , أو أي شخص يكشف عن مكالمة هاتفية أو يفتح رسالة إلكترونية غير موجهة إليه أو إليها.[60]

- **قانون سرّية المصارف الصادر بتاريخ 09/03/1956** : يمنع القانون المصارف من مشاركة أسرارها ومعلوماتها البنكية مع أي جهة عامة أو خاصة باستثناء الحالات التي ينص عليها القانون.[61]

- **قانون الاتصالات رقم 431 /2002:** تجدر الإشارة إلى أن هذا القانون الذي ينظم قطاع خدمات الاتصالات لا يتطرق إلى مسألة حماية البيانات الشخصية, باستثناء المادة 38, التي تفرض على المراقبين والمفتشين احترام سرية المعلومات التي يطلعون عليها أثناء أداء مهامهم الرسمية.[62]

---

[58] أنظر المرجع 36.

[59] CYRILLA . *قانون الآداب الطبية رقم 288 لسنة 1994 وتعديلاته لسنة 2012*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي:
https://cyrilla.org/en/entity/s4tb7viliry0tyjiuzsi6n7b9?page=1

[6460] CYRILLA. *قانون العقوبات عدد 340 لسنة 1943*. وقع الاطلاع عليه في 10 يناير 2021 على الرابط التالي:
https://cyrilla.org/en/entity/o9438um4ko3gq0omr3sicc8fr?page=128

[61] CYRILLA. *قانون سرّية المصارف (1956)*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي:
https://cyrilla.org/en/entity/vj24q5xwaxx1hhm4h48b5u3di

[62] البنك الدولي. *لبنان قانون الاتصالات رقم 431/2002*. وقع الاطلاع عليه يوم 10 يناير 2021 على الرابط التالي:
https://ppp.worldbank.org/public-private-partnership/library/lebanon-telecommunications-law-law-431-2002

- **قانون رقم 140 الصادر في 7/10/1999:** ينص هذا القانون على حماية الحق في سرية الاتصالات وعلى أنه لا يمكن إخضاعه لأي شكل من أشكال التنصت أو الرقابة أو الاعتراض أو الانتهاك, باستثناء الحالات الطارئة للغاية وبموجب إذن قضائي أو إداري. ويشمل ذلك الاتصالات السلكية واللاسلكية؛ والخطوط الأرضية, والهواتف الجوالة, والفاكس, والبريد الإلكتروني.

في بلد يُعاني من تفشي الفساد وتشابك مصالح الدولة والشركات, لا يُوفر الإطار القانوني الخاص بحماية البيانات سوى مستوى ضعيف وغير كافي من الحماية ضد سوء استخدام السلطة, والتي تتجلى مظاهرها في الصفقات المُبرمة مع الشركات الخاصة المقرّبة أو ذات العلاقة بالوزراء أو المسؤولين السياسيين في سعيٍ للنفاذ للبيانات الشخصية للمواطنين والمتاجرة بها مقابل أرباحٍ مادية. فعلى سبيل المثال, نقلت تقارير إعلامية اعتراف أكبر شركتي اتصالات في لبنان, ''ألفا'' و''تاتش'' المملوكتين للحكومة, ''ببيع بيانات مشتركيها لشركات أو أفراد يرغبون في إرسال رسائل نصية لمجموعات مستهدفة على أساس الجنس والسن والمهنة'' [63]. كما يمكن لشركة ''تاتش'' بيع البيانات الخاصة بمستخدميها استنادا على سلوكيات المستخدمين [64].

كما أن الاستعمال المتزايد للتكنولوجيا البيومترية للتعرف على الهوية يستدعي العمل على تعزيز حماية البيانات في لبنان. في شهر أغسطس 2016, شرعت المديرية العامة للأمن العام بإصدار جوازات سفر بيومترية ذات شريحة رقمية تحمل اسم صاحبها الكامل وتاريخ ميلاده وصورته وبصمته. [65] تلى ذلك شروع وزارة الداخلية في شهر يناير من سنة 2017 في إصدار رخص سياقة بيومترية. [66] كما أعلن الأمن العام بعد ثلاث أشهر من ذلك اعتزامه إصدار تصاريح إقامة بيومترية للمقيمين العرب والأجانب. من جانب آخر, اقترحت وزارة الاتصال في شهر ديسمبر إدراج شرائح الهاتف البيومترية لدواعي أمنية والتي بموجبها يتعين على أي شخص يرغب في شراء شريحة هاتف أن يقدم معلوماته البيومترية. [67]

---

[63] أنظر الملاحظة 36 أعلاه.
[64] صفحة شركة تاتش الإعلانية حول الرسائل النصية، وقع الاطّلاع عليه في 10 يناير 2021
https://www.touch.com.lb/autoforms/portal/touch/business/sms-advertising/mobile-media
[65] وثيقة المديرية العامة للأمن العام حول إصدار جواز السفر البيومتري، وقع الاطّلاع عليه في 10 يناير 2021
https://www.general-security.gov.lb/en/posts/182
[66] أنظر الملاحظة 36 أعلاه.
[67] سمكس (2020، 29 يوليو). *تاريخ موجز لجمع البيانات الشخصية في لبنان*. وقع الاطّلاع عليه في 10 يناير 2021
https://smex.org/a-brief-history-of-personal-data-collection-in-lebanon/

وساهم افتقار لبنان لاستراتيجية أمن سيبراني في تفاقم المخاطر المترتبة عن جمع معلومات المواطنين الحساسة خاصة في ظل غياب إطار حماية معطيات متين[68]. إذ لم يبادر مجلس الوزراء اللبناني بتقديم الاستراتيجية الوطنية للأمن السيبراني، التي تم تطويرها بدعم من الاتحاد الأوروبي، [69] إلا في شهر أغسطس من سنة 2019. بيد أن هذه الاستراتيجية قوبلت بتشكيك نابع من افتقار الدولة للموارد والكفاءات الضرورية لضمان تنفيذها. [70] نتيجة لذلك، قد تضطر الحكومة لتسليم مسؤولياتها في تأمين الفضاء الإلكتروني لشركات خاصة، وهو من شأنه إثارة المزيد من المخاوف والأسئلة المرتبطة بحماية البيانات.

2- دراسات حالة

1) سوء التصرف في بيانات الناخبين الشخصية خلال الانتخابات

تعتبر بيانات الناخبين، مثل سجلّات الناخبين الرسمية وقوائم الناخبين المستعملة لخدمة الحملات السياسية، من المعلومات الأساسية والضرورية للعملية الانتخابية والديمقراطية، وهذا يجعلها عرضة لعمليات الاختراق والقرصنة والتسريب، فضلا عن استغلالها لتحقيق مطامع ربحية أو سياسية. [71] في لبنان، "يتم مشاركة قوائم الناخبين أو بيعها مقابل مبلغ زهيد (قد تبلغ كلفة القرص المضغوط التي خزنت فيه)". [72] على سبيل المثال، تلقى مواطن لبناني مقيم في فرنسا دعوة عبر واتساب مرسلة من مرشح سياسي لسيدة ناخبة وزوجها للقاء خاص بالناخبين في باريس، [73] وذلك بعد أن استعمل رقم

[68] تقييم هيئة تنظيم الاتصالات في لبنان لأمن الفضاء الإلكتروني في لبنان. وقع الاطّلاع عليه في 10 يناير 2021 http://www.tra.gov.lb/Cybersecurity-in-Lebanon

[69] معهد الشرق الأوسط (1 ديسمبر 2020). *ظهور استراتيجية لبنان للأمن السيبراني*. https://mei.edu/publications/lebanons-cybersecurity-strategy-emerges

[70] حسان خضر (31 أغسطس 2019). *الأمن السيبراني بقدر خطورة أمن الحدود: حماية الدولة والمواطنين*. وقع الاطّلاع عليه في 10 يناير 2021، عنوان الموقع الإلكتروني https://www.almodon.com/economy/2019/8/31/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A8%D8%AE%D8%B7%D9%88%D8%B1%D8%A9-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%AD%D8%AF%D9%88%D8%AF-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D8%A9-%D9%88%D8%A7%D9%84%D9%85%D9%88%D8%A7%D8%B7%D9%86%D9%8A%D9%86

[71] التقنية التكتيكية (2019). *الخروقات والتسريبات والقرصنة: الحياة الهشة لبيانات الناخبين*. وقع الاطلاع عليه في 10 يناير 2021، عنوان الموقع الإلكتروني https://ourdataourselves.tacticaltech.org/posts/breaches-leaks-hacks/

[72] مقابلة مع غرانت بايكر، مدير أبحاث في منظمة تبادل الإعلام الاجتماعي. 2020

[73] تغريدة من @JpierreAn تم نشرها في 29 مارس 2018. وقع الاطّلاع عليها في 10 يناير 2021، من الموقع الإلكتروني https://twitter.com/JPierreAn/status/979336312527491073

هاتفه الشخصي لملء استمارات تسجيل الناخبين في فرنسا. كما اشتبه في أن وزارة الخارجية اللبنانية قد قامت بإرسال أو بيع قاعدة بيانات الناخبين للمرشحين السياسيين.

وفقا لمنظمة سمكس، "يتميز الإطار القانوني لحماية البيانات في لبنان بالهشاشة، وتُلزم الألفاظ الغامضة في المادة 118 من قانون الانتخابات لسنة 2017 وزارة الشؤون الخارجية والمغتربين بنشر وتعميم قائمات أسماء الناخبين المقيمين في الخارج باستعمال "جميع الأساليب الممكنة" من أجل ضمان تطابق هوية المغتربين مع المعلومات الموجودة في سجلات الأحوال الشخصية". [74] قبيل الانتخابات التشريعية لسنة 2018 مثلا، سرّبت السفارة اللبنانية في الإمارات العربية المتحدة البيانات الشخصية لما يزيد عن 5000 مواطن لبناني مقيم في البلد. حيث أرسلت السفارة بريد إلكتروني للناخبين المسجلين من أجل التثبت من معلوماتهم الشخصية مرفقة بملف إكسل يحمل الأسماء الكاملة وأسماء الأمهات والآباء ومعلومات خاصة بالجنس وتاريخ الميلاد والديانة والمذهب والحالة المدنية والعنوان. [75]

تحصّلت سمكس على نسخة مشابهة من البريد الإلكتروني تم إرسالها لأكثر من 200 ناخب لبناني مسجلين في لاهاي، هولندا. وتضمنت الرسالة كذلك ملف اكسل مرفق يحمل معلومات شخصية. وفي مؤشر واضح لعدم مبالاة الحكومة اللبنانية بموضوع حماية البيانات الشخصية، قامت السفارة بإدخال العنوان الإلكتروني للناخبين في خانة النسخة الكربونية (Cc) عوضا عن استعمال خانة النسخة الكربونية المخفية (Bcc).[76]

2) *تجاهل شركات الاتصالات ومزودي خدمة الإنترنت للخصوصية وحماية البيانات*

يضُّم لبنان عدداً كبيراً من مزودي خدمة الأنترنت، إذ وفقا لأبحاث أجرتها سمكس، بلغ عدد مزودي خدمة الإنترنت المرخّص لهم حاليا 144 مزود. ولكن لا يوجد سوى 39 موقع إلكتروني، فيما يعتمد 4 مزودين

[74] مقابلة مع منظمة سمكس، 2020
[75] سمكس (16 يونيو 2019). *السفارات اللبنانية تكشف البيانات الشخصية للناخبين المسجلين المقيمين بالخارج*. وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني https://smex.org/lebanese-embassies-expose-the-personal-data-of-registered-voters-living-abroad/
[76] نفس المصدر.

فقط سياسة لحماية الخصوصية منشورة على الموقع الإلكتروني. ولم تنشر سوى 4 شركات شروط الخدمة.[77] من جانب آخر، لا تنشر شركة أوجيرو لخدمة الإنترنت المملوكة للدولة، والتي توفر شبكة الإنترنت لكل مزودي الإنترنت في لبنان، سياسة حماية الخصوصية على موقعها على الإنترنت، كما لا تنشر معلومات متعلقة باستعمال وإدارة بيانات المستخدمين.

لا تشارك معظم شركات خدمة الإنترنت أية معلومات حول كيفية جمعها وتخزينها وبيعها لبيانات المستخدمين قبل وبعد تسجيلهم في خدماتها. ومع الأسف، حتى القلة القليلة من مزودي خدمة الإنترنت الذي يعتمدون سياسة لحماية الخصوصية يفتقرون للشفافية الكاملة. ووفقا لسمكس، " لا تقدم مواقع الأنترنت التي تتضمن سياسات حماية الخصوصية، والمتوفرة حصريا باللغة الإنجليزية، مضمون هذه السياسة سوى بعد توقيعهم للعقد. أما بالنسبة للسياسة المتوفرة والمنشورة للعموم، فيقتصر تطبيقها على الموقع الإلكتروني. بالتالي، لا يمكن للمستعملين تحديد كيفية قيام مزودي خدمة الإنترنت بجمع وبيع بياناتهم سواء قبل أو بعد التسجيل للانتفاع بالخدمات".[78]
يتفاقم التهديد لخصوصية المستخدمين بسبب استخدام شركات الاتصالات لتقنية فحص حزم البيانات (DPI) , والتي تتيح فحص حزم البيانات المنقولة في شبكة معينة، ما يسمح عادة بالبحث عن البرمجيات الضارة أو عدد الزيارات غير المرغوب فيها من خلال حمولة إرسال المستخدم المحدد. كما أن استعمال هذه التقنية يُسهل القيام بعمليات الرقابة الجماعية وحجب المواقع. من جانب آخر، تتمكن شركات الاتصالات من خلال هذه التقنية من رصد اتصالات المستخدمين غير المشفرة بصفة دائمة، فضلا عن تحديد وتحليل عادات المستخدمين عبر الإنترنت، وتنفيذ إجراءات الحظر المستهدف وحجب الإنترنت.

في فبراير 2020، ذكرت صحيفة الأخبار أن شركة ألفا قد اشترت برمجية فحص حزم البيانات من شركة ساندفين في سنة 2015 وشرعت باستخدام هذه التكنولوجيا لمشاركة المعلومات الشخصية لمشتركيها مع الأجهزة الأمنية.[79] جددت الشركة في عام 2018 تقنية فحص حزم البيانات الخاصة بها

[77] سمكس (26 فبراير 2020). *نقص الشفافية لدى مزودي خدمة الإنترنت*. وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني: https://smex.org/lebanese-isps-lack-transparency/

[78] نفس المصدر.

[79] الأخبار (14 فيفري 2020). *«التجسس» على مشتركي الخلوي*. وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني: https://al-akhbar.com/Community/284136/%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D8%AC-%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%B9%D9%84%D9%89-%D9%85%D8%B4%D8%AA%D8%B1%D9%83%D9%8A-%D8%A7%D9%84%D8%AE%D9%84%D9%88%D9%8A-%D9%87%D8%AF%D8%B1-%D8%A3%D9%85-%D9%86%D8%AC%D8%A7%D8%AD-%D9%88%D8%B4%D9%8A%D9%83

بتوقيعها عقد جديد بقيمة 3 ملايين دولار مع شركة ناكسيوس الموجودة في الولايات المتحدة. ومع ذلك، فإن التكنولوجيا لا تزال غير مشغلة، وبحسب مسؤول أمني، لا حاجة للأجهزة الأمنية لها.[80] كما فكرت شركة تاتش أيضًا في شراء نفس التكنولوجيا من شركة ناكسيوس.[81] وبحسب تقرير حديث صادر عن جمعية مسار ومتعلق بأنشطة ساندفين أن لبنان موطن لأحد أهم شركاء هذه الشركة في منطقة الشرق الأوسط وشمال إفريقيا، وهي نظم المعلومات الحاسوبية (CIS). تتضمن شراكة شركة CIS مع شركة ساندفين تطوير حلول لتقنية الفحص العميق لحزم البيانات (DPI) وقائمة مؤكدة للعملاء في لبنان تشمل شركات المدى وألفا وتاتش وأجيرو وسودوتال ووزارة الاتصال وهيئة تنظيم الاتصالات.[82]

فلسطين

1- الإطار القانوني لاحترام الخصوصية وحماية البيانات

على قدر تعقيد الحالة الفلسطينية فيما يتعلق بحماية البيانات، تُبرز هذه التجربة بوضوح استغلال أجهزة الدولة للبيانات والمعلومات الشخصية لفرض القمع والرقابة في سياقات الحروب والصراعات المسلحة. حيث يواجه مستخدمي الإنترنت الفلسطينيون ثلاث تحديات منفصلة، ولكن مترابطة؛ تتمثل الأولى في خضوعهم للقوانين العسكرية لقوة محتلة، أما الثاني فيتجسّد في سيادة إسرائيل وتحكمها في البنية التحتية لتكنولوجيا المعلومات والاتصالات الفلسطينية، فيما يكمن التحدي الثالث في تعرضهم لواحدة من أكبر عمليات المراقبة في العالم.[83]

[80] نفس المصدر
[81] سمكس. *جنة الأمن، جحيم الخصوصية: شركات الاتصالات اللبنانية تشرع في استخدام الفحص العميق لحزم البيانات*. وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني https://smex.org/security-heaven-privacy-hell-lebanese-telcos-introduce-deep-packet-inspection-dpi/
[82] جمعية مسار (15 نوفمبر 2020). *ساندفين ... أخطبوط المراقبة في العالم العربي*.وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني https://masaar.net/en/sandvine-the-surveillance-octopus-in-the-arab-region/
[83] صحيفة هارتس (15 يوليو 2019). *هذه الشركة الإسرائيلية الناشئة المُطورة لتقنية التعرف على الوجوه تتعقب الفلسطينيين سراً* (*This Israeli Face-recognition Startup Is Secretly Tracking Palestinians*) وقع الاطّلاع عليه في 10 يناير 2021 من الموقع الإلكتروني: https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359

تقع الأراضي الفلسطينية – الضفة الغربية وقطاع غزة والقدس الشرقية – تحت الاحتلال الإسرائيلي منذ 1967. وتواجه التجمّعات الفلسطينية الموجودة في الأراضي الفلسطينية المحتلة منظومات قانونية متعددة وشديدة التعقيد. [84] فعلى سبيل المثال، يجد الفلسطينيون الذين يعيشون في الضفة الغربية [85] أنفسهم خاضعين لمنظومة قانونية مزدوجة. نجد من جهة القانون الفلسطيني الذي تتولى السلطة الفلسطينية إنفاذه في مناطق محدودة من الأراضي (وكذلك القانون الأردني لعام 1967)، [86] ونجد من جهة أخرى الأوامر العسكرية الإسرائيلية الصادرة منذ سنة 1967. وتشمل هذه الأوامر العسكرية التي سمحت بتطبيق قانون الدفاع (الطوارئ) لائحة سنة 1945 (التي قام الانتداب البريطاني بسنها)، والأمر العسكري عدد 101 الصادر في أغسطس 1967، والأمر العسكري رقم 1651 الصادر في سنة 2010. عولت إسرائيل بشكل منهجي على ترسانة من الأوامر العسكرية ذات الصياغة الفضفاضة لتقييد حقوق التجمع بحرية وتكوين الجمعيات والحق في التعبير والصحافة و انتهاك حقوق الفلسطينيين الذين يعيشون في الضفة الغربية المحتلة. [87] على النقيض من ذلك، فإن المستوطنين الإسرائيليين الذين يعيشون في الضفة الغربية يخضعون للقانون الإسرائيلي المدني ونظام المحاكم، ممّا يفضي إلى تمييز مؤسسي ومنهجي. [88] بناءً على ذلك، حرمت السلطات الإسرائيلية " ما يقارب 2.5 مليون فلسطيني خاضعين لسلطتها في الضفة الغربية من حقوقهم الأساسية – وهي نفس الحقوق التي يتمتع بها أكثر من 400,000 مستوطن إسرائيلي يعيشون في مستوطنات غير قانونية في نفس المنطقة". [89]

لذلك، فإن قانون الخصوصية وحماية البيانات الإسرائيلي، والذي تم اقراره في سنة 1981، بالإضافة إلى المبادئ التوجيهية لهيئة الخصوصية الإسرائيلية التي تأسست سنة 2006، لا يسري على الفلسطينيين

[84] وتشمل القوانين العثمانية، وأنظمة الطوارئ تحت الانتداب البريطاني، والقانون المدني الإسرائيلي للقدس الشرقية والمستوطنين اليهود، والقانون المدني الأردني في الضفة الغربية، والقانون المدني المصري في غزة، والقانون العسكري الإسرائيلي في الضفة الغربية، والتشريعات والمراسيم التنفيذية الصادرة عن السلطة الفلسطينية، بالإضافة إلى الاتفاقيات والبروتوكولات الموقعة بين إسرائيل والفلسطينيين. بالنظر إلى هذا التعقيد والنطاق والغرض المحددين في هذا التقرير، سنتناول قضايا حماية البيانات في الضفة الغربية فقط.

[85] الحسيني (2016). *الازدواجية القانونية في الضفة الغربية المحتلة*، وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني https://pij.org/articles/1683/legal-duality-in-the-occupied-west-bank

[86] وفقًا للاتفاقية المؤقتة بشأن الضفة الغربية وقطاع غزة المترتبة عن اتفاقيات أوسلو الموقعة بين إسرائيل والفلسطينيين في عام 1995، فإن السلطة الفلسطينية تتمتع بسيطرة مدنية وأمنية كاملة على المنطقة أ (18٪ من الضفة الغربية) وتتمتع بالسيطرة المدنية الكاملة والسيطرة الأمنية الإسرائيلية الفلسطينية المشتركة على المنطقة ب (حوالي 22٪ من الضفة الغربية).

[87] هيومن رايتس واتش (18 ديسمبر 2019). *ولادة بدون حقوق مدنية*. وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني https://www.hrw.org/report/2019/12/17/born-without-civil-rights/israels-use-draconian-military-orders-repress

[88] منظمة الدفاع عن الحقوق المدنية في إسرائيل (أكتوبر 2014). *قاعدة واحدة ونظامان قانونيان: نظام القوانين الإسرائيلي في الضفة الغربية*. وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني: https://law.acri.org.il/en/wp-content/uploads/2015/02/Two-Systems-of-Law-English-FINAL.pdf

[89] أنظر الملاحظة 78 أعلاه.

في الضفة الغربية ولا في قطاع غزة. من الجدير بالذكر هنا أن المفوضية الأوروبية أقرت في 31 يناير 2011, وفقًا للمادة 25 (6) من المذكرة التوجيهية 95/46, أن إسرائيل توفر حماية كافية فيما يتعلق بالمعالجة الآلية للبيانات الشخصية.[90] يتم تطبيق قرار المفوضية الأوروبية "على ألا يتم المساس بالوضع القائم في مرتفعات الجولان وقطاع غزة والضفة الغربية, بما في ذلك القدس الشرقية, وفقا لأحكام القانون الدولي" [91], وهو ما يعتبر تغاضيا فعليا عن فشل إسرائيل على هذا الصعيد وانتهاكاتها المنهجية للحق في الخصوصية وحماية بيانات الفلسطينيين في الأراضي الفلسطينية المحتلة.

تقع على عاتق إسرائيل, بصفتها قوة احتلال, التزامات قانونية تجاه الفلسطينيين في الأراضي المحتلة, وتعتبر مُلزمة بتنفيذها بموجب قانون الاحتلال والقانون الدولي لحقوق الإنسان.[92] وقّعت إسرائيل على العهد الدولي الخاص بالحقوق المدنية والسياسية الصادر عن الأمم المتحدة في سنة 1966, وصادقت عليه في سنة 1991. ومع ذلك, فقد أكدت السلطات الإسرائيلية منذ فترة طويلة أن التزاماتها بحقوق الإنسان بموجب القانون الدولي ليست شاملة للفلسطينيين في الأراضي المحتلة. وتدعي إسرائيل على هذا الصعيد بأن العهد الدولي الخاص بالحقوق المدنية والسياسية لا يُطبق خارج حدودها الجغرافية, وبالتالي تستثني الأراضي الفلسطينية المحتلة.[93] قوبل هذا الموقف بالرفض من كل من لجنة حقوق الإنسان التابعة للأمم المتحدة, وهي هيئة الأمم المتحدة الموكّلة من قبل الدول الأعضاء بمراقبة تنفيذ العهد الدولي الخاص بالحقوق المدنية والسياسية, ومحكمة العدل الدولية.[94]

من ناحية أخرى, يجّرم القانون الأساسي الفلسطيني, الذي يعتبر بمثابة الإطار الدستوري للنظام القانوني الفلسطيني, "أي انتهاك لأية حرية شخصية, أو لحرمة الحياة الخاصة للإنسان, أو أي من

---

[90] الجريدة الرسمية للاتحاد الأوروبي (31 جانفي 2011). وقع الاطّلاع عليه في 10 يناير 2021، من الموقع الإلكتروني https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2011%3A027%3A0039%3A0042%3AEN%3APDF

[91] نفس المصدر السابق، المادة 2.

[92] تكمن واجبات القوة المحتلة بشكل أساسي في لوائح لاهاي لعام 1907، واتفاقية جنيف الرابعة (اتفاقية جنيف الرابعة، المواد 27-34 و47-78) ، وكذلك في بعض أحكام البروتوكول الإضافي الأول والقانون الدولي الإنساني العرفي. انظر دليل اللجنة الدولية للصليب الأحمر حول الاحتلال والقانون الدولي الإنساني. وقع الاطّلاع عليه في 10 جانفي 2021 من الموقع الإلكتروني https://www.icrc.org/en/doc/resources/documents/misc/634kfc.htm#:~:text=The%20main%20rules%20o%20f%20the,acquire%20sovereignty%20over%20the%20territory.&text=Transfers%20of%20the%20civilian%20population,Collective%20punishment%20is%20prohibited.

[93] يذهب التفسير الإسرائيلي الرسمي للمادة 2 (1) من العهد الدولي الخاص بالحقوق المدنية والسياسية الى أن حماية العهد الدولي الخاص بالحقوق المدنية والسياسية تمتد فقط إلى الأفراد الموجودين فعليًا "داخل أراضيها" و "الخاضعين لولايتها القضائية" من الناحية القانونية. (2019). انظر مجلة جورجتاون للقانون الدولي، حق دولي في الخصوصية: تجميع الاستخبارات الإسرائيلية في الأراضي الفلسطينية المحتلة. وقع الاطّلاع عليه في 10 جانفي، 2021 من الموقع الإلكتروني https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2019/10/GT-GJIL190033.pdf

[94] نفس المصدر السابق.

الحقوق أو الحريات''، [95] كما أنه يكفل للمواطنين الفلسطينيين سبل انتصاف عادلة في حال تعرضت حقوقهم الأساسية للانتهاك. ولكن من الناحية العملية، لم تبذل السلطة الفلسطينية سوى مجهودات محدودة لحماية خصوصية الأفراد الفلسطينيين وحفظ معلوماتهم الشخصية.

حتى هذا الوقت، لا يوجد أثر لأي قانون لحماية البيانات، والذي يبقى خارج أولويات للسلطة الفلسطينية. بدلاً من ذلك، أعطت السلطة الفلسطينية الأولوية لاعتماد قانون الجرائم الإلكترونية (القانون رقم 16/2017)، والذي تم اصداره في سنة 2017 في كنف السرية التامة بموجب مرسوم رئاسي. [96] لاقى القانون معارضة شديدة من قبل النشطاء والصحفيين والمجتمع المدني الفلسطيني نظرا لتضمنه لبنود ذات صياغة فضفاضة من شأنها أن تهدد حرية التعبير والحق في الخصوصية على الإنترنت، كما يمكن للسلطات الفلسطينية أن تسيء استخدامه بهدف قمع المعارضة السياسية ووسائل الإعلام المستقلة. [97] مدفوعةً بضغط المعارضة القوية للقانون، أصدرت السلطة الفلسطينية قانون مُعدل بموجب مرسوم (رقم 10 لسنة 2018). وعلى الرغم من أن هذه التعديلات جاءت للاستجابة لبعض المخاوف التي أثارها الخبراء القانونيون والمجتمع المدني الفلسطيني، الاّ أن القانون لا يزال محمّلا ببعض المواد الإشكالية. [98]

تجرّم المادة الرابعة من قانون الجرائم الإلكترونية (2018) النفاذ غير القانوني إلى أنظمة المعلومات التي قد يؤدي إلى "حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو استنساخ أو إرفاق بيانات أو معلومات إلكترونية". [99] وبموجب المادة السابعة، يُعاقب كل من تلقى أو سجل أو اعترض أي بيانات عن قصد أو بطريقة غير مشروعة بالسجن لمدة سنة على الأقل وغرامة تتراوح بين 1000 و3000 دينار أردني. زيادة على ذلك، تحظر المادة الثانية والعشرون "التدخل التعسفي أو غير

[95] المادة 32 من القانون الأساسي المعدل لسنة 2003. وقع الاطّلاع عليه في 10 يناير 2021 من الموقع الإلكتروني https://www.elections.ps/Portals/0/pdf/The_Amended_Basic_Law_2003_EN.pdf

[96] منظمة الأصوات العالمية. (5 أغسطس 2017). *هل يمهد قانون مكافحة الجرائم الإلكترونية الجديد الفلسطيني الطريق لمزيد من انتهاكات الحقوق؟* وقع الاطّلاع عليه في 10 يناير 2021 من الموقع الإلكتروني https://globalvoices.org/2017/08/03/will-palestines-new-cybercrime-law-pave-the-way-for-more-rights-violations/

[97] المرسوم الرئاسي عدد 16 لسنة 2017 حول أمن الفضاء الإلكتروني. وقع الاطّلاع عليه في 10 يناير 2021 من الموقع الإلكتروني https://security-legislation.ps/sites/default/files/law/Law%20by%20Decree%20No.%2010%20of%202018%20on%20Cybercrime.pdf

[98] جمعية الاتصالات التقدمية (2018). *هل تم بالفعل تعديل قانون الجرائم الإلكترونية الفلسطيني؟* وقع الاطّلاع عليه في 10 يناير 2021 من الموقع الإلكتروني https://www.apc.org/en/news/has-palestinian-cybercrime-law-really-been-amended

[99] نفس المصدر السابق.

القانوني في خصوصية أي شخص أو شؤون أسرته أو منزله أو مراسلاته" ونشر المعلومات المتصلة بذلك.

وفي المقابل, يتضمن القانون عددًا من الأحكام المتعلقة بالتعدي على الخصوصية. ومن أهم ما يجدر ذكره هو أنه يُلزم مزودي خدمات الإنترنت بالاحتفاظ ببيانات المستخدمين لمدة ثلاث سنوات على الأقل وتمكين المدعي العام من إمكانية النفاذ إلى جميع البيانات والمعلومات إن اقتضت الحاجة. كما يُناط بعهدة المدعي العام سلطة الأمر بالجمع الفوري للبيانات غير المقيدة بما في ذلك مراقبة الاتصالات الخاصة وبيانات المرور والبيانات الوصفية. [100]

إلى أي مدى يمكن أن يوفر قانون حماية البيانات الفلسطيني الضمانات الضرورية للخصوصية؟ مع الأسف, ليس بالقدر الكبير. وحتى إن تبنت السلطة الفلسطينية قانونا لحماية البيانات, فإن ذلك لن يوفر سوى مستوى محدود من الحماية نظرا لخضوع البنية التحتية الخاصة بتكنولوجيا المعلومات والاتصالات الفلسطينية للسيطرة الكاملة لإسرائيل, التي حافظت على هذا الوضع منذ احتلالها للأراضي الفلسطينية في عام 1967. إبان توقيع اتفاقية أوسلو للسلام في سنة 1995, سلمت إسرائيل السيطرة الجزئية على البنية التحتية لتكنولوجيا المعلومات والاتصالات في الضفة الغربية وقطاع غزة إلى السلطة الفلسطينية. على الرغم من أن الاتفاقية تمنح للفلسطينيين الحق في تطوير تكنولوجيا المعلومات والاتصالات المستقلة والخاصة بهم, [101] لا تزال السلطات الإسرائيلية تسيطر بشكل كامل على الموجات الكهرومغناطيسية بالإضافة إلى تحكمها في عمليات استيراد وتركيب أي معدات من قبل شركات الاتصالات الفلسطينية ومقدمي خدمات الإنترنت وذلك "لدواعي أمنية" غير معلنة. [102] نتيجة لذلك, تحُول إسرائيل بشكل روتيني دون وصول الفلسطينيين إلى التقنيات الجديدة. فعلى سبيل المثال, تطلبت موافقة السلطات الإسرائيلية على طلب مشغلي الهاتف المحمول الفلسطينيين لإدخال شبكات الجيل الثالث [103] مدة تجاوزت العقد من الزمن, ولم يسمحوا بعد بإدخال شبكات الجيل الرابع.

---

[100] نفس المصدر السابق

[101] تحدد المادة 36 من الملحق الثالث لاتفاقيات أوسلو الأحكام التي تنظم مجال الاتصالات في الأرض الفلسطينية المحتلة.

[102] حملة. (2018). *توقف الاتصال: سيطرة إسرائيل على البنية التحتية لتكنولوجيا المعلومات والاتصالات الفلسطينية وتأثيرها على الحقوق الرقمية*. وقع الاطّلاع عليه 10 يناير 2021 من الموقع الإلكتروني https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf

[103] رويترز (2018). *الفلسطينيون يحصلون على خدمات الجيل الثالث للهاتف المحمول في الضفة الغربية*. وقع الاطّلاع عليه 10 يناير 2021 من الموقع الإلكتروني https://www.reuters.com/article/israel-palestinians-telecom-idUSL8N1PJ3FW

لقد لعبت هذه البنية القانونية والبنية التحتية دورا جوهريا للسماح بالمراقبة الجماعية للمجتمعات الفلسطينية واستغلال بياناتهم الشخصية لعقود دون أي مساءلة. عند إدلائه بشهادته حول انتهاكات الخصوصية التي ارتكبتها المخابرات الإسرائيلية, أكّد ضابط إسرائيلي أن "أي معلومات من شأنها أن تفضي لابتزاز شخص ما تعتبر معلومات مهمة. وسواء كان الشخص المذكور ذو ميول جنسية معينة, أو يخون زوجته, أو يحتاج إلى علاج في إسرائيل أو الضفة الغربية – فهو يبقى هدفً للابتزاز". [104] في الواقع, يتم ابتزاز المنتسبين لمجتمع الميم في فلسطين من قبل المخابرات الإسرائيلية لتحويلهم لمخبرين وإلّا يتم فضح ميولهم أو كشف علاقتهم بالمخابرات. [105]

يتم جمع البيانات الشخصية للأفراد الفلسطينيين بشتى الطرق. في سنة 2018, أقام الجيش الإسرائيلي حواجز تفتيش مؤقتة في الضفة الغربية حيث كانوا يستوقفون الرجال الفلسطينيين ويطلبون منهم ملء استمارات حول الاسم والعمر ورقم الهاتف والهوية ورقم الترخيص, فضلا عن صورة من بطاقة هويتهم. [106] ووفقًا لوسائل الإعلام الإسرائيلية, يقع الاستعانة بهذا الإجراء التعسفي لجمع البيانات الشخصية من أجل إنشاء قاعدة بيانات لمكافحة الإرهاب. لا يتمتع الفلسطينيون بأي إمكانية للوصول إلى سبل انتصاف نظير الانتهاكات المنهجية لخصوصيتهم وإساءة استخدام بياناتهم الشخصية, إذ كما سبق و أوضحنا, لا تتوفر أي حماية قانونية للفلسطينيين الذين يعيشون في الضفة الغربية.

إثر صعود جهاز الأمن الداخلي الإسرائيلي ''الشاباك'' الى الواجهة عند تفشي مرض كوفيد-19 في إسرائيل, كُشف النقاب عن احتفاظ الوكالة بقاعدة بيانات سرية طوال الثماني عشر سنة الأخيرة تحتوي على بيانات كل شخص يستعمل خدمات الاتصالات اللاسلكية في إسرائيل. تتضمن قاعدة البيانات, المعروفة باسم "الأداة" (the Tool), بيانات توضح موقع جهاز المستخدم, ومنطقة الخلية والهوائي التي يتصل بها, والبيانات الوصفية لكل مكالمة صوتية ورسالة نصية مرسلة أو مستلمة علاوة على

[104] صحيفة الجارديان (12 سبتمبر 2014). *كل الفلسطينيون عرضة لرقابة الأخ الأكبر الإسرائيلي*. وقع الاطّلاع عليه 10 يناير 2021 من الموقع الإلكتروني https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-unit-testimonies

[105] موندوويس (15 سبتمبر 2014). *إسرائيل تراقب وتبتز فلسطينيين مثليين جنسيا لتحويلهم لمخبرين لديها*. *وقع الاطّلاع عليه في* 10 يناير 2021 من الموقع الإلكتروني https://mondoweiss.net/2014/09/blackmails-palestinian-informants/

[106] هآرتس (8 مارس 2018). *الجيش الإسرائيلي ينشئ قاعدة بيانات موسعة تتضمن تفاصيل شخصية عن الفلسطينيين وقع جمعها عند نقاط التفتيش*. وقع الاطّلاع عليه 10 يناير 2021 من الموقع الإلكتروني: https://www.haaretz.com/israel-news/.premium-idf-info-we-collect-on-palestinians-meant-for-anti-terror-database-1.5886616

سجل تصفح الإنترنت. تُحفظ المعلومات التي تم جمعها بواسطة الأداة لفترة غير معلومة, وتتسم القواعد الخاصة بكيفية تخزينها وحمايتها وحذفها بالسرية التامة.[107]

2- دراسات الحالة

1) تطبيق المنسق والجمع التعسفي لمعلومات الفلسطينيين

أطلقت وحدة تنسيق أعمال الحكومة في المناطق (COGAT) – وهي وحدة تابعة للجيش الإسرائيلي ومكلفة بالشؤون المدنية داخل الأراضي الفلسطينية المحتلة - في شهر فبراير 2019 تطبيقاً للهواتف المحمولة يُدعى 'المنسّق' لتوفّر للفلسطينيين داخل الأراضي المحتلة إمكانية الوصول إلى مجموعة من خدماتها رقميا والتي تتعلق في الغالب بطلبات الحصول على تصاريح الإقامة والدخول إلى إسرائيل.

وفي حين تزعم وحدة تنسيق أعمال الحكومة في المناطق (COGAT) أنّ "هذا التطبيق قد تم وضعه على نحو يعود بالنفع على عموم الفلسطينيين"[108]، فإن طرق جمعه المتطفلة للبيانات تُشير إلى وجود دافع مختلف. وفقاً لشروط الخدمة الخاصة بالتطبيق, يُطلب من المستخدمين الفلسطينيين الموافقة على جمع بياناتهم واستخدامها "لأي غرض, بما في ذلك الأغراض الأمنية".[109] ويتضمن ذلك الوصول إلى بيانات تحديد الموقع الجغرافي والرسائل والملفات المخزنة على الهاتف والوصول إلى الكاميرا. وتوضح شروط الخدمة أيضا أن استخدام بيانات المستخدمين وتخزينها يعود لتقدير السلطات الإسرائيلية وحدها:

"يجب أن توافق وتعلن أنك تعلم أن جميع المعلومات التي يُطلب منك تقديمها لا يتم تقديمها بموجب القانون أو اللوائح الخاصة بالدفاع. بل يتم توفيرها بمحض إرادتك حتى نتمكن من الاستفادة منها على النحو الذي نراه مناسبا. بالإضافة إلى ذلك, فإنك توافق على أنه يجوز لنا تخزين المعلومات التي قدمتها إلينا داخل قواعد بياناتنا بناء على اعتباراتنا".[110]

---

[107] معهد بروكينغز (06 يوليو 2020). *كيف تتم عملية الرقابة الجماعية الإسرائيلية لمرض كوفيد ١٩*. وقع الاطّلاع عليه 10 يناير 2021 من الموقع الإلكتروني: https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/

[108] هآرتس (15 مايو 2020). *إسرائيل تعلن إنّ المحكمة ستصدر قرارا يوقف إجبار العمال الفلسطينيين على منحها حق الوصول إلى بيانات هواتفهم الشخصية*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.haaretz.com/middle-east-news/palestinians/.premium-over-50-000-palestinians-forced-to-give-phone-data-to-israel-1.8844580

[109] المصدر نفسه.

[110] ميدل إيست مونيتور (09 أبريل 2020). *إسرائيل تطلب من الفلسطينيين استخدام تطبيق التعقب للتحقق من حالة إقامتهم*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021:

ولقد أصبح هذا التطبيق موضع تدقيق في أعقاب جائحة كوفيد-19. وفي ادّعت وحدة تنسيق أعمال الحكومة في المناطق أن استخدام التطبيق طوعي، فإن المقيمين والعمال الفلسطينيين في إسرائيل قد أُجبروا على تنزيل التطبيق واستخدامه أثناء الجائحة.[111] إذ أصدرت وزارة الزراعة الإسرائيلية في أبريل 2020 تعليمات إلى أرباب العمل الإسرائيليين بإلزام العملة الفلسطينيين بملء تصريح صحي على التطبيق الخاص بوحدة تنسيق أعمال الحكومة في المناطق (COGAT) قبل دخولهم إلى إسرائيل. وبحلول نوفمبر 2020، تضاعف عدد مستخدمي التطبيق مع أكثر من 100.000 عملية تحميل مقارنة بـ 50.000 في يونيو من نفس السنة.

وللتوضيح، ينبغي التوضيح بأنه يتعين على فلسطينيي الأراضي المحتلة الذين يقيمون أو يعملون في إسرائيل الحصول على تصاريح من وحدة تنسيق أعمال الحكومة في المناطق (COGAT) من أجل ضمان وضعيتهم القانونية، وخاصة في ظل إغلاق وحدات التنسيق في الضفة الغربية بسبب الجائحة. وبالتالي صدرت تعليمات للفلسطينيين تنص على اعتماد تطبيق المنسق دون غيره للتحقق من حالة تصاريحهم. وكما أوضح كل من مركز الدفاع عن الفرد (هموكيد) وجمعية أطباء لحقوق الإنسان الإسرائيلية، فإنّ "الفلسطينيين لا يملكون خيارا حرا حقيقيا في هذا الشأن ويجب عليهم تثبيت هذا التطبيق المتطفّل". إذ يتعين على الفلسطينيين المتقدمين بطلبات الحصول على تصريح "أن يؤكّدوا وجودهم داخل منازلهم بشكل قانوني - وإلا فإنهم سيواجهون خطر الترحيل والانفصال عن عائلاتهم".[112]

ونتيجة لذلك، قدم هموكيد عريضة إلى محكمة العدل العليا أبدى فيه اعتراضه على انتهاك التطبيق لحق مستخدميه في الخصوصية والكرامة بموجب القانونين الإسرائيلي والدولي. ورفضت المحكمة هذه العريضة لعدم ثبوت حدوث ضرر فعلي. ومع ذلك، عدّلت وحدة تنسيق أعمال الحكومة في

/https://www.middleeastmonitor.com/20200409-israel-tells-palestinians-to-use-tracking-app-to-verify-their-residency-status

[111] ميدل إيست آي (08 أبريل 2020). *"المنسق": إسرائيل تفرض على الفلسطينيين تحميل التطبيق الذي يتعقب هواتفهم*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021:
https://www.middleeasteye.net/news/coordinator-israel-instructs-palestinians-download-app-tracks-their-phones

[112] هموكيد (2020). *هموكيد ومنظمة أطباء لحقوق الإنسان - إسرائيل: يجب على إسرائيل التوقف عن إجبار الفلسطينيين الذين يحملون تصاريح إقامة إسرائيلية على تنزيل تطبيق هواتف ذكية متطفّل من أجل التأكد من تجديد تصاريحهم*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
http://www.hamoked.org/Document.aspx?dID=Updates2157

المناطق شروط الخدمة لتوضح أن التطبيق ليس لديه حق الوصول إلى الملفات وجهات الاتصال والصور وأن موافقة المستخدم مرتبطة حصرا بتوفير البيانات المحددة التي تتطلبها الخدمة قيد الاستخدام.[113]

ومع ذلك، فقد حذر الائتلاف الفلسطيني للحقوق الرقمية من تحميل التطبيق واستخدامه واصفا إياه بـ "الخطير". وفي الواقع، ومع الأخذ بعين الاعتبار أن وحدة تنسيق أعمال الحكومة في المناطق تقدم خدمات تتطلب، من بين بيانات أخرى، معالجة المعلومات الشخصية للفلسطينيين على غرار الاسم الكامل ورقم بطاقة الهوية ومكان وتاريخ الولادة وعدد أفراد الأسرة ومكان الإقامة والعمر، فإن جمع بيانات خاصة إضافية عبر تطبيق المنسق يشكل انتهاكا خطيرا لحق الفلسطينيين في الخصوصية وقد يؤدي إلى مزيد من الانتهاكات لحقوق الإنسان ولاسيما في ظل استخدامها من قبل سلطة احتلال.[114]

2) *تكنولوجيا التعرف على الوجه: تجارة إسرائيلية مزدهرة تمثل كابوسا لخصوصية الفلسطينيين*

في أوائل أكتوبر 2019، عثر فلسطينيون على كاميرا مراقبة مُمَوَّهة في شكل حجر ومزروعة داخل مقبرة قرية بالقرب من مدينة رام الله بالضفة الغربية. ولقد أُفادت تقارير أن الكاميرا المُمَوَّهة تم تصنيعها بواسطة "أني فيجن" AnyVision وهي شركة إسرائيلية مختصّة في بيع تكنولوجيا التعرف على الوجه.[115] ومع أن الشركة نفت صحة هذه التقارير، فإنها تورطت في مشروع سّري آخر للمراقبة العسكرية في كافة أنحاء الضفة الغربية. ووفقا لتحقيق نشرته هيئة الإذاعة الوطنية الأمريكية إن بي سي NBC، فقد تم استخدام تكنولوجيا أني فيجن ضمن مخطط مراقبة سّري إسرائيلي لرصد حركات الفلسطينيين، وهو مخطط يعرف باسم "Google Ayosh" في إشارة إلى قدرة التكنولوجيا على البحث عن الأشخاص والعثور عليهم.[116] ولقد مكن نجاح المشروع الشركة من الحصول على أعلى وسام من

---

[113] هموكيد (2020). *على إثر طلب هموكيد: قام الجيش بتعديل شروط الاستخدام التعسفية لتطبيق الهاتف الجوال لتمكين الفلسطينيين من التحقق من حالة طلبات التصاريح، 2020*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
http://www.hamoked.org/Document.aspx?dID=Updates2175

[114] APC. *حملة: ائتلاف الحقوق الرقمية الفلسطيني يحذر من تطبيق "المنسق"*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.apc.org/en/news/7amleh-palestinian-digital-rights-coalition-warns-against-phone-application-coordinator

[115] ميدل إيست مونيتور (07 أكتوبر 2019). *فلسطينيون يكتشفون جهاز مراقبة مُموّه داخل مقبرة رام الله*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
/https://www.middleeastmonitor.com/20191007-palestinians-discover-camouflaged-surveillance-device-in-ramallah-cemetery

[116] إن بي سي (19 نوفمبر 2019). *لماذا مولت مايكروسوفت شركة إسرائيلية تراقب الفلسطينيين في الضفة الغربية؟* تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

وزارة الدفاع الإسرائيلية في سنة 2018 "لمساهمتها في الحيال دون وقوع مئات الهجمات الإرهابية" باستخدام "كميات كبيرة من البيانات". وإلى جانب كشفها عن هذا المشروع السري، أفادت إن بي سي أنها تلقت جملة من الأدلة التي تثبت أن تكنولوجيا أني فيجن AnyVision قد تم استخدامها كذلك من قبل الشرطة الإسرائيلية لتعقب حركة الفلسطينيين في كافة أرجاء القدس الشرقية.[117]

والتكنولوجيا قيد النظر في معرض هذا الحديث هي إحدى منتجات أني فيجن AnyVision الأساسية والتي تعرف باسم "غد أفضل" "Better Tomorrow". فمن خلال كاميرات التعرف على الوجه المثبتة، يمكن لنظام التنبيه الآلي الخاص بقائمة الرصد تحديد وجوه "المشتبه فيهم" وسط الحشود وتتبع المركبات وتصنيفها. وتعد هذه التكنولوجيا مقترنة بقاعدة بيانات التوصيف الإسرائيلية أداة مراقبة فعالة. إذ توفر أني فيجن AnyVision أيضا تكنولوجيا التعرف على الوجه في 27 نقطة تفتيش عسكرية إسرائيلية في الضفة الغربية للتحقق من هويات الفلسطينيين العابرين إلى إسرائيل.[118] ومن المهم الإشارة إلى أن هذه التكنولوجيا لا تُستخدم عند نقاط التفتيش التي يستخدمها الإسرائيليون.

وعقب تقرير إن بي سي وما أثاره من احتجاج عام بين النشطاء وداخل المجتمع المدني [119] والذين أشاروا إلى الأدلة التي تؤكد أن برمجيات أني فيجن قد ساعدت على ترسيخ الاحتلال العسكري الإسرائيلي، قررت شركة مايكروسوفت التحقيق [120] فيما إذا كان استخدام تكنولوجيا التعرف على الوجه التي طورتها أني فيجن يتوافق مع أخلاقياتها ومبادئها.[121] ولقد وكّلت مايكروسوفت المدعي العام الأمريكي السابق إريك هولدر وفريقه العامل في مؤسسة كوفينغتون وبيرلينغ Covington & Burling لإجراء تدقيق على أني فيجن والذي انتهى إلى أن "تكنولوجيا أني فيجن لم تقم سابقا ولا حاليا بتشغيل برنامج

---

[117] المصدر نفسه.

[118] هآرتس (15 يوليو 2019). *هذه الشركة الإسرائيلية الناشئة للتعرف على الوجوه تتعقب الفلسطينيين سرا*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359

[119] الصوت اليهودي من أجل السلام. *أخبر ميكروسوفت: #إسقط_آني_فيجن Tell Microsoft: #DropAnyVision*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://dropanyvision.org/

[120] ميدل إيست آي (16 نوفمبر 2019). *مايكروسوفت ستحقق في عمل تقنية التعرف على الوجه الإسرائيلية التي مولتها*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.middleeasteye.net/news/microsoft-investigate-work-israeli-facial-recognition-technology-it-funded

[121] مايكروسوفت (2018). *ستة مبادئ لتطوير ونشر تكنولوجيا التعرف على الوجه*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf

للمراقبة الجماعية في الضفة الغربية كما زُعم في تقارير وسائل الإعلام".[122] وعلى الرغم من نتائج التدقيق، أعلنت كل من شركة مايكروسفت و شركة أني فيجن في بيان مشترك في مارس 2020 أنهما "اتفقتا على أنه من مصلحة كلا المؤسستين أن تقوم مايكروسوفت بتصفية حصتها داخل شركة أني فيجن".[123]

وفي يونيو 2020، ومع مواصلة شركات التكنولوجيا الكبرى تخليها عن تكنولوجيا التعرف على الوجه،[124] ضاعفت أني فيجن من استثماراتها في هذا المجال معربة عن عدم نيتها ترك العمل في هذا المجال.[125] حيث تبقى صناعة المراقبة الإسرائيلية مزدهرة منذ عقود من خلال تصدير تكنولوجيا المراقبة إلى الأنظمة القمعية في جميع أنحاء العالم والتي تُستخدم لاستهداف النشطاء والمعارضين.[126] ويتعزز "نجاحها" من خلال العلاقة المترابطة ما بين صناعة التكنولوجيا الإسرائيلية والجيش فضلاً عن استخدام المجتمعات المحلية الفلسطينية كحقل تجارب لمثل هذه التقنيات.

لقد استخدمت أني فيجن الأراضي الفلسطينية المحتلة بمثابة "حقل اختبار" قبل تسويق برامج التجسس الخاصة بها وتصديرها إلى دول أجنبية حيث أن 95% من إيرادات الشركة تأتي من عملاء من خارج إسرائيل. إذ تعتبر "إسرائيل المنطقة الأولى" التي "تتحقق من تكنولوجياتها" قبل تصديرها وفقا للمؤسس المشارك للشركة والمدير التنفيذي السابق إيلون إتشتاين.[127] ومن الجدير بالذكر أن إتشتاين

---

[122] م12. (08 أبريل 2020). *بيان مشترك لشركتي مايكروسوفت وأني فيجن حول عملية التدقيق التي خضعت لها أني فيجن*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://m12.vc/news/joint-statement-by-microsoft-anyvision-anyvision-audit/

[123] المصدر نفسه.

[124] موقع ذي فيرج (09 يونيو 2020). *لن تقدم شركة إي بي إم IBM أو تطور أو تبحث في مجال تكنولوجيا التعرف على الوجه بعد الآن*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software

[125] هآرتس (2020). *عمالقة التكنولوجيا ينسحبون من مجال تكنولوجيا التعرف على الوجه، ولكن الشركات الناشئة الإسرائيلية بقيت في اللعبة*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.haaretz.com/israel-news/business/.premium-tech-giants-stage-facial-recognition-retreat-but-israeli-other-startups-stay-in-1.8920814

[126] وفقا لتحقيق مستفيض استنادا إلى 100 مصدر مستقل في 15 دولة نشرته صحيفة هآرتس سنة 2018، باعت الشركات الإسرائيلية أنظمة المراقبة المستخدمة في استهداف نشطاء في كل من البحرين وإندونيسيا وأنغولا وموزمبيق وجمهورية الدومينيكان وأذربيجان وسوازيلاند وبوتسوانا وبنغلاديش والسلفادور وبنما ونيكاراغوا والمكسيك وأوزبكستان وكازاخستان وجنوب السودان وهندوراس وبيرو وكولومبيا وأوغندا ونيجيريا والإكوادور والإمارات العربية المتحدة وغيرها من الدول. انظر هآرتس، كشف صحفي: صناعة التجسس السيبراني الإسرائيلية تساعد دكتاتوري العالم في مطاردة المنشقين والمثليين. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027201

[127] إن بي سي (19 نوفمبر 2019). *لماذا مولت مايكروسوفت شركة إسرائيلية تراقب الفلسطينيين في الضفة الغربية؟* تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

نفسه قد خدم في جيش الدفاع الإسرائيلي وأن مدير الشركة أمير كان هو أيضا المدير السابق لإدارة الأمن بوزارة الدفاع وأن أحد أعضاء مجلسها الاستشاري هو رئيس الموساد السابق تامير باردو.[128]

تونس

1. الإطار القانوني للخصوصية وحماية البيانات الشخصية

لا تزال ثقافة الخصوصية على الإنترنت وحماية البيانات الشخصية متواضعة في تونس على الرغم من أن الحق في الخصوصية منصوص عليه في الدستور التونسي لسنة 2014 هذا إلى جانب قانون حماية المعطيات الشخصية (عدد 63).[129] ولقد كانت تونس رائدة في منطقة الشرق الأوسط وشمال إفريقيا عبر تبنيها لقوانين وسياسات متعلقة بالخصوصية تهدف إلى حماية البيانات الشخصية للأفراد من المعالجة غير القانونية منذ سنة 2004. ولكن طبيعة النظام لا تزال غير ملائمة لتفعيل مثل هذه القوانين والسياسات.

تم اعتماد القانون الأساسي المتعلق بحماية المعطيات الشخصية (عدد 63) في سنة 2004 في ظل نظام الرئيس التونسي السابق زين العابدين بن علي والذي عُرف بفرضه للرقابة والسيطرة على محتوى الإنترنت. وإلى يومنا هذا, لا يزال هذا الإطار القانوني المُعيب لحماية البيانات ساري المفعول على الرغم من اعتباره مرارا وتكرارا غير متوافق مع المبادئ التي تم ترسيخها في الدستور التونسي لسنة 2014 و مع الالتزامات الدولية لتونس. ويولد هذا الوضع مخاوف مشروعة فيما يتعلق بتأثيرات الواقع على تكريس الحق في حماية البيانات في تونس.

[128] فوربس (1 أغسطس 2019). *انتقدت شركة مايكروسوفت لاستثمارها في تكنولوجيا التعرف على الوجه الإسرائيلية "للتجسس على الفلسطينيين"*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.forbes.com/sites/thomasbrewster/2019/08/01/microsoft-slammed-for-investing-in-israeli-facial-recognition-spying-on-palestinians/

[129] الهيئة الوطنية لحماية المعطيات الشخصية. *تقرير نشاط الهيئة 2009-2017*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
http://www.inpdp.nat.tn/Rapport_2009-2017.pdf

يُفصل قانون سنة 2004 نطاق حماية البيانات وينص على إنشاء هيئة وطنية مكلّفة بإنفاذه. ويستند هذا القانون إلى مبادئ المشروعية والمعالجة والمساءلة: إذ يمنح جملة من الحقوق للأفراد الذين تتم معالجة بياناتهم, ويحدد التزامات المؤسسات والأفراد المسؤولين عن عملية المعالجة. ومع ذلك, يحتوي هذا القانون على عدد من أوجه القصور التي ترجع في المقام الأول إلى حقيقة أنه قد عفا عليه الزمن مما يفسر عجزه عن معالجة المخاطر المتزايدة المرتبطة بتطوير تكنولوجيات جديدة واستخدامها. فعلى سبيل المثال, يُعرِّف الفصل الرابع من القانون المعطيات الشخصية على أنها "كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصا طبيعيا معرفا أو قابلا للتعريف بطريقة مباشرة أو غير مباشرة باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانونا" [130] والملاحظ أنه ليس هناك ما يشير إلى ما إذا كان القانون ينطبق على معالجة البيانات الشخصية لمستخدمي الإنترنت. علاوة على ذلك, فإنه يتم إعفاء الهيئات العمومية مثل مراكز الشرطة بموجب القانون من أي التزام قد ينطبق على معالجي البيانات الشخصية. كما أن الهيئات العمومية ليست ملزمة بالإعلان عن معالجة البيانات, ونتيجة لذلك, فإن حق الأفراد في الموافقة المستنيرة محدود للغاية.

وينص هذا القانون على إنشاء الهيئة الوطنية لحماية المعطيات الشخصية (INPDP), والتي ظهرت إلى حيز الوجود في سنة 2009 بعد خمس سنوات من إقرار القانون. ولا تملك الهيئة الوطنية لحماية المعطيات الشخصية سلطة إصدار لوائح أو اتخاذ قرارات بشأن انتهاكات البيانات. ووفقا للفصل 76, تقتصر صلاحياتها على تلقي شكايات المواطنين حول انتهاكات الخصوصية وتقديم توصيات رسمية بشأن القضايا المتعلقة بحماية البيانات دون أن يكون لها سلطة إنفاذها. وتتعارض وظيفة الهيئة الوطنية لحماية المعطيات الشخصية هذه مع طبيعة الهيئات التنظيمية والرقابية والتي يجب أن تكون استباقية ومستقلة في إنفاذ أحكامها للحيلولة دون انتهاكات البيانات الشخصية.

[130] أكسس ناو (09 نوفمبر 2018). *نقاش مفتوح في تونس حول حماية البيانات والحق في النفاذ إلى المعلومات*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.accessnow.org/in-tunisia-an-open-debate-on-data-protection-and-the-right-to-access-information/

ولا تتناول التشريعات الحالية الحق في جبر الضرر والتعويض المناسبين عند حدوث انتهاكات للخصوصية. ولعل الأمر الأكثر إثارة للقلق، على حد علمنا، أنه لم يكن هناك أي حكم قضائي أو قرار محكمة يعاقب على انتهاكات معايير حماية البيانات هذه بعد 16 سنة من دخول القانون حيز التنفيذ. وعلى نفس المنوال، لا توجد آلية واضحة لتتبع القضايا المحالة إلى القضاء بما في ذلك تلك القضايا المحالة من قبل الهيئة الوطنية لحماية المعطيات الشخصية.

لقد أصبحت تونس في نوفمبر 2017 الدولة العضو رقم 51 التي توقع على اتفاقية مجلس أوروبا 108+ الخاصة بحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية. كما صادقت الدولة على البروتوكول المعدل للاتفاقية.[131] وباعتمادها هذه الاتفاقية، أضحت تونس ملزمة بضمان إنفاذ الاتفاقية بشكل كامل وفعال من خلال إصلاح قوانينها الداخلية الخاصة بحماية البيانات للالتزام بالمبادئ التوجيهية لأفضل الممارسات المنصوص عليها في الاتفاقية 108+.

وبناء على ذلك، قدمت تونس مشروع قانون جديد بشأن حماية البيانات الشخصية ليحل محل القانون الحالي لسنة 2004 في شهر مارس 2018. ولقد تمت صياغة مشروع القانون في ضوء المبادئ الرئيسية للائحة العامة لحماية البيانات داخل الاتحاد الأوروبي (GDPR) حيث ينص على ضرورة التزام كل جهة تقوم بمعالجة البيانات الشخصية بمبادئ الشفافية والنزاهة واحترام كرامة الإنسان. كما يعمل مشروع القانون هذا على توسيع نطاق متطلبات الحماية لتشمل المعالجات غير التونسية للبيانات الشخصية في البلاد. إلى جانب ذلك، يعتزم مشروع قانون 2018 إدخال عدد من التحسينات الأخرى على القانون الساري المفعول. فعلى سبيل المثال، يوسع نص مشروع القانون مفهوم البيانات الشخصية لتشمل الأنشطة والمعلومات على شبكة الإنترنت من قبيل عنوان بروتوكول الإنترنت (IP) لجهاز الكمبيوتر و إحداثيات نظام تحديد المواقع العالمي (GPS) وعنوان البريد الإلكتروني والبيانات البيومترية وغيرها.

[131] التشريع التونسي (2017). *التصديق على انضمام الجمهورية التونسية إلى اتفاقية مجلس أوروبا عدد 108+ الخاصة بحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية وبروتوكولها الإضافي عدد 181 المتعلق بسلطات الإشراف وتدفق البيانات عبر الحدود*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: http://www.legislation.tn/en/content/ratifying-accession-republic-tunisia-convention-n%C2%B0108-he-council-europe-convention-protectio

يسعى مشروع القانون كذلك إلى تعيين مسؤولين مكلفين بحماية البيانات في مختلف المؤسسات المكلفة بمعالجة البيانات الشخصية وحمايتها. ومع ذلك, فإن تعريف البيانات الشخصية لا يميز بين المعلومات الشخصية والبيانات العامة وهو الأمر الذي قد يمس دون قصد بالحق في النفاذ إلى المعلومات. وبالتالي, فمن الضروري الوصول إلى تحقيق توازن بين الحقين من أجل ضمان مبادئ الشفافية والمساءلة وهي نقطة أبرزها عماد الحزقي الرئيس السابق لهيئة النفاذ إلى المعلومة.[132]

وبينما تواصل تونس جهودها من أجل القيام بإصلاحات سياسية وقانونية بصفتها دولة ديمقراطية ناشئة, بات من الملح اليوم وأكثر من أي وقت مضى إعطاء الأولوية للمسائل المتعلقة بالخصوصية وحماية البيانات. فأمام انعدام الاستقرار السياسي, يمكن أن تؤدي الانتهاكات الجسيمة بيانات الشخصية إلى تهديد عملية الانتقال الديمقراطي الجارية في تونس في أعقاب ثورة 2011. ولقد تجلت هذه المسألة خلال الانتخابات الرئاسية والتشريعية لسنة 2019 عندما استغل المرشحون للإنتخابات الرئاسية والتشريعية البيانات الشخصية للمواطنين التونسيين على غرار أرقام بطاقات التعريف الوطنية والأسماء والتوقيعات للحصول على "تزكيات" دون موافقة صريحة من الأفراد المعنيين.[133]

ولا تقتصر انتهاكات الحق في الخصوصية وانعدام الشفافية على المؤسسات الحكومية والعمومية فقط ولكنها تشمل كذلك القطاع الخاص والشركات العاملة في قطاع تكنولوجيا المعلومات والاتصالات ومزودي خدمات الإنترنت. ووفقا للتقرير السنوي حول نشاط الهيئة الوطنية لحماية المعطيات الشخصية, فإنه قلّما يتعامل معالجو البيانات مثل الشركات الخاصة مع الهيئة الوطنية لحماية المعطيات الشخصية للمطالبة بمعالجتها الخاصة وفقا للقانون.[134]

---

[132] أكسس ناو. (13 نوفمبر 2018). *تونس: حوصلة حول اللقاء التفاعلي حول مشروع قانون حماية المعطيات الشخصية والحق في النفاذ إلى المعلومات*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.accessnow.org/%D8%AA%D9%88%D9%86%D8%B3-%D8%AD%D9%88%D8%B5%D9%84%D8%A9-%D8%AD%D9%88%D9%84-%D8%A7%D9%84%D9%84%D9%82%D8%A7%D8%A1-%D8%A7%D9%84%D8%AA%D9%81%D8%A7%D8%B9%D9%84%D9%8A-%D8%AD%D9%88%D9%84-%D9%85%D8%B4%D8%B1/

[133] أكسس ناو. (13 أكتوبر 2019). *تونس: تزوير التزكيات في الانتخابات الرئاسية السابقة لأوانها*. ماذا حدث بعد ذلك؟ تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.accessnow.org/tunisia-falsified-endorsements-in-the-presidential-elections-what-happens-next/

[134] المصدر نفسه.

ولقد أدى الافتقار إلى الإنفاذ السليم للتشريعات والقوانين في تونس إلى حدوث خروقات كبرى تتعلق بالبيانات الشخصية. حيث قدمت وزارة الداخلية في سنة 2016 مشروع قانون يطالب المواطنين باستبدال بطاقات التعريف الوطنية الحالية ببطاقة تعريف بيومترية مزودة بشريحة إلكترونية (الهوية البيومترية).[135] ولقد قوبل هذا الاقتراح بانتقادات واسعة النطاق من قبل منظمات المجتمع المدني لأن بطاقة التعريف الجديدة ستفسح المجال لحدوث انتهاكات كبيرة للخصوصية ولإساءة استخدام البيانات الشخصية بالإضافة إلى زيادة مراقبة وتتبع وتخزين البيانات الصحية والمصرفية للمواطنين.[136] ولم يتضمن مشروع القانون هذا بل لم يقم بالإشارة حتى إلى أية ضمانات إجرائية أو ضمانات كافية أو إلى أية قيود مفروضة على نوعية البيانات التي سيتم جمعها وكيف سيتم استخدام قاعدة البيانات الضخمة هذه الخاصة بالمعلومات الشخصية للمواطنين. ولقد كانت بطاقة التعريف البيومترية المقترحة ستتيح للمسؤولين إمكانية الوصول غير المقيد إلى ملفات بيانات ثرية والتي يمكن أن يساء استخدامها وأن يتم توظيفها على نحو يتعارض مع مصلحة المواطنين. وعلى الرغم من سحب مشروع القانون هذا في سنة 2018 استجابةً للمخاوف التي أثارتها كل من الهيئة الوطنية لحماية المعطيات الشخصية ومنظمات حقوق الإنسان التونسية, إلا أننا نخشى أنه من المحتمل أن يعود مثل هذا المشروع من جديد.

ويمكن للظروف الاستثنائية الحالية الناجمة عن الأزمة الصحية العالمية أن تستخدم كغطاء للحكومة التونسية لإعطاء الأولوية للتشريعات التي تفتقر إلى الشفافية والانفتاح وتمريرها كما هو الحال مع المرسوم المتعلق بالمعرف الوحيد للمواطن حيث صدر هذا المرسوم في مايو 2020 إثر قرار من رئيس الحكومة الأسبق إلياس الفخفاخ بالتعاون مع وزير الشؤون المحلية ووزير تكنولوجيات الاتصال والتحول الرقمي. ولقد صنفته الحكومة باعتباره إحدى أهم الأولويات للتعامل مع أزمة كوفيد- 19 على الرغم من أن نص المرسوم يحتوي على عدة نقاط غامضة قد تؤدي إلى مخاطر أمنية كبيرة.[137] ويسعى هذا المرسوم إلى إدماج المعلومات الخاصة بالمواطنين التونسيين الموجودة في مختلف الخدمات الإدارية.

---

[135] أكسس ناو. (13 جوان 2020). *برامج بطاقات الهوية الوطنية الرقمية: ماذا بعد؟* تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.accessnow.org/national-digital-identity-programmes-whats-next/

[136] أكسس ناو. (02 ديسمبر 2016). *تونس: بيان بشأن بطاقة التعريف الوطنية المقترحة*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.accessnow.org/tunisia-statement-proposed-national-id-card/

[137] أكسس ناو (14 يوليو 2020). *تونس: ما هو المعرف الوحيد للمواطن؟ ولماذا يتم الدفع به الآن؟* تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.accessnow.org/what-is-tunisias-unique-identifier-and-why-is-it-being-pushed-now/

ولكنه لا يتضمن تفاصيل دقيقة تبين ما إذا كانت الحكومة ستستخدم قاعدة بيانات مركزية لجمع البيانات الشخصية عن المواطنين وتخزينها.

2- دراسات الحالة

1) *التعقّب عبر تحديد موقع الهواتف المحمولة والتصريحات المتضاربة*

أعلن رئيس الحكومة السابق إلياس الفخفاخ في 14 يونيو 2020 خلال مقابلة مباشرة أن وحدة العمليات الحكومية الخاصة التي أطلق عليها اسم "قاعة العمليات" قامت بتعقّب مواقع الهواتف المحمولة أو حسب تعبيره "تعقّب المواقع والحركات عبر شرائح الهواتف المحمولة" أثناء فترة الحجر الشامل الناجم عن جائحة كوفيد-19.[138] وعلى إثر موجة من ردود الفعل السلبية من قبل المواطنين على تويتر،[139] ادعى الفخفاخ أن حكومته لم تقم بأية أنشطة مراقبة غير قانونية وأن جميع عمليات التعقّب كانت بالتعاون مع الهيئة الوطنية لحماية المعطيات الشخصية.

ونفى بدوره رئيس الهيئة الوطنية لحماية المعطيات الشخصية, شوقي قداس, صحة ما أفاد به رئيس الحكومة إلياس الفخفاخ مؤكدا أن الهيئة لا علم لها باستخدام تكنولوجيات المراقبة هذه.[140] ولكنه تراجع في اليوم التالي عن تصريحه السابق مشيراً إلى أن الحكومة قد طلبت بالفعل استخدام برمجيّة "المنارة" التي تقوم على تعقّب مواقع الهواتف المحمولة وأنه تم منحها الإذن للقيام بذلك طالما كانت البيانات الشخصية للمواطنين مخفية.[141] وبغض النظر عن هذه التصريحات المتضاربة, فإنه من غير

---

[138] قناة التاسعة (15 يونيو 2020). *مقابلة مع رئيس الحكومة السابق إلياس الفخفاخ*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.youtube.com/watch?v=GnXTBtWDBRg

[139] تغريدة نشرها رئيس الوزراء السابق إلياس الفخفاخ على حسابه. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://twitter.com/ElyesFakhfakh/status/1272279318467674115?s=20

[140] راديو موزاييك إف إم (14 يونيو 2020). *هيئة حماية المعطيات الشخصية لا علم لها بمراقبة هواتف التونسيين*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.mosaiquefm.net/ar/%D8%AA%D9%88%D9%86%D8%B3-D8%A3%D8%AE%D8%A8%D8%A7%D8%B1-%D9%88%D8%B7%D9%86%D9%8A%D8%A9/755697/%D9%87%D9%8A%D8%A6%D8%A9-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D8%B7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%84%D8%A7-%D8%B9%D9%84%D9%85-%D9%84%D9%87%D8%A7-%D8%A8%D9%85%D8%B1%D8%A7%D9%82%D8%A8%D8%A9-%D9%87%D9%88%D8%A7%D8%AA%D9%81-%D8%A7%D9%84%D8%AA%D9%88%D9%86%D8%B3%D9%8A%D9%8A%D9%86

[141] الشارع المغاربي (15 يونيو 2020). *تضارب بين هيئة حماية المعطيات الشخصية ورئيسها شوقي قداس*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://acharaa.com/uncategorized/%D8%AA%D8%B6%D8%A7%D8%B1%D8%A8-%D8%A8%D9%8A%D9%86-%D9%87%D9%8A%D8%A6%D8%A9-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D8%B7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9/

الواضح ما إذا كان لدى الهيئة الوطنية لحماية المعطيات الشخصية القدرات التقنية اللازمة لمراجعة تكنولوجيات التعقّب وضمان إخفاء المعلومات الشخصية للمواطنين.

2) *استخدام الروبوتات والطائرات المُسيّرة للقيام بدوريات في شوارع تونس لإنفاذ الحجر الشامل المرتبط بكوفيد-19*

استخدمت وزارة الداخلية التونسية روبوتات وكاميرات التصوير الحراري لرصد امتثال المواطنين لتدابير التباعد الاجتماعي منذ مارس 2020 تزامنا مع بداية تفشي جائحة كوفيد-19[142] حيث وقعت شركة إينوفا روبوتيكس Enova Robotics التونسية اتفاقية مع وزارة الداخلية لبدء العمل بروبوتات المراقبة المسماة "PGuard" والتي أطلقت عليها وسائل الإعلام المحلية اسم روبوكوبس[143] "robo-cops ". ولقد تم تجهيز أجهزة الروبوت هذه بمجموعة من الكاميرات التي تستخدم الأشعة تحت الحمراء.

أما عدد روبوتات المراقبة التونسية الصنع والمنتشرة في الشوارع غير معروف حيث صرحت الشركة المصنعة إينوفا روبوتيكس لبي بي سي أن المسألة سرية رغم أنه لم يتم رصد سوى روبوت واحد يقوم بدوريات ويستجوب المواطنين في شوارع العاصمة التونسية.[144] وبالإضافة إلى ذلك، تسلمت وزارة الصحة في 23 أبريل 2020 أربع طائرات مُسيَّرة عن بعد مجهزة بكاميرات حرارية ومضخمات صوتية في شكل تبرع من قبل الشركة التونسية الخاصة "تلنات القابضة" Telnet Holding.[145]

ولقد نفذت وزارة الصحة تجربة نموذجية لاستخدام الطائرات المُسيّرة في مدينة سيدي ثابت من ولاية أريانة. ثم وقعت في الثاني من يونيو 2020 اتفاقية تعاون مع وزارة الفلاحة لاستغلال الطائرات المُسيّرة "دعما لجهود وزارة الصحة في مجابهة الجائحة وذلك من خلال إجراء مسوحات على نطاق واسع لقياس

---

[142] بي بي سي. (03 أبريل 2020). *فيروس كورونا: تونس تنشر روبوت شرطي يقوم بدوريات للإشراف على الحجر الشامل*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.bbc.com/news/world-africa-52148639

[143] الصفحة الرسمية لوزارة الداخلية التونسية على الفيسبوك (2020). *وزارة الداخلية تستعمل التقنيات الحديثة في تطبيق إجراءات الحظر الصحي العام*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.facebook.com/ministere.interieur.tunisie/videos/1106579619691659/?v=1106579619691659

[144] المصدر نفسه.

[145] جوهرة إف إم (2020). *للتصدي لفيروس كورونا: "تلنات" تتبرع بـ 4 طائرات مسيّرة لوزارة الصحة*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط: https://www.jawharafm.net/ar/article/%D8%AA%D8%A7%D9%84%D9%86%D8%A7%D8%AA-%D8%AA%D8%AA%D8%A8%D8%B1%D9%91%D8%B9-%D8%A8%D8%B7%D8%A7%D8%A6%D8%B1%D8%AA%D9%8A-%D8%AF%D8%B1%D9%88%D9%86-%D9%84%D9%88%D8%B2%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%B5%D8%AD%D8%A9-%D9%84%D9%84%D8%AA%D8%B5%D8%AF%D9%8A-%D9%84%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D9%83%D9%88%D8%B1%D9%88%D9%86%D8%A7/105/165554

درجات الحرارة لدى المواطنين في محيط يتسع قطره إلى 7 كيلومترات, و لبث رسائل توعوية عبر المضخمات الصوتية".[146] وتجدر الإشارة إلى أن نص الاتفاقية لم ينشر للعلن.

ويُزعم أن "تلنات القابضة" قد تحصّلت على الطائرات دون طيار من الصين حيث ادعت الشركة عبر صفحتها على الفايسبوك أنها نفس الطائرات دون طيار التي وقع استخدامها في مدينة ووهان الصينية.[147] وعلى غرار الروبوتات, لا توجد معلومات متاحة للعموم حول تكنولوجيات الطائرات المُسيّرة وقدراتها. كما لم تكن هناك تعليقات من قبل الهيئة الوطنية لحماية المعطيات الشخصية بهذا الخصوص. ومن غير الواضح ما إذا كان قد تمت استشارتها قبل نشر هذه الطائرات المُسيّرة.

١٧. كوفيد-19 وحماية البيانات

منذ أواخر 2019, دأب العالم على مجابهة جائحة كوفيد-19, و سارعت الحكومات في منطقة الشرق الأوسط وشمال إفريقيا وفي بقيّة أنحاء العالم لاستعمال تكنولوجيات مثل تطبيقات تعقّب مخالطي المرضى وتتبّع المواقع الجغرافيّة في إطار الجهود الرامية لاحتواء الفيروس ووقف انتشاره. ولا يكفي أنه لا توجد أدلّة علميّة كافية لإثبات فعاليّة استعمال مثل هذه التطبيقات كإحدى تدابير الصحّة العامة, إلا أنها تمثّل خطرا كبيرا على الخصوصيّة وحماية البيانات.

رسم بياني: ما مدى الحماية التي توفّرها تطبيقات تعقّب مخالطي المرضى للبيانات والخصوصيّة في منطقة الشرق الأوسط وشمال إفريقيا؟

في محاولة للتخفيف من مخاطر اختراق الخصوصيّة المرتبطة باستعمال هذه التكنولوجيات, قامت أكسس ناو بنشر مجموعة من التوصيات الأساسيّة للحكومات لحماية البيانات والخصوصيّة, بما في ذلك قائمة بما يجب القيام به وما يجب تجنّبه فيما يتعلّق بحماية الخصوصيّة في تطبيقات تعقّب مخالطي

[146] الصفحة الرسمية لوزارة الصحة التونسية على الفيسبوك (2020). *اتفاقية تعاون بين وزارة الصحة ووزارة الفلاحة لاستغلال طائرات مسيّرة في تقصي فيروس كورونا*. تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.facebook.com/santetunisie.rns.tn/photos/a.186499378055841/3146685808703835/?type=3&theater

[147] الصفحة الرسمية لتيلنات القابضة على الفيسبوك. (2020). تم الاطلاع على المصدر بتاريخ 10 يناير 2021. الرابط:
https://www.facebook.com/telnet.holding.tn/posts/207318817354557

المرضى الخاصّة بكوفيد-19.[148] في الجدول أسفله، نستعرض مدى توافق تطبيقات تعقّب مخالطي المرضى المستعملة في كل من الأردن ولبنان وفلسطين وتونس بناء على التوصيات المذكورة أعلاه، ونوضّح في القسم الذي يليه تفاصيل أكثر عن كلّ دولة.

التوصيات	معًا (لبنان)	أمان (الأردن)	أمانكم (فلسطين)	من أجلكم (فلسطين)[941]	احمي (تونس)
طوعيّة/ إلزاميّة	طوعيّة	إلزاميّة	طوعيّة	إلزاميّة	طوعيّة
مصدر مفتوح/ مصدر مغلق	مصدر مفتوح	مصدر مغلق	مصدر مغلق	مصدر مغلق	مصدر مغلق
لامركزيّة/ مركزيّة	مركزيّة	لامركزيّة	لامركزيّة	لامركزيّة	مركزيّة
يحتوي التطبيق على سياسة الخصوصيّة وموافقة المستخدم	نعم	نعم	نعم	غير معروف	نعم
استخدام البيانات مجهولة المصدر	نعم	نعم	لا	غير معروف	نعم

[148] أكسس ناو، (مارس 2020). *الخصوصيّة والصحّة العامّة: ما يجب القيام به وما يجب تجنّبه في تطبيقات تعقّب مخالطي المرضى الخاصّة بكوفيد 19*. تم الاطلاع المصدر بتاريخ 10 يناير 2021، الرابط:
https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf

[149] هذا التطبيق هو تطبيق لتعقّب مرضى كوفيد 19 باستخدام نظام تحديد المواقع وليس تطبيق لتعقّب مخالطي المرضى. لقد تم إدراجه في هذه القائمة لإبراز الإشكاليّات التي يطرحها.

البلوتوث و/أو بيانات الموقع	البلوتوث قد يتطلّب بيانات الموقع في أجهزة أندرويد	بيانات الموقع	البلوتوث وبيانات الموقع	نظام تحديد المواقع	البلوتوث
تأمين البيانات المخزّنة عبر التشفير	نعم	نعم	غير معروف	غير معروف	نعم
تفويضات متناسبة للاحتفاظ بالبيانات	نعم "يتم حذف بيانات الاتصال المخزّنة على الجهاز آليا بعد 21 يوما، وسيتمّ حذف جميع البيانات الموجودة في مخزن البيانات بعد انقضاء جائحة كوفيد-19."	جزئيا يتم حذف البيانات آليا بعد 14 يوما للمستخدمين غير المصابين، ولا تعرف مدّة الاحتفاظ بالبيانات للمستخدمين المعرّضين أو المصابين	غير معروف	غير معروف	جزئيا يتم حذف البيانات آليا بعد 14 يوما للمستخدمين غير المصابين، ولا تعرف مدّة الاحتفاظ بالبيانات للمستخدمين المعرّضين أو المصابين

الأردن

في 20 مايو 2020, أطلقت الأردن تطبيقا جديدا يُدعى "أمان" كجزء من الإستراتيجيّة الرامية لإبطاء سرعة انتشار فيروس كوفيد-19 والسيطرة عليه. شملت الشراكة من أجل تطوير التطبيق كلّ من وزارة الصّحة ومكتب رئاسة الوزراء والشركة الخاصّة ديليفري أسوشياتس ديجيتال (Delivery Associates Digital) و"مجموعة من المتطوعين الخبراء في مجال التكنولوجيا الذين يهدفون إلى الاستفادة من المواهب التقنيّة الأردنية في محاربة جائحة كورونا" تسمّى مجموعة جوتك (Jotech Community). [150]

يعتمد هذا التطبيق على احداثيات تحديد الموقع الجغرافي بالبلوتوث ويتطلّب الإذن للوصول إلى بيانات الحركة الماديّة - التي تحدّد إذا ما كان الشخص بصدد التنقل مشيا على الأقدام أو جريا أو على دراجة أو على متن سيارة- والمدّة التي قضّاها الشخص قرب موقع جغرافي محدّد. يُخزّن تطبيق 'أمان' هذه البيانات على جهاز المستخدم ويُرسل إلى موظّف في وزارة الصحّة ملفاً يحتوي على بيانات الشخص المُصاب لمدّة 14 يوما قبل تاريخ تأكّد العدوى ثمّ يتم تحميل البيانات في خادم وزارة الصحّة.

لا يعتمد هذا التطبيق على بروتوكولات المصادر المفتوحة ممّا يعيق القدرة على فهم كيفيّة عمله ومدى توافق تصميمه مع الالتزام بحماية الحق في الخصوصيّة وأمن المعلومات. [151]

بينما كان تحميل التطبيق طوعياً في المراحل الأولى من انتشار جائحة كوفيد-19, إلا أنه أصبح إلزاميّا للقطاعات العامة والخاصّة والمسافرين داخل الأردن وخارجها كذلك. الأشخاص الذين يزورون الإدارات والمؤسسات العامة أيضا مُلزمون بتحميل التطبيق. في 11 أغسطس 2020, وفي بيان صادر عن رئيس الوزراء عمر الرزّاز لكلّ الوزارات والمؤسسات والإدارات الحكوميّة, أكّدت الحكومة على اتخاذ كلّ التدابير الضروريّة لمنع الزوار من الدخول للدوائر الحكوميّة بدون تفعيل تطبيق تعقّب مخالطي المرضى. كما تمّ تعيين موظّف من كلّ مؤسّسة لتحميل التطبيق لكلّ الموظّفين فيها. كما طلب الرزّاز من كلّ الوزارات

[150] الموقع الرسمي لتطبيق تعقّب مخالطي المرضى "أمان" أطّلع على:https://amanapp.jo/en/page/8/AboutAman

[151] الجمعية الأردنية للمصدر المفتوح (30 أغسطس 2020). *يجب على تطبيقات تعقّب مخالطي المرضى احترام الخصوصيّة و مبادئ الأمن الرقمي*. أطلع عليه في 10 يناير 2021:
https://jordanopensource.org/blog/24/contact-tracing-apps-must-respect-privacy-and-digital-security-principles

والمؤسسات والادارات الحكوميّة مدّه بتقرير أسبوعي عن مدى امتثال الموظفين والزّوار للمتطلّبات والالتزامات الجديدة.[152]

لبنان

لجأت السلطات اللبنانيّة كذلك للتكنولوجيا استجابةً للجائحة, حيث قامت وزارة الصحّة بالشراكة مع كليّة الصحّة والعلوم في الجامعة الأمريكيّة في بيروت بإطلاق تطبيق "معًا" في سبتمبر 2020. ويستعمل التطبيق تقنية البلوتوث لتنبيه المستخدمين عندما يخالطون مستخدمين آخرين تأكّدت إصابتهم بفيروس كوفيد-19. يجمع التطبيق 'بيانات الاتصال' التي تتضمن هويّة مشفّرة للمستخدم ورموزا عشوائيّة ومؤقّتة ينتجها الخادم وقوّة إشارة البلوتوث لدى مستخدمي التطبيق الآخرين الذين يخالطهم المستخدم وتاريخ ووقت المخالطة.[153]

وفقا لتحليل أولي قام بأدائه فريق الأمن الرقمي ضمن منظمة تبادل الإعلام الاجتماعي (SMEX) فإن التطبيق لا يجمع سوى كميّة محدودة من البيانات الشخصيّة لكنّه يحتوي على ثغرات أمنيّة. على سبيل المثال, يفتقر التطبيق للتشفير ويمكن أن يترك المستخدمين الذين لديهم أجهزة أندرويد غير حديثة عرضة لهجمات فجائية. كذلك, فإن العديد من الملفات في التطبيق محدّدة بتعليمات برمجيّة ثابتة, مما يعني أن معلومات سريّة وحسّاسة مثل اسم المستخدم وكلمة السّر الخاصة بمدير البرنامج قد تكون متاحة لجهات أخرى قد تستغلها لغايات خبيثة.[154]

---

[152] الدّستور (11 أغسطس 2020). *بيان من رئيس الوزراء عمر الرزاز حول "أمان" تطبيق تعقّب مخالطي المرضى*. تم الاطّلاع عليه في 10 يناير 2021، https://www.addustour.com/articles/1165890-%D8%AA%D8%B9%D9%85%D9%8A%D9%85-%D9%85%D9%86-%D8%A7%D9%84%D8%B1%D8%B2%D8%A7%D8%B2-%D9%84%D9%84%D9%85%D9%88%D8%B8%D9%81%D9%8A%D9%86-%D9%88%D8%A7%D9%84%D9%85%D8%B1%D8%A7%D8%AC%D8%B9%D9%8A%D9%86-%D8%AD%D9%88%D9%84-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%A3%D9%85%D8%A7%D9%86%D8%8C

[153] وزارة الصّحة العامة اللبنانيّة (2020). *"معًا" معًا ضدّ الكورونا*. أطّلع عليه في 10 يناير 2021: https://moph.gov.lb/en/ma3an

[154] سمكس (17 سبتمبر 2020). *المخاوف الأمنيّة المتعلّقة بالتطبيق الجديد لتعقّب مخالطي المرضى في لبنان*. أطلع عليه في 10 يناير 2021: https://smex.org/security-concerns-with-lebanons-new-contact-tracing-app/

تونس

مع انتشار جائحة كوفيد-19، سارعت الحكومة التونسيّة إلى حلول قائمة على التكنولوجيا في سياق التدابير الرامية للسيطرة على انتقال العدوى. في إطار شراكة بين القطاع العام والخاصّ، تعاقد المرصد الوطني للأمراض الجديدة والمتجدّدة التابع لوزارة الصّحة مع شركة ناشئة تدعى ويزلابز (Wizzlabs) لإطلاق تطبيق تعقّب مخالطي المرضى "احمي".

في 24 يوليو 2020، أكّدت الهيئة الوطنيّة لحماية المعطيات الشخصيّة في بيان صحفي أنها سمحت للتطبيق بجمع البيانات ومعالجتها بدون الإشارة إلى القيام بتقييمات تقنيّة للتطبيق.[155] وقد قامت أكسس ناو بتقديم طلب للوصول للمعلومات حول تطبيق احمي، أولا لوزير الصحّة عبد اللطيف المكي في يوليو 2020، ثمّ قدّمت مطلب تذكيري لوزير الصحة بالنيابة محمد حبيب كشو في أغسطس 2020.[156] طلبنا الحصول على نسخة من الاستشارة التي أجريت بين وزارة الصحّة والهيئة الوطنيّة لحماية المعطيات الشخصيّة حول امتثال تطبيق احمي لمتطلّبات قانون حماية المعطيات الشخصيّة لسنة 2004، إضافة إلى نسخة من العقد الممضي بين الشركة الناشئة "ويزلابز" ووزارة الصحّة بشأن شروط وأحكام استخدام تطبيق احمي.[157]

بعد مرور 20 يوماً -وهي المدّة القصوى التي يجب على الحكومة خلالها الاستجابة لطلب رسمي للوصول للمعلومات بموجب المادّة 14 من القانون العضوي عدد 2016-22- لم نتحصّل على أي إجابة لطلبنا كما لم نتحصّل على إشعار يبرز الأسس القانونيّة الكافية التي تمنعهم من إجابة طلبنا.

[155] الهيئة المستقلّة لحماية المعطيات الشخصيّة. (2020). بيان صحفي (باللغة العربية). أطلع عليه في 10 جانفي 2021 من https://www.facebook.com/INPDP.TN/photos/a.880606318675657/3142913009111632/?type=3&theater

[156] أكسس ناو. (18 سبتمبر 2020). لحماية الخصوصيّة يجب على تونس توخّي الشفافيّة حول التقنيات المستخدمة لمحاربة كوفيد 19. أطّلع عليه في 10 جانفي 2021 من https://www.accessnow.org/to-safeguard-privacy-tunisia-must-be-transparent-on-tech-used-to-fight-covid-19/

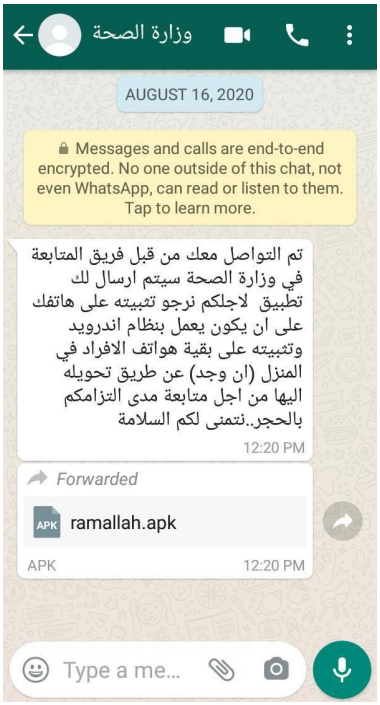
[157] *نفس المصدر*.

فلسطين

في خضم جائحة كوفيد-19, قامت السلطة الفلسطينيّة بإطلاق عدد من تطبيقات تعقّب مخالطي المرضى وتحديد المواقع ذات المصدر المغلق دون اية شفافيّة. بين شهري يونيو ويوليو 2020 ووفقا لشهادات تمّ مشاركتها معنا عبر مركز حملة فقد تم إجبار الطلاب الفلسطينيين العائدين من الخارج على تحميل تطبيق من قبل قوات الأمن على الحدود. لا يمكن التأكد من اسم التطبيق لأنه لم يتمّ إخبار الطلاب عنه, بدل من ذلك قامت القوات الأمنيّة بأخذ هواتف الطلاب وتنزيل التطبيق مباشرة. أفاد بعض الطلاب بأن التطبيق قد تم تحميله من متصفّح كروم (Chrome) وليس من أحد متاجر التطبيقات وأنه ربّما قد يكون اسم التطبيق "من أجلكم".

وفقا لبحثنا, نعتقد أن الأمر يتعلّق بنفس التطبيق الذي أبلغ عنه مواطن فلسطيني في أغسطس 2020, بعد تأكد إصابته بكوفيد-19, عن طريق رسالة عبر الواتس آب من وزارة الصحة في فلسطين تحمل ملف حزمة أندرويد (APK) للتنزيل.[158]

[158] أبك (APK) هو صيغة حزمة الملفات المستخدمة من قبل نظام تشغيل أندرويد وعدد من نظم التشغيل الأخرى المبنية على أندرويد لتوزيع تطبيقات الهواتف وتحميلها.



الصورة 2. صورة عن رسالة الواتس أب المُرسلة من قبل وزارة الصحّة في فلسطين والمرفقة بملف حزمة أندرويد (APK).

لقد تحصّلنا على نسخة من ملف حزمة أندرويد (APK) من مركز حملة. وبعد التحقيق فيها عبر أبكتول (Apktool)[159] , وجدنا أن التطبيق المذكور أعلاه يُدعي بالفعل "من أجلكم" وهو تطبيق يتطلّب إذنا لجمع البيانات من الهاتف عبر موقع الجهاز. وقد تم تطوير التطبيق من قبل قوات الأمن الفلسطينيّة وهو يهدف لرصد تحرّكات مرضى كوفيد-19 وامتثالهم لقواعد الحجر المنزلي.[160] ومع أن مدير الأمن وحدة السايبر في الأمن الوقائي قد أفاد بأنه قد تم تطوير التطبيق وفقا "للمعايير الدوليّة",[161] إلا أنه لا توجد شفافيّة حول التكنولوجيا المستخدمة أو سياسة الخصوصيّة في التطبيق.

عند القيام ببحثنا في سبتمبر 2020, عثرنا على صفحة في موقع وزارة الصحّة حول تطبيق تعقّب خاص بكوفيد-19 يدعى "منيع". ووفقا لوثيقة حول الخصوصيّة وشروط الاستخدام, فإنّ التطبيق يستعمل كلّ من البلوتوث ونظام تحديد المواقع.[162] لكننا لم نتمكن من العثور على الرابط الخاص بتحميل التطبيق

[159] أداة مفتوحة المصدر تمكّن من فكّ تشفير مصادر تطبيقات أندرويد.

[160] الغد (15 يوليو 2020). *فلسطين تطوّر تطبيق تعقّب مخالطي المرضى للسيطرة على انتشار كوفيد 19*. أطّلع عليه في 10 يناير 2021 من https://www.alghad.tv/%D9%81%D9%84%D8%B3%D8%B7%D9%8A%D9%86-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%84%D9%85%D8%B1%D8%A7%D9%82%D8%A8%D8%A9-%D8%A7%D9%84%D9%85%D8%B5%D8%A7%D8%A8/

[161] نفس المصدر.

[162] وزارة الصحّة في فلسطين (2020). *شروط استخدام تطبيق تعقّب مخالطي المرضى*. أطلع عليه في 20 يناير 2021 من http://site.moh.ps/Content/File/kwGvJ8oDcPxnQBaKgvwTL5af_EzMT7VqDTzoCvRwN66FEthB7.pdf

كما لم نجده في متاجر تطبيقات آبل أو جوجل. وتم الإشارة للخصوصيّة في فقرة في شروط الاستخدام "كأحد أهم أولويات الوزارة" لكن بدون توفير تفاصيل أو معلومات إضافيّة. وبحلول أكتوبر 2020, لم يعد من الممكن الوصول لتلك الصفحة مما يدفعنا للتفكير بأنه قد تم التخلّي عن هذا المشروع في نهاية المطاف.[163]

في 26 أكتوبر 2020, أعلنت وزارة الصحة عن إطلاق تطبيق جديد لتعقّب مخالطي المرضى يدعى "أمانكم" [164]. يعتمد هذا التطبيق على تقنية البلوتوث, ووفقا لوزارة الصحة فإن البيانات المجموعة يتم تسجيلها على الهاتف. [165] ويحيل الرابط المخصص لتنزيل التطبيق إلى تحميل ملف حزمة أندرويد (APK). كان هذا التطبيق أيضا متاحا على متاجر تطبيقات غوغل وأبل وقد تم تحميله أكثر من 5000 مرّة بحلول نوفمبر 2020.

عند تحليل ملف حزمة أندرويد عبر أداة أبكتول (Apktool), وجدنا أن "أمانكم" هو اسم جديد أو صيغة جديدة من تطبيق "منيع" يتطلّب إذنا لجمع البيانات عبر تقنية البلوتوث ونظام تحديد المواقع. حتى إذا ادّعت وزارة الصحّة عبر المعلومات القليلة المتاحة للعموم أن تطبيق تعقّب مخالطي المرضى مبني على تكنولوجيا البلوتوث, فإن مصادرنا في فلسطين اختبرت التطبيق وأكّدت أنه لا يمكن فتح التطبيق دون السماح له بالوصول لموقع الجهاز. أما وزارة الصحّة, فهي لم تقدّم أي توضيح لسبب حاجة التطبيق للوصول لمعلومات موقع الجهاز.

قامت وزارة الصحة بنشر سياسة الخصوصيّة الخاصة بالتطبيق على موقعها. [166] لكن سياسة الخصوصيّة لا توفر بعض المعلومات الأساسيّة المحدّدة مثل نوع المعلومات التي يجمعها التطبيق ومن يمكنه الوصول لها وكيف سيتم استخدامها, كما لا تتضمن بندا يتعلق بانقضاء مدّة استخدامها.

---

[163] الموقع الرسمي لوزارة الصّحة الفلسطينيّة. أطلع عليه في 10 يناير 2021 من #http://site.moh.ps/index/ArticleView/ArticleId/4976/Language/ar

[164] أخبار اليوم (2020). *"أمانكم" تطبيق لتعقّب مخالطي المرضى يهدف لرصد انتشار فيروس كوفيد 19 في فلسطين*. أطلع عليه في 10 يناير 2021 من https://akhbarelyom.com/news/newdetails/3144846/1/-%D8%A3%D9%85%D8%A7%D9%86%D9%83%D9%85-..-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%B0%D9%83%D9%8A-%D9%81%D9%8A-%D9%81%D9%84%D8%B3%D8%B7%D9%8A%D9%86-%D9%84%D8%B1%D8%B5%D8%AF-%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D9%83%D9%88%D8%B1%D9%88%D9%86%D8%A7

[165] وزارة الصحة في فلسطين (2020). *"أمانكم" تطبيق تعقّب مخالطي المرضى* . أطلّع عليه في 10 يناير 2021 moh.ps/mohsite/index/Amankom/Language/ar

[166] نفس المصدر.

بدل من ذلك، تشير الوزارة إلى أنّه "سيتم حذف كلّ بيانات المستخدمين عند نهاية جائحة كوفيد مع إعلان وزارة الصحة الفلسطينيّة عن نهايتها في فلسطين".[167]

علاوة على ذلك، وفي قسم تحت عنوان "طريقة عمل التطبيق وسياسة الخصوصيّة"، توجد إشارة إلى "خوادم مؤمنة ومشفرة" بدون الاشارة إلى ضمانات الأمن والخصوصيّة التي تتحقق من أن الاتصال بين المستخدمين والخوادم مؤمن ومشفّر أيضا. إعدادات شبكة الأمن في التطبيق تخوّل مرور النصّ بشكل واضح وهو أمر غير مفاجئ بما أن التطبيق يحتوي على روابط لبعض الموارد المتاحة على الموقع الرسمي لوزارة الصحة الذي لا يعتبر مؤمنا بدوره.

٧. توصيات متعلّقة بالسياسة العامة

منذ تأسيس أكسس ناو في 2009، دأبت المنظمة على العمل على تشريعات وسياسة حماية البيانات، ولا يزال ذلك في قائمة الأولويات الإقليميّة والدوليّة لمنظمتنا. تنبع توصياتنا المتعلّقة بالسياسة المذكورة أسفله من تجاربنا في العمل على تشريعات حماية الخصوصيّة والبيانات حول العالم وبرامج الهوية الرقميّة ومؤخرا أبحاثنا المتعلّقة بحماية الخصوصيّة خلال جائحة كوفيد-19.

للحكومات	
1. **اعتماد قانون شامل لحماية البيانات يتمحور حول حقوق الأشخاص**	يجب على المشرّعين في المنطقة إعطاء الأولويّة لاعتماد أطر قانونيّة قويّة لحماية البيانات ترتكز على حماية الحقوق الأساسيّة للمستخدمين وتقديمها على المصالح الاقتصادية للحكومة والشركات الخاصّة. لهذا الغرض، قمنا بإعداد دليل للمشرعين، **وضع إطار لحماية البيانات: دليل بما يجب القيام به وما يجب تجنّبه من قبل المشرّعين**، وذلك بناء على تجربتنا والدروس المستقاة من اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي [168].

[167] نفس المصدر.
[168] أكسس ناو. (نوفمبر 2018). وضع إطار لحماية البيانات: دليل بما يجب القيام به وما يجب تجنّبه من قبل المشرّعين _ دروس مستقاة من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي. أطلع عليه في 10 جانفي 2021 من https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

	ومن المهم أن يتضمّن القانون حقوقاً ملزمة للمستخدمين بما في ذلك الحق في الموافقة الصريحة والاعتراض والحذف والتصحيح والوصول لبياناتهم. والأهم من ذلك, يجب على الحكومات أن تعقد مشاورات مفتوحة وشفافة وشاملة عند الشروع في أي إصلاحات أو عند اعتماد مثل هذه الأطر وذلك لتجنّب سنّ قوانين ضعيفة تخلق نتائج عكسيّة, ويجب ضمان المشاركة الهادفة لمؤسسات المجتمع المدني في كافة مراحل صنع القانون.
2. **إنشاء هيئة مستقلة لحماية البيانات وآليات فعّالة للتنفيذ**	لا يمكن أن يكتمل أي إطار قانوني لحماية البيانات, مهما كان متقدّما, بدون آليات قويّة للتنفيذ تتضمن إنشاء هيئة أو لجنة مستقلّة لحماية البيانات. يجب أن يكون للهيئة السلطات والموارد والخبرات اللازمة لرصد التنفيذ وفتح التحقيقات وفرض العقوبات في حالات اهمال حماية البيانات او وقوع الانتهاكات. كما يجب فصل إدارة هيئة حماية البيانات ووظائفها عن السلطة التنفيذيّة والمؤسسات الأمنيّة.
3. **تجنّب الاستثناءات واسعة النطاق من حماية البيانات وتقييد الخصوصيّة باسم الأمن القومي.**	عادة ما تقوم الأجهزة الأمنية في منطقة الشرق الأوسط وشمال إفريقيا بتقييد وانتهاك حق المواطنين في الخصوصيّة تحت ذريعة حماية الأمن القومي ومحاربة الإرهاب. وغالبا ما تعمل هذه الأجهزة في كنف السريّة وبدون رقابة. لذلك, يجب ألا تقدّم قوانين وتشريعات حماية البيانات والخصوصيّة إعفاءات لأجهزة الأمن القومي. وفي هذا السياق, من الضروري أن يخضع أي وصول للبيانات الشخصيّة للمستخدمين لمبدأ الضرورة والتناسب.
4. **ترسيخ مبادئ "الخصوصيّة بحكم التصميم" في أي مقترحات أو برامج تعالج البيانات.**	تعدّ برامج الهويّة الرقميّة و جوازات السفر البيومترية والخدمات الحكوميّة الالكترونيّة برامج مثقلة بالبيانات, وخاصّة البيانات الحساسة والمعلومات المحدّدة للهوية الشخصيّة. ولذلك, من بالغ الأهميّة أن تلتزم الحكومات بمفهوم حماية البيانات ابتداءاً من مرحلة التصميم. يجب أن يتحقق مهندسو مثل هذه البرامج من مراعاة الخصوصية وحماية البيانات في كلّ من المراحل الأوليّة لتصميم المنتج أو الخدمات وطوال مدّة التوزيع والاستخدام, كما يجب التأكد من إعدادها وفقا لأعلى معايير ضمانات الخصوصيّة ومراجعتها بشكل دوري.

5. عند إطلاق برامج الهويّة الرقميّة والبيومتريّة، يجب على الحكومات التحقق من:[169]	• تحديد وتقييد نطاق استخدام برامج الهويّة الرقميّة بشكل واضح ومنصوص عليه في القانون مع شرح استخدامه للجمهور. • طوعية تسجيل الهويّة الرقميّة واستخدامها. لا يجب أن يُشترط على المواطنين استخدام الهوية الرقمية لتمكينهم من الوصول للخدمات الحكوميّة مثل الرعاية الصحيّة والتعليم. • عمليّة جمع البيانات وتخزينها ليست مركزيّة. من شأن جمع البيانات الخاصّة بالهويّة الوطنيّة الرقميّة وتخزينها بشكل مركزي خلق موضع فشل واحد والتسبب في مخاطر كبيرة ولذلك يجب تجنّب قواعد البيانات المركزية. • وجود بنية تحتيّة تكنلوجيّة قويّة ومؤمّنة ضمن إطار شامل للأمن السيبراني.

للشركات الخاصّة
• نشر التزام رسمي وصريح باحترام وحماية الحق في الخصوصيّة والبيانات الشخصيّة.
• إصدار تقارير دوريّة عن الشفافيّة تكشف عن طلبات جهات إنفاذ القانون للحصول على معلومات المستخدمين وتهديدات الخصوصيّة والمراقبة. يجب أن توفر هذه التقارير أيضا معلومات عن الإجراءات التي تتخذها الشركة عند الاستجابة لهذه الطلبات وإخطار المستخدمين المعنيين والمساعدة على تحديد المخاطر على الخصوصيّة.
• الامتثال للوائح حماية البيانات والخصوصيّة حيثما ينطبق، نظرا لأنها توفّر تعليمات أساسيّة حول جمع البيانات الشخصيّة ومعالجتها.
• توفير آليات شكوى وتبليغ فعالة متوافقة مع الحقوق للمستخدمين ليتمكنوا من الإبلاغ عن أية انتهاكات لخصوصيّتهم بشكل مبكّر وصريح.

[169] للاطلاع على إطار أشمل للبرنامج الوطني للهوية الرقميّة، راجع توصياتنا الأساسيّة المتعلّقة بالهوية الرقمية في ورقة العمل: *البرامج الوطنيّة للهويّة الرقميّة: ماذا بعد؟* أطلع عليه في 10 يناير 2021 https://www.accessnow.org/national-digital-identity-programmes-whats-next/

للمنظمات الدوليّة	
تستخدم المنظمات الدولية تكنولوجيا الاستدلال البيومتري التي تجمع بيانات بيومتريّة للتعرّف على اللاجئين والتأكد من هوياتهم, وتعلل المنظمات ذلك بأن هذه التقنيات تجعل توصيل المساعدات الانسانيّة والدفعات الماليّة أكثر دقّة وفعاليّة, كما تمنع الاحتيال وتعزّز المسائلة. لكن, كما وضّحنا سابقا في هذا التقرير, فإن جمع البيانات البيومتريّة واستخدامها يمثّل خطرا على الأفراد. ونظرا لارتفاع مخاطر استغلال هذه البيانات وعدم امكانيّة إصلاح ضرر هذه الانتهاكات, فإن أكسس ناو تدعو لإيقاف جمع البيانات البيومتريّة واستخدامها (بما في ذلك تقنية التعرّف على الوجه) لأغراض التحقق من هويّة الأشخاص.[170] يجب أن تكون مطالبة الأشخاص بتوفير البيانات البيومتريّة الشخصيّة وغير المتغيّرة التي تطرح مخاطر كبيرة على الخصوصيّة تدبيرا يُلجأ إليه كملاذ أخير.	
1. **التحقق من أن تقديم المعرّفات البيومتريّة أمر طوعي اختياري وليس إجراءاً إلزاميا**	يجب عدم إكراه الأشخاص, خاصّة أولئك الذين ينتمون إلى مجموعات مهمّشة ومستضعفة, على توفير بياناتهم البيومتريّة كشرط مسبق للحصول على المساعدات والخدمات. يجب أن يكون استعمال البرامج البيومتريّة والهويّة الرقميّة مبنيّا على موافقة المستخدمين. يمكن أن يؤدي اعتماد التسجيل أو الالتحاق الإجباري المبني على برنامج تحديد هويّة واحد إلى تفاقم خطر الإقصاء والتنميط والمراقبة. بدلا عن ذلك, يجب تعزيز وتنفيذ أطر اختيارية متعدّدة لتحديد الهويّة والتحقق منها.
2. **القيام بتقييمات مسبقة ولاحقة للآثار المترتبة على حقوق الإنسان**	يجب على المنظمات الإنسانيّة التحقق من أن التكنولوجيا المستخدمة مبنيّة على أساس حماية الحقوق الأساسيّة للمستخدمين وخاصّة الحق في الخصوصيّة. ويجب القيام بتقييمات الأثار على حقوق الإنسان قبل تفعيل هذه البرامج وخلال تطبيقها وطوال دورة حياة هذه البرامج.
3. **عدم إنشاء قواعد بيانات مركزيّة للبيانات البيومتريّة للأشخاص**	نظرا لحساسيّة المعلومات البيومتريّة, نوصي بتخزين مثل هذه البيانات بطريقة غير مركزيّة. تخلق قواعد البيانات المركزيّة موضع فشل وحيد مما يجعلها أكثر عرضة للتهديدات والهجمات.

[170] راجع (#WhyID) الرسالة المفتوحة إلى الأمم المتحدة، المنظمات الدوليّة الانسانيّة ووكالات التمويل والحكومات الوطنيّة حول استخدام برامج الهويّة الرقميّة: https://www.accessnow.org/whyid/

4. توفير الشفافيّة فيما يتعلّق بالكشف عن سياسات الأمن الإلكتروني.	يجب أخذ الخطوات اللازمة لضمان الكشف للعموم عن مبادئ وسياسات الأمن السيبراني الموضوعة لحماية البنية التحتيّة لبرامج الهويّة الرقميّة. ونظرا لأهميّة وحجم مثل هذه المشاريع للعموم , فإن الإفصاح عن هذه المعلومات يجب أن يكون حقا للمواطنين. إضافة إلى ذلك, فإن مثل هذه الممارسات من شأنها تشجيع الخبراء والأطراف المعنيّة الأخرى على مراجعة هذه السياسات. وهذا من شأنه إطلاع الحكومة وطرح المسائل التي تستوجب مشاورات وتطوير سياسات أمن إلكتروني أكثر قوة ومنظومة أكثر أمانا بشكل عام.
5. إجراء تقييمات إلزاميّة للأثر على حقوق الإنسان واتخاذ إجراءات الحيطة الواجبة لكلّ شراكة بين القطاع العام والخاص	يجب التحرّي عن الشركات الخاصّة التي تملك في عهدتها بيانات شخصيّة حسّاسة خاصّة بملايين الأشخاص للتأكد من احترامها وحمايتها لحقوق الإنسان عبر عمليّة شاملة لاتخاذ الحيطة الواجبة. كما يجب أن تكون الشراكات بين القطاع العام والخاص شفافة وأن تتبع إجراءات الشراءات العامة المفتوحة والشفافة والتعاقد المفتوح وتقارير الشفافيّة, مع إتاحتها للجمهور.
6. التقليل من جمع البيانات ونقلها	يجب على من يبادر لخلق برامج الهويّة الرقميّة التقليل من جمع وتحويل البيانات الخاصّة بالمعرّفات البيومتريّة. هذا من شأنه التقليص من المخاطر والضرر الذي قد يقع إذا تم اختراق البيانات. بصفة عامة, نحن نوصي مطوري البرامج باستعمال التحقق من الهوية عبر الجهاز عند استعمال المعرّفات البيومتريّة "كلمة عبور"على سبيل المثال بدلا من استخدام تخزين البيانات/التحقق منها بشكل مركزي عبر السحابة (cloud).

٧. الخلاصة

يوضّح تحليل الأطر القانونيّة والأمثلة المعروضة في هذا التقرير للحكومات الوطنيّة في منطقة الشرق الأوسط وشمال إفريقيا أهميّة إعطاء الأولويّة لاعتماد تشريعات قويّة وفعّالة لحماية البيانات ترتكز على حقوق المستخدمين وتخوّل لهم الاستقلاليّة والقدرة على الاختيار فيما يتعلّق بمعلوماتهم الشخصيّة, وتحمي خصوصيتهم من المراقبة والاستغلال لغايات الرّبح ومن التهديدات والاختراقات والانتهاكات العرضيّة أو غير القانونيّة. عند صياغة قوانين حماية البيانات, يجب على الحكومات التحقق من إجراء مشاورات عامّة وشفافة وشاملة مع كلّ الأطراف المعنيّة وخاصّة مع المنظمات غير الحكوميّة والمجتمع المدني. ولبلوغ هذه الغاية, تُرحّب منظّمة أكسس ناو بفرصة التعاون مع صانعي السياسات العامة في المنطقة لتعزيز وحماية الحق في الخصوصيّة وحماية البيانات الشخصيّة في المنطقة.

ومع ذلك, فما هذه سوى الخطوة الأولى, إذ أن إنفاذ هذه التشريعات هو مفتاح النجاح. وتتشارك كل من الحكومات والشركات الخاصة والمنظمات الدوليّة التي تجمع البيانات الشخصيّة للمواطنين وتعالجها في مسؤوليّة حماية البيانات الشخصيّة وتوفير الشفافيّة حول كيفيّة القيام بجمع واستعمال وتخزين ومشاركة البيانات- ومع من. و في هذا الصدد نشجع قرّاء هذا التقرير, وخاصّة الصحفيين الاستقصائيين ومنظمات المجتمع المدني , على مواصلة التحقيق في انتهاكات حماية البيانات واستغلالها في كامل المنطقة, إذ يمثّل ذلك خطوة ضروريّة لتسليط الضوء على هذه القضايا وللدفاع عن الحقوق الرقميّة في منطقة الشرق الأوسط وشمال إفريقيا.