الأمم المتحدة

A/HRC/51/17

الجمعية العامة

Distr.: General
4 August 2022
Arabic
Original: English

مجلس حقوق الإنسان

الدورة الحادية والخمسون

12 أيلول/سبتمبر – 7 تشرين الأول/أكتوبر 2022

البندان 2 و3 من جدول الأعمال

التقرير السنوي لمفوضة الأمم المتحدة السامية لحقوق الإنسان وتقارير المفوضية السامية والأمين العام

تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية

الحق في الخصوصية في العصر الرقمي

تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان*

موجز

يناقش هذا التقرير، المقدم عملاً بقرار مجلس حقوق الإنسان 4/48، الاتجاهات والتحديات الأخيرة المتعلقة بالحق في الخصوصية. ويركز التقرير، بوجه خاص، على ما يلي: (أ) إساءة استخدام أدوات الاختراق الحاسوبي الاقتحامية؛ (ب) الدور الرئيسي للتشفير في ضمان التمتع بالحق في الخصوصية وغيره من الحقوق؛ (ج) تفشي رصد الأماكن العامة. ويسلط الضوء على خطر إنشاء نظم للمراقبة والرقابة الشاملة التي قد تقوض تنمية مجتمعات نابضة بالحياة تحترم الحقوق.

* اتُّفق على نشر هذا التقرير بعد تاريخ النشر المعتاد لظروف خارجة عن إرادة الجهة المقدِّمة له.

أولاً- مقدمة

1- يقدم هذا التقرير عملاً بقرار مجلس حقوق الإنسان 4/48 الذي طلب فيه المجلس إلى مفوضية الأمم المتحدة السامية لحقوق الإنسان أن تعد تقريراً يحدد الاتجاهات والتحديات الأخيرة فيما يتعلق بحق الإنسان في الخصوصية وأن تحدد مبادئ حقوق الإنسان وضماناتها وأفضل ممارساتها ذات الصلة وتوضحها، وتقديم التقرير إلى المجلس في دورته الحادية والخمسين. ويعكس التقرير الردود الواردة تلبيةً للدعوة التي وجهتها المفوضية من أجل تقديم إسهامات[(1)].

2- يشهد الناس في جميع أنحاء العالم تطورات تكنولوجية مثيرة للإعجاب، بالإضافة إلى الابتكارات التي تعمل على تحسين حياة الناس والنهوض بالاقتصادات. ومع ذلك، فالناس شهود أيضاً على استخدام الأدوات الرقمية ضدهم، مما يعرضهم لأشكال جديدة من المراقبة والتنميط والتحكم. وضمان احترام وحماية الحق في الخصوصية، المعترف به في المادة 12 من الإعلان العالمي لحقوق الإنسان، والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، وفي العديد من الصكوك الدولية والإقليمية الأخرى لحقوق الإنسان[(2)]، يمكن أن يؤدي دوراً محورياً في إدارة التهديدات الرقمية الجديدة لحقوق الإنسان، التي ترتبط ارتباطا وثيقا بالبيانات الشخصية التي تشغل محركات المجتمعات الرقمية.

3- واستناداً إلى التقارير السابقة المقدمة إلى مجلس حقوق الإنسان التي تتناول التحديات التي تواجه الحق في الخصوصية[(3)]، يركز هذا التقرير على ثلاثة اتجاهات بارزة تتعلق بدور الدول في حماية وتعزيز الحق في الخصوصية، وهي: إساءة استخدام أدوات الاختراق الحاسوبي الاقتحامية؛ (ب) الدور الرئيسي للتشفير القوي في ضمان التمتع بالحق في الخصوصية وغيره من الحقوق؛ (ج) تفشي رصد الأماكن العامة. ويسلط التقرير الضوء على الخطر الحقيقي والمتسارع المتمثل في إنشاء نظم للمراقبة والسيطرة الشاملة التي قد تخنق في نهاية المطاف تنمية مجتمعات نابضة بالحياة ومزدهرة وتحترم الحقوق، ويختتم بعرض مجموعة من التوصيات لمنع هذا الوضع من الحدوث.

ثانياً- مراقبة الأجهزة الشخصية والاتصالات

ألف- الاختراق الحاسوبي

4- في تموز/يوليه 2021، نشرت مجموعة "قصص محرمة" (Forbidden Stories)، وهي اتحاد للصحافة الاستقصائية، تدعمه منظمة العفو الدولية، روايات عن استخدام برنامج "بيغاسوس" (Pegasus) مما لفت الانتباه الدولي إلى أزمة حقوق الإنسان التي كانت تتزايد منذ سنوات، وهي الانتشار العالمي لأدوات الاختراق الحاسوبي لأغراض المراقبة المستهدفة والسرية للأجهزة الرقمية. وفي حين يزعم أن أدوات التجسس هذه تستخدم لمكافحة الإرهاب والجريمة، فإنها كثيراً ما تستخدم لأسباب غير مشروعة، بما في ذلك قمع الآراء الناقدة أو المعارضة ومن يعبرون عنها، بمن فيهم الصحفيون والشخصيات السياسية المعارضة والمدافعون عن حقوق الإنسان.

(1) انظر https://www.ohchr.org/en/calls-for-input/2022/call-inputs-report-right-privacy-digital-age-2022.

(2) انظر المادة 16 من اتفاقية حقوق الطفل؛ والمادة 14 من الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم؛ والمادة 22 من اتفاقية حقوق الأشخاص ذوي الإعاقة؛ والمادة 10 من الميثاق الأفريقي لحقوق الطفل ورفاهيته؛ والمادة 11 من الاتفاقية الأمريكية لحقوق الإنسان؛ والمادة 8 من اتفاقية حماية حقوق الإنسان والحريات الأساسية.

(3) انظر A/HRC/27/37 وA/HRC/39/29 وA/HRC/44/24 وA/HRC/48/31.

5- إن نطاق عمليات برامج التجسس بيغاسوس وعدد الضحايا مذهلان. واستناداً إلى قائمة مسربة تضم أكثر من 50 000 من أرقام هواتف جهات مستقصدة خاضعة فعلاً أو يحتمل أن تخضع للرقابة وتحليل الطب الشرعي للعديد من الهواتف المخترقة، كشفت التقارير في عام 2021 أن ما لا يقل عن 189 صحفياً و85 مدافعاً عن حقوق الإنسان وأكثر من 600 سياسي ومسؤول حكومي، بمن فيهم وزراء في مجلس الوزراء ودبلوماسيون تأثروا بصفتهم أهدافا لتلك العمليات[4]. وكشفت التحقيقات عن تجسس على قضاة ومحامين وأطباء وقادة نقابيين وأكاديميين[5]. واعترفت مجموعة NSO، الشركة التي تصنع وتبيع برنامج بيغاسوس، بأن عملائها يستهدفون ما بين 000 12 و000 13 فرداً في السنة[6].

6- ويعد برنامج التجسس بيغاسوس أبرز مثال في عالم برامج التجسس التي تسوقها الشركات إلى الحكومات في جميع أنحاء العالم، وهو عالم ما فتئ يكبر[7]. ووفقاً للباحثين، حصلت 65 حكومة على الأقل على برامج تجارية لأدوات المراقبة والتجسس[8]. وذكرت NSO أن من بين عملائها توجد 60 وكالة حكومية في 45 دولة. وقبل أيام فقط من كشف المعلومات المتعلقة ببرنامج بيغاسوس، أصدر سيتيزن لاب ومايكروسوفت تقريراً يشرح بالتفصيل كيف استخدمت الحكومات برنامجا آخر، كانديرو (Candiru)، لاستهداف المدافعين عن حقوق الإنسان والمعارضين والصحفيين والناشطين والسياسيين[9]. وفي تشرين الثاني/نوفمبر 2021، أعلنت شركة التواصل الاجتماعي Meta أنها عطلت سبعة كيانات استهدفت الأشخاص عبر الإنترنت في أكثر من 100 دولة. ونبهت الشركة حوالي 000 50 شخصاً تعتقد أنهم استهدفوا بمثل هذه الأنشطة[10]. وأفيد بأن أكثر من 500 شركة تقوم بتطوير أدوات المراقبة هذه وتسويقها وبيعها للحكومات[11].

7- وقدرات أدوات وخدمات برامج التجسس المعروضة في السوق العالمية هائلة. فعلى سبيل المثال، يمنح بيغاسوس، بمجرد تثبيته، وصولا كاملا وغير مقيد إلى جميع أجهزة الاستشعار والمعلومات الموجودة على الأجهزة المخترقة، مما يحول معظم الهواتف الذكية بشكل فعال إلى أجهزة مراقبة تعمل على مدار الساعة، والوصول إلى الكاميرا والميكروفون، وبيانات تحديد الموقع الجغرافي، ورسائل البريد الإلكتروني،

(4) انظر https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.

(5) انظر https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; https://forbiddenstories.org/about-the-pegasus-project/; https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

(6) في شهادة أمام البرلمان الأوروبي، لجنة التحقيق للتحقيق في استخدام بيغاسوس وبرامج التجسس والمراقبة المكافئة، 21 حزيران/يونيه 2022، على الرابط التالي: https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

(7) انظر https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf, p. 29.

(8) انظر https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019.

(9) انظر https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

(10) انظر https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. وللاطلاع على أمثلة أخرى، انظر https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/; https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating; and https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

(11) A/HRC/41/35، الفقرة 6؛ انظر أيضاً https://data.mendeley.com/datasets/csvhpkt8tm/2 للحصول على مخزون عالمي من برامج التجسس التجارية.

والرسائل، والصور ومقاطع الفيديو، وكذلك جميع التطبيقات. ويسمح للجهة الدخيلة بالحصول على صورة مفصلة عن حياة ضحاياها وأفكارهم وتفضيلاتهم وأنشطتهم المهنية وتفكيرهم السياسي وصحتهم ووضعهم المالي وحياتهم الاجتماعية والحميمة. ومع أن العديد من أدوات الاختراق الحاسوبي تتطلب بعض الإجراءات من جانب الضحية، مثل النقر على رابط أو فتح مرفق برسالة، يتم تثبيت بيغاسوس عن طريق التخفي، من خلال الهجوم الذي لا يتطلب من الضحية أي عملية نقر (المسمى "هجوم النقر الصفري‘‘)[12]. ويجعل البرنامج من المستحيل تقريباً على الضحايا تجنب الاختراق بمجرد استهدافهم.

8- ويمكن أن تتخذ عمليات الاختراق الحاسوبي أشكالا عديدة بدرجات متفاوتة من التدخل الاقتحامي. ومع أن الحصول على السيطرة الكاملة على الهاتف المحمول أو الحاسوب يساعد على رسم صورة مفصلة عن حياة أولئك المستهدفين، فإن مجموعة متنوعة من تقنيات الاختراق الأخرى يمكن أن تكون أقل تدخلاً، وإن كانت على درجة بالغة من الخطورة، بما في ذلك الوصول إلى حسابات البريد الإلكتروني. ويمكن للاختراق الحاسوبي أن يقود أيضاً للوصول إلى الأجهزة المتصلة الأخرى، مثل الأجهزة التكنولوجية الملبوسة أو المركبات، والتي قد توفر معلومات إضافية، بما في ذلك بيانات الصحة والموقع الجغرافي. ويمكن أيضاً تحويل الأجهزة المزودة بكاميرات أو ميكروفونات، مثل مكبرات الصوت الذكية أو أجهزة التلفزيون، إلى أدوات مراقبة سمعية بصرية. وقد تؤدي مهاجمة البنية التحتية لجهات تقديم الخدمات إلى تهيئة الوصول إلى كميات هائلة من المعلومات حول آلاف العملاء، بما في ذلك اتصالاتهم وبيانات التصفح والمواقع الخاصة بهم[13]. وتركز المناقشة في الفقرات التالية على اختراق أجهزة الاتصال الشخصية.

9- ويشكل اختراق أجهزة الاتصال الشخصية تدخلاً خطيراً في الحق في الخصوصية ويمكن ربطه بانتهاكات مقلقة لمجموعة من الحقوق الأخرى. وبالنظر إلى أن التسلل إلى أجهزة الاتصالات الرقمية يتيح الوصول إلى المسودات وتاريخ البحث والتصفح، فإنه قد يسمح أيضاً بالغوص في أساليب وأنماط تفكير الأفراد الخاضعين للاختراق الحاسوبي، فضلاً عن وجهات نظرهم ومعتقداتهم السياسية والدينية، وبالتالي التدخل في حرية الرأي وحرية الفكر[14]. ويمكن أن تخلّف عمليات الاختراق الحاسوبي تجارب مؤلمة للغاية، مما يؤثر في الصحة العقلية للضحايا وأسرهم. وتفيد التقارير بأن الاختراق الحاسوبي أدى إلى اعتقال واحتجاز المدافعين عن حقوق الإنسان والسياسيين، الذين يزعم أن بعضهم تعرض للتعذيب[15]. وثمة روابط أيضاً بين الاختراق الحاسوبي لأشخاص مستهدفين وبين عمليات القتل خارج نطاق القضاء[16].

10- وعلاوة على ذلك، فإن استهداف الصحفيين ووسائل الإعلام بأدوات الاختراق الحاسوبي يقوض بشدة حرية الإعلام لأسباب ليس أقلها أن مصادر المعلومات قد تخشى كشفها وما يترتب على ذلك. ومجرد وجود برامج اختراق حاسوبي يمكن أن يكون له آثار مخيفة على حرية التعبير وعمل وسائل الإعلام والنقاش العام والمشاركة في الحياة العامة، مما قد يؤدي إلى تقويض الحكم الديمقراطي. وعلى حد

(12) تجدر الإشارة إلى أن برنامج بيغاسوس ليس الأداة الوحيدة التي تتمتع بهذه القدرات كما أن عدد هذه الأدوات آخذ في الازدياد.

(13) جمع التحقيق الذي أجرته شركة EncroChat بالتعاون بين الشرطة في فرنسا وهولندا، حيث تمكنت من اقتحام البنية التحتية لخوادم شبكة اتصالات مشفرة، معلومات عن أكثر من 000 32 هاتف في 121 بلداً؛ انظر German Federal Court of Justice, decision of 2 March 2022, 5 StR 457/21, para. 18.

(14) A/HRC/29/32، الفقرة 20. وللاطلاع على تحليل شامل لحرية الفكر، انظر A/76/380.

(15) انظر https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/.

(16) A/HRC/41/35، الفقرة 1؛ انظر أيضاً ورقة غرفة الاجتماعات التي أعدها المقرر الخاص المعني بحالات الإعدام خارج نطاق القضاء أو بإجراءات موجزة أو تعسفاً، المعنونة “Annex to the report of the Special Rapporteur: investigation into the unlawful death of Mr. Jamal Khashoggi” على الرابط التالي: https://www.timesofisrael.com/nso-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

تعبير المحكمة العليا في الهند في حكمها الأخير بشأن استخدام برنامج بيغاسوس، فإن التأثير المرعب للمراقبة سيكون "اعتداء على الدور الرقابي العام الحيوي للصحافة"[17].

11- وقد يكون للاختراق الحاسوبي أيضاً تأثير سلبي على الحق في الإجراءات القانونية الواجبة والمحاكمة العادلة[18]. ولا يسمح الوصول إلى جهاز ما بتمكين المتسلل من مراقبة محتويات هذا الجهاز وتفاعلاته مع الأجهزة الأخرى فحسب بل يمكّن أيضاً من التلاعب بالجهاز، بما في ذلك عن طريق تغيير الملفات أو حذفها أو إضافتها[19]. وبالتالي يمكن تزوير الأدلة من أجل تجريم الأفراد المستهدفين أو ابتزازهم[20].

12- وعلاوة على ذلك، قد لا تؤثر برامج التجسس على أهداف عمليات الاختراق الحاسوبي فحسب، بل على كل شخص على اتصال مع هؤلاء الأفراد، أو، إذا تم تنشيط كاميرا الجهاز أو الميكروفون أو الموقع الجغرافي، أي شخص موجود في نفس الموقع الجغرافي[21].

13- وأخيراً، يعتمد الاختراق الحاسوبي على وجود ثغرات أمنية في نظم الكمبيوتر لكي يستغلها. فمن خلال إبقاء نقاط الضعف هذه مفتوحة، أو حتى بسبب خلقها، قد يساهم أولئك الذين يلجؤون إلى الاختراق الحاسوبي في تهديدات الأمن والخصوصية لملايين المستخدمين والنظام البيئي للمعلومات الرقمية في عمومها[22].

14- وقد دقت منذ سنوات هيئات حقوق الإنسان والخبراء ناقوس الخطر بشأن برامج التجسس. وذكرت الجمعية العامة وذكر مجلس حقوق الإنسان مراراً وتكراراً أنه ينبغي للدول الأعضاء أن تمتنع عن المراقبة غير القانونية أو التعسفية، بما في ذلك عن طريق الاختراق الحاسوبي[23]. وأعرب العديد من المقررين الخاصين عن انتقادهم الشديد لممارسات الاختراق الحاسوبي التي تتجاوز بكثير ما هو ضروري لتحقيق أهداف مشروعة، مثل مكافحة الإرهاب والجريمة[24]. وأعربت اللجنة المعنية بحقوق الإنسان أيضاً عن قلقها إزاء عمليات الاختراق الحاسوبي التي ترعاها الدولة، ولا سيما عندما تستخدم دون إشراف أو ضمانات كافية[25]. وعلى الصعيد الإقليمي، أدان المقرر الخاص السابق المعني بحرية التعبير التابع للجنة البلدان الأمريكية لحقوق الإنسان عمليات الاختراق الحاسوبي لأغراض غير مسموح بها ودعا إلى فرض عقوبات قاسية على الجناة، بما يشمل أيضاً الإجراءات المتخذة لأسباب سياسية ضد الصحفيين ووسائط الإعلام المستقلة[26].

15- ورداً على ما كشف عنه من معلومات عن استخدام برنامج بيغاسوس، أعربت مؤسسات إقليمية ووطنية مختلفة، بما فيها مجلس أوروبا، ولجنة البلدان الأمريكية لحقوق الإنسان، والبرلمان الأوروبي،

(17) Supreme Court of India, *Manohar Lal Sharma v. Union of India*, order of 27 October 2021, para. 39.

(18) A/HRC/23/40، الفقرة 62.

(19) A/HRC/39/29، الفقرة 19.

(20) انظر https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/ للحصول على مثال على هذه الادعاءات.

(21) انظر https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

(22) A/HRC/39/29، الفقرة 19.

(23) قرار الجمعية العامة 176/75 وقرارا مجلس حقوق الإنسان 4/48 و18/45.

(24) A/HRC/17/27؛ A/HRC/20/17؛ A/HRC/23/40، الفقرة 62؛ A/HRC/41/35؛ A/HRC/41/41؛ وA/73/438؛ انظر أيضاً https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

(25) انظر CCPR/C/DEU/CO/7؛ CCPR/C/NLD/CO/5؛ وCCPR/C/ITA/CO/6.

(26) انظر https://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&lID=1.

والمحكمة العليا في الهند، عن قلقها إزاء انتشار برامج التجسس وشرعت في عقد جلسات استماع وتحقيقات[27]. وتجري حالياً أيضاً تحقيقات[28] جنائية ودعاوى مدنية[29].

16- ويمكن للإرشادات المتعلقة بالحد الأدنى من المتطلبات والضمانات اللازمة لأي استخدام حكومي لبرامج التجسس أن تستند إلى مجموعة واسعة من التحليلات القائمة لحقوق الإنسان المتعلقة بالمراقبة[30]. وتستدعي الآثار السلبية البعيدة المدى المترتبة على الاختراق الحاسوبي اتباع نهج بالغ الحذر إزاء استخدامه، والاقتصار فيه على أكثر الظروف استثنائية، مع التقيد الصارم بما يقتضيه القانون الدولي لحقوق الإنسان.

17- ومع ذلك، فإن العديد من الولايات القضائية لم تضع مثل هذه الضمانات القانونية الأساسية وليست لديها قوانين واضحة ودقيقة ومتاحة للجمهور تحكم عمليات الاختراق الحاسوبي. ومع أن بعض الدول قد اشترعت أطراً قانونية من شأنها أن تمتثل للقانون الدولي لحقوق الإنسان، فإن دولاً أخرى تعتمد على قوانين مفرطة الاتساع أو عفا عليها الزمن حيث سُنت قبل ظهور التكنولوجيات الحديثة.

18- وكما أظهرت المعلومات المكتشفة المتعلقة ببرنامج بيغاسوس والتقارير ذات الصلة، فإن عمليات الاختراق الحاسوبي التي تقوم بها مختلف الجهات الفاعلة الحكومية كثيراً ما تسعى، فيما يبدو، إلى تحقيق أهداف غير مشروعة بموجب القانون الدولي لحقوق الإنسان. ومع أن تدابير المراقبة الاقتحامية قد تكون مسموحا بها، في ظروف معينة، بموجب المادتين 17 و19 من العهد الدولي الخاص بالحقوق المدنية والسياسية على أساس حماية الأمن القومي أو النظام العام، فإن عمليات الاختراق الحاسوبي لا يمكن أبداً تبريرها لأسباب سياسية أو تجارية، وهو ما يحدث في كثير من الأحيان عندما يستهدف المدافعون عن حقوق الإنسان أو الصحفيون.

19- وحتى لو كان السعي إلى تحقيق أهداف مشروعة، مثل أهداف الأمن القومي أو حماية حقوق الآخرين، فإن تقييم مدى ضرورة وتناسب استخدام برامج التجسس يحد بشدة من السيناريوهات التي يجوز فيها استخدام برامج التجسس[31]. وهناك حجج قوية مفادها أن أدوات مثل بيغاسوس، التي تمكّن من

(27) انظر https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1207&lID=1; https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/media_center/PReleases/2022/022.asp; https://www.theguardian.com/world/2022/mar/17/pegasus-spyware-ban-el-salvador-iachr-hearing; https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; https://tvn24.pl/tvn24-news-in-english/polands-senate-lunches-special-committee-to-examine-use-of-pegasus-software-5557023; and Supreme Court of India, *Manohar Lal Sharma v. Union of India*, order of 27 October 2021.

(28) انظر https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali; and https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.

(29) https://www.glanlaw.org/nso-spyware-hacking; https://privacyinternational.org/examples/2605/lawsuits-target-nso-group-selling-spyware-governments-targeting-activists-and; https://www.washingtonpost.com/technology/2021/11/23/apple-pegasus-lawsuit-spyware-nso/; and https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf. للحصول على نظرة عامة شاملة على الإجراءات القانونية المتخذة، انظر https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

(30) انظر A/HRC/27/37؛ A/HRC/39/29؛ A/HRC/23/40 وA/HRC/23/40/Corr.1؛ CCPR/C/UKR/CO/8؛ CCPR/C/DEU/CO/7؛ CCPR/C/ARM/CO/3؛ CCPR/C/BWA/CO/2؛ وCCPR/C/FIN/CO/7.

(31) انظر Federal Constitutional Court of Germany, judgment of 27 February 2008 (1 BvR 370, 595/07), at 247 (aa).

التدخل دون قيد أو شـــرط في حياة الناس ويمكن أن تصـــل حتى إلى دوائر تفكيرهم، يمكن أن تؤثر في جوهر الحق في الخصـــوصـــية[32] وتمسّ بالحقوق المطلقة في حرية الفكر والرأي. وبالنظر إلى الآثار السلبية الكبيرة لاستخدام برامج التجسس ومدى وصولها إلى ما هو أبعد من أي هدف مقصود، ينبغي أن يقتصـــر اســـتخدامها على الحالات التي يمكن أن تعمل فيها على منع جريمة أو فعل خطير محدد أو التحقيق فيه حيثما كان يرقى إلى مستوى التهديد الجسيم للأمن القومي. وينبغي أن يُحصر استخدامها في التحقيق مع الشخص أو الأشخاص المشتبه في ارتكابهم لهذه الأفعال. وينبغي أن يكون ذلك ملاذاً أخيراً، وبعبارة أخرى، ينبغي أن تكون جميع التدابير الأقل تدخلا قد اســـتنفدت أو ثبُت أنها غير مجدية، وينبغي أن يكون الاستخدام محدود النطاق والمدة على نحو صارم. وينبغي أن يقتصر الأمر كله على الوصول إلى البيانات ذات الصلة فقط وجمعها[33]. وينبغي أيضاً أن تخضع هذه التدابير لرقابة مستقلة صارمة؛ ومن الضروري الحصول على موافقة مسبقة من هيئة قضائية[34]. وبالإضافة إلى ذلك، فإن الضوابط القوية والشفافة المفروضة على التصدير، التي تأخذ في الحسبان بصورة صريحة مخاطر حقوق الإنسان، قد تكون أداة قوية لمنع انتهاكات الحقوق وتجاوزاتها[35]. وتكرر المفوضية السامية لحقوق الإنسان دعوتها الأخيرة وكذلك دعوة خبراء وجماعات حقوق الإنســـان إلى وقف اختياري لبيع أدوات الاختراق الحاســـوبي ونقلها واستخدامها إلى أن يتم وضع نظام ضمانات قائم على حقوق الإنسان[36].

باء- القيود المفروضة على التشفير

20- في السنوات الأخيرة، اتخذت حكومات مختلفة إجراءات تخاطر، عن قصد أو عن غير قصد، بتقويض أمن وسرية الاتصالات المشفرة. ويترتب على ذلك آثار مقلقة على التمتع بالحق في الخصوصية وغيره من حقوق الإنسان.

21- والتشفير هو عامل تمكين رئيسي للخصوصية والأمن عبر الإنترنت وهو ضروري لحماية الحقوق، بما في ذلك الحق في حرية الرأي والتعبير، وحرية تكوين الجمعيات والتجمع الســـلمي، والأمن والصحة وعدم التمييز. ويضمن التشفير تمكن الأشخاص من تقاسم المعلومات بحرية، دون خوف من أن تصبح معلوماتهم معروفة للآخرين، سواء كانوا سلطات الدولة أو مجرمي الإنترنت. والتشفير ضروري إذا كان للناس أن يشعروا بالأمان في تبادل المعلومات بحرية مع الآخرين حول مجموعة من الخبرات والأفكار والهويات، بما في ذلك المعلومات الصـحية أو المالية الحسـاسـة، المعارف المتعلقة بالهويات الجنسـانية والتوجه الجنسـي، والتعبير الفني والمعلومات المتعلقة بوضـع الأقلية. وفي بيئات الرقابة السـائدة، يمكّن التشفير الأفراد من الحفاظ على مساحة للاحتفاظ بالآراء والتعبير عنها وتبادلها مع الآخرين. وفي حالات محددة، لا يمكن للصحفيين والمدافعين عن حقوق الإنسان القيام بعملهم دون حماية تشفير قوي، وحماية

(32) European Data Protection Supervisor, see https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

(33) انظر https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf.

(34) انظر A/HRC/39/29 بشأن الضمانات الدنيا لتدابير المراقبة السرية.

(35) A/HRC/39/29، الفقرة 25؛ A/HRC/44/24، الفقرة 40؛ A/HRC/48/31، الفقرة 46؛ وA/HRC/41/35، الفقرتان 34 و66. وقد اتخذ الاتحاد الأوروبي مؤخرا خطوة نحو اعتبارات أقوى لحقوق الإنسان باعتماد لائحة جديدة لمراقبة الصادرات.

(36) انظر https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; https://www.amnesty.org/en/documents/doc10/4516/2021/en/; and https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/.

مصـــادرهم وحمايتها من الجهات الفاعلة القوية أثناء التحقيق. ويوفر التشـــفير للنســـاء، اللواتي يواجهن تهديدات خاصـــة بالمراقبة والتحرش والعنف عبر الإنترنت، مســـتوى مهما من الحماية من الكشـــف غير الطوعي عن المعلومات[37]. وفي النزاعات المسلحة، لا غنى عن الرسائل المشفرة لضمان الاتصال الآمن بين المدنيين. ومن الجدير بالذكر أنه في الشـــهرين التاليين لبدء النزاع المســـلح في أوكرانيا في 24 شباط/فبراير 2022، ارتفع عدد التنزيلات في أوكرانيا لتطبيق المراسلة المشفرة سيجنال بأكثر من 1 000 في المائة مقارنة بالأشهر السابقة[38].

22- واعتُرف على نطاق واسع بالدور الحيوي للتشفير كعامل تمكين للخصوصية وحقوق الإنسان، بما في ذلك من قبل الدول وهيئات الأمم المتحدة ومفوض الأمم المتحدة الســامي لحقوق الإنســان وخبراء حقوق الإنسان[39]. وأبرزت الجمعية العامة ومجلس حقوق الإنسان أهمية التشفير في صون حقوق الإنسان في عدة قرارات، ودعيا الدول إلى الامتناع عن التدخل في تكنولوجيات التشـفير[40]، وشـجعا مؤسـسـات الأعمال على العمل من أجل إيجاد حلول تمكينية لتأمين وحماية سـرية الاتصـالات والمعاملات الرقمية، بما في ذلك تدابير التشـــفير، وإخفاء الهوية وحجب الهوية[41] وأعرب المقررون الخاصـــون والخبراء الإقليميون عن تأييدهم للتشفير القوي بوصفه عاملاً تمكينياً للحقوق، وأوصوا بتعزيز وحماية التشفير القوي وحذروا من التدابير التي من شـأنها أن تقيد اسـتخدام هذه التكنولوجيا الرئيسـية بصـورة تعسـفية أو غير قانونية[42]. وشددت لجنة حقوق الطفل على أن أي تدابير للكشف عن مواد الاستغلال والاعتداء الجنسيين للأطفال في الاتصـــالات المشـــفرة يجب أن تكون محدودة للغاية وفقا لمبادئ الشـــرعية والضـــرورة والتناسب[43]. وأكد مجلس حقوق الإنسان والأمم المتحدة وخبراء حقوق الإنسان الإقليميون أن التشفير أمر حيوي للعمل الصـحفي وحماية المصـادر[44]. وتؤكد مؤشـرات عالمية الإنترنت الصـادرة عن منظمة الأمم المتحدة للتربية والعلم والثقافة على أهمية التشفير من أجل الثقة والأمن على الإنترنت[45].

23- وبالرغم من فوائد التشـفير، تقيد الحكومات أحياناً اسـتخدام التشـفير، مثلا لحماية الأمن القومي ومكافحة الجريمة، ولا ســيما للكشــف عن مواد الاعتداء الجنســي على الأطفال. وتشــمل القيود حظر الاتصـالات المشـفرة وتجريم عرض أو اسـتخدام أدوات التشـفير[46] أو التسـجيل الإلزامي وترخيص أدوات

(37) A/HRC/35/9، الفقرة 18.

(38) انظر https://sensortower.com/blog/signal-telegram-ukraine-russia-2022.

(39) انـظـر https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid.

(40) قرار الجمعية العامة 176/75، وقرارات مجلس حقوق الإنسان 6/39 و12/44 و18/45 و4/48.

(41) قرار الجمعية العامة 176/75 وقرار مجلس حقوق الإنسان 48/4.

(42) انـظـر A/HRC/29/32; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf; A/HRC/41/41; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf; https://www.osce.org/representative-on-freedom-of-media/379351; and https://www.oas.org/en/iachr/expression/reports/ENGIA2020.pdf.

(43) لجنة حقوق الطفل، التعليق العام رقم 25(2021) بشأن حقوق الطفل فيما يتعلق بالبيئة الرقمية، الفقرة 70.

(44) قـرار مـجـلـس حـقـوق الإنســـان 18/45؛ and https://www.osce.org/representative-on-freedom-of-media/379351.

(45) انظر indicator D.5, https://en.unesco.org/internet-universality-indicators .

(46) انظر PSE 2/2017 و LBY 3/2022. All communications mentioned in the present report are available from https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

التشفير[47] وبالمثل، في بعض الحالات، طلب من مقدمي خدمات التشفير ضمان وصول وكالات إنفاذ القانون أو الوكالات الحكومية الأخرى إلى جميع الاتصالات عند الطلب، الأمر الذي يمكن أن يرقى فعليا إلى حد تقييد شامل للتشفير يمكن أن يتطلب، أو على الأقل يشجع، إنشاء مسار شبيه بالدخول من الباب الخلفي (مسار مدمج لتجاوز التشفير، يسمح بالوصول السري إلى البيانات في صيغة النص العادي)[48]. وثمة شكل آخر من أشكال التدخل في التشفير يتمثل في اشتراط إنشاء نظم الضمان الرئيسية وصيانتها، وتسليم جميع المفاتيح الخاصة اللازمة لفك تشفير البيانات إلى الحكومة أو إلى طرف ثالث معين[49]. وفرض متطلبات التتبع، التي يحتاج مقدمو الخدمات بموجبها إلى أن يكونوا قادرين على تتبع أي رسالة إلى منشئها المفترض، يمكن أن يتطلب أيضاً إضعاف معايير التشفير[50]. وفي الآونة الأخيرة، بدأت دول مختلفة في فرض التزامات رصد عامة لمقدمي خدمات الاتصالات الرقمية، بمن فيهم مقدمو خدمات الاتصالات المشفرة أو النظر في فرضها[51]. ويمكن لهذه الاشتراطات أن تجبر هؤلاء المزودين فعليا على التخلي عن التشفير القوي من طرف إلى طرف أو تحديد حلول بديلة تنطوي على إشكاليات كبيرة (انظر الفقرتين 27-28 أدناه).

24- وما من شك في أن قدرات التشفير المستخدمة على نطاق واسع، وهي القدرات التي طالب بها الجمهور كرد فعل على المراقبة الجماعية والجرائم السيبرانية، تخلق معضلة للحكومات التي تسعى إلى حماية السكان، ولا سيما أضعف أفرادها، من الجرائم الخطيرة والتهديدات الأمنية. ومع ذلك، وكما أشار المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، فإن تنظيم التشفير يهدد بتقويض حقوق الإنسان[52]. وكثيراً ما أخفقت الحكومات التي تسعى إلى الحد من التشفير في إظهار أن القيود التي ستفرضها ضرورية لتلبية مصلحة مشروعة معينة، نظراً لتوافر مختلف الأدوات والنهج الأخرى التي توفر المعلومات اللازمة لإنفاذ القانون المحدد أو لأغراض مشروعة أخرى[53]. وتشمل هذه التدابير البديلة تحسين أعمال الشرطة التقليدية وتحسين مواردها، والعمليات السرية، وتحليل البيانات الفوقية، وتعزيز التعاون الدولي في مجال الشرطة.

25- وعلاوة على ذلك، فإن تأثير معظم قيود التشفير على الحق في الخصوصية والحقوق المرتبطة بها غير متناسب، وغالباً ما لا يؤثر على الأفراد المستهدفين فحسب، بل على عامة السكان. ولا يمكن تبرير الحظر الصريح من جانب الحكومات، أو تجريم التشفير على وجه الخصوص، لأنها ستمنع جميع المستعملين داخل ولاياتها القضائية من الحصول على طريقة آمنة للتواصل. وتحتوي نظم الضمان الرئيسية على نقاط ضعف كبيرة، لأنها تعتمد على سلامة مرفق التخزين وتعرض المفاتيح المخزنة

(47) انظر https://hrsly.com/wp-content/uploads/2022/06/OL-LBY-3.2022-DownLoadPublicCommunicationFile.pdf (LBY 3/2022).

(48) انظر GBR 4/2015 وMYS 2/2018 وAUS 5/2018 وAUS 6/2018.

(49) انظر RUS 7/2016 and RUS 7/2018.

(50) انظر IND 31/2018 وIND 3/2019 وBRA 6/2020 وBRA 7/2020.

(51) على سبيل المثال، the "EARN IT" Act adopted in the United States of America in 2020 (see USA 4/2020); the draft Online Safety Bill in the United Kingdom (see GBR 5/2022); the European Commission proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 11 May 2022 (COM(2022) 209); and Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (see IND 8/2021).

(52) انظر A/HRC/29/32.

(53) المرجع نفسه، الفقرة 39.

للهجمات الإلكترونية. وعلاوة على ذلك، فإن مسارات الدخول من الأبواب الخلفية الإلزامية في أدوات التشفير تخلق التزامات تتجاوز بكثير فائدتها فيما يتعلق بمستخدمين محددين تم تعيينهم على أنهم مشتبه بهم في ارتكاب جرائم أو تهديدات أمنية. فهي تعرض للخطر خصوصية وأمن جميع المستعملين وتعرضهم للتدخل غير المشروع، ليس من جانب الدول فحسب، بل أيضاً من جانب الجهات الفاعلة من غير الدول، بما في ذلك الشبكات الإجرامية[54]. ومتطلبات الترخيص والتسجيل لها آثار غير متناسبة مماثلة لأنها تتطلب أن تحتوي برامج التشفير على نقاط ضعف قابلة للاستغلال[55]. ولا تقتصر هذه الآثار الضارة بالضرورة على الولاية القضائية التي تفرض التقييد؛ بل من المرجح أن تصبح مسارات الدخول من الأبواب الخلفية، بمجرد إنشائها في الولاية القضائية لدولة ما، جزءا من البرامجيات المستخدمة في أجزاء أخرى من العالم.

26- وفي الآونة الأخيرة، تم اقتراح مفهوم ما يسمى بالمسح من جانب العميل للكشف عن أشكال معينة من المحتوى المرفوض لتجنب العديد من المشاكل الموضحة أعلاه. وينقل المسح من جانب العميل خطوة اكتشاف المحتوى من الخوادم التي يتم من خلالها إرسال الاتصالات إلى الأجهزة الشخصية نفسها. وبهذه الطريقة، يتم فحص المحتوى المعني قبل تشفيره تمهيداً لنقله. وفي آب/أغسطس 2021، أعلنت شركة آبل عن خطط لتقديم مثل هذا النظام لخدمات iMessage وiCloud الخاصة بها، لكنها علقت تنفيذ التغيير المقترح بعد انتقادات قوية من مجموعة واسعة من خبراء أمن تكنولوجيا المعلومات وخبراء التشفير وجماعات حقوق الإنسان[56]. بيد أن مختلف المحاولات التشريعية قد تجبر خدمات الاتصالات عبر الإنترنت بصورة غير مباشرة على الأقل على تنفيذ هذه النظم بفرض التزامات رصد واسعة النطاق لجميع الاتصالات، بما فيها تلك المشفرة[57]. وبما أن محتوى الرسائل، بمجرد تشفيره، لا يمكن لأي شخص الوصول إليه باستثناء المرسل والمستلم، فإن أي التزام عام بالمراقبة من شأنه أن يجبر مقدمي الخدمات إما على التخلي عن تشفير النقل أو السعي إلى الوصول إلى الرسائل قبل تشفيرها.

27- ومن شأن فرض مسح عام من جانب العميل أن يشكل نقلة نوعية تثير مجموعة من المشاكل الخطيرة ذات العواقب الوخيمة المحتملة على التمتع بالحق في الخصوصية وغيرها من الحقوق. وعلى عكس التدخلات الأخرى، فإن فرض المسح العام من جانب العميل سيؤثر حتما على كل من يستخدم وسائل الاتصال الحديثة، وليس فقط الأشخاص المتورطين في الجريمة والتهديدات الأمنية الخطيرة. ويغير المسح من جانب العميل قدرة الأشخاص على التحكم الكامل في أجهزة الاتصال المرتبطة ارتباطا جوهريا بجميع جوانب حياتهم والحد من المعلومات التي تشاركها هذه الأجهزة[58]. وعلاوة على ذلك، لا يمكن تجنب المطابقات الكاذبة المتكررة، في المسح العام للاتصالات، حتى لو كانت معدلات الدقة مرتفعة، مما يورط العديد من الأفراد الأبرياء[59]. وبالنظر إلى إمكانية حدوث مثل هذه الآثار، فمن المرجح أن يكون

(54) A/HRC/39/29، الفقرة 20.

(55) A/HRC/29/32، الفقرة 41.

(56) انظر https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf.

(57) المفوضية الأوروبية، اقتراح لتنظيم البرلمان الأوروبي والمجلس يضع قواعد لمنع ومكافحة الاعتداء الجنسي على الأطفال، 11 أيار/مايو 2022 (COM (2022) 209)؛ انظر أيضاً draft Online Safety Bill in the United Kingdom of Great Britain and Northern Ireland, available at https://www.gov.uk/government/publications/draft-online-safety-bill.

(58) Submissions by the Global Encryption Coalition Steering Committee and Privacy International.

(59) انظر https://doi.org/10.48550/arXiv.2110.07450.

للمراقبة العشـــوائية تأثير مخيف كبير على حرية التعبير وتكوين الجمعيات، حيث يحد الناس من طرق تواصلهم وتفاعلهم مع الآخرين وينخرطون في الرقابة الذاتية[60].

28- ويفتح المسـح من جانب العميل أيضـاً تحديات أمنية جديدة، مما يجعل الخروقات الأمنية أكثر احتمالا[61]. ويمكن أيضـاً التلاعب بعملية الفحص، مما يجعل من الممكن إنشـاء ملفات تعريف مطابقة كاذبة أو سـلبية كاذبة بشـكل مصـطنع[62]. وحتى إذا كان المسـح من جانب العميل، للأغراض الراهنة، مصـمما بشـكل مُضـيّق، فمن المرجح أن يؤدي فتح أجهزة للفحص الذي تأذن به الحكومة إلى محاولات مستقبلية لتوسيع نطاق المحتوى المستهدف بهذه التدابير[63]. وعلى وجه الخصـوص، عندما تكون سيادة القانون ضـعيفة وحقوق الإنسان مهددة، يمكن أن يكون تأثير المسح من جانب العميل أوسع بكثير، على سـبيل المثال يمكن اسـتخدامه لقمع النقاش السـياسـي أو لاسـتهداف شـخصـيات المعارضـة والصـحفيين والمدافعين عن حقوق الإنسـان[64]. وبالنظر إلى النطاق الواسـع للمخاطر الكبيرة التي تهدد حماية حقوق الإنسـان من جراء المسـح العام المكلف به من جانب العميل، ينبغي عدم فرض هذه المتطلبات دون مزيد من النظر الجوهري في آثارها المحتملة على حقوق الإنسان والتدابير التي تخفف من تلك الأضرار. وبدون إجراء تحقيق وتحليل متعمقين، يبدو من غير المرجح أن تعتبر هذه القيود متناسـبة بموجب القانون الدولي لحقوق الإنسان، حتى عندما تفرض سعياً لتحقيق أهداف مشروعة، نظراً لخطورة عواقبها المحتملة[65].

ثالثاً- مراقبة الجمهور

29- أعربت المفوضـة السامية عن قلقها إزاء المراقبة الجماعية في عدة مناسبات، ولا سيما من حيث اعتراض الاتصـــالات جملةً واحدة[66]. ومع أن بعض الدول قد حســنت الضــمانات ضــد المراقبة، فإن الممارســة المقلقة للغاية المتمثلة في مراقبة الأنشــطة الإلكترونية لنســب كبيرة من الســكان، أو حتى لمجموعات سكانية بأكملها، لم تتوقف. وبينما ركزت التقارير السابقة في معظمها على مراقبة الاتصـالات الخاصـــة، فإنها لم تتطرق إلا لماماً إلى الآثار المترتبة على الخصـــوصـــية فيما يتعلق بمراقبة الأماكن العامة، والتي نناقشها أدناه.

(60) وللاطلاع على مزيد من المعلومات عن الآثار المرعبة للمراقبة، انظر الفقرة 47 أدناه.

(61) بالمقارنة مع الهجمات على خوادم الشـركات، يمكن تنفيذ الهجمات على الأجهزة الشـخصـية من قبل المزيد من الجهات الفاعلة وعلى البنية التحتية الأقل أماناً. يمكن للخصوم استخدام وصولهم إلى الجهاز لإجراء هندسة عكسية لآلية المسح الضوئي، انظر https://doi.org/10.48550/arXiv.2110.07450 2110,07450.

(62) https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; and https://openrevi ew.net/forum?id=CQbqeGAM_Ki.

(63) https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/; https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; and https://doi.org/10.48550/arXiv.2110.07450.

(64) المرجع نفسه.

(65) A/HRC/39/29، الفقرة 20، وA/HRC/29/32، الفقرة 43. وتؤيد آراء محكمة العدل التابعة للاتحاد الأوروبي هذا الاستنتاج. وقضـت المحكمة مؤخراً بأن التحليل الآلي لبيانات حركة المرور والموقع بطريقة عامة وعشـوائية يجب أن يقتصـر على ما هو ضـروري للغاية للرد على تهديد خطير أو حقيقي أو حالي أو متوقع للأمن القومي. ورفضـت المحكمة أي مبرر آخر. انظر La Quadrature du Net and Others v. Premier ministre and Others, judgment of 6 October 2020 (joined cases C-511/18, C-512/18 and C-520/18), para. 177. وعلاوة على ذلك، تشـير السـوابق القضـائية إلى شـكوك أقوى تجاه فحص بيانات المحتوى، محكمة العدل التابعة للاتحاد الأوروبي، Maximillan Schrems v. Data Protection Commissioner, judgment of 6 October 2015 (C-362/14), para. 94.

(66) انظر A/HRC/27/37; A/HRC/39/29; and https://www.ohchr.org/en/press-releases/2013/07/mass-surveillance-pillay-urges-respect-right-privacy-and-protection.

ألف- مراقبة الأماكن العامة

30- أصبحت كاميرات المراقبة، التي يتم نشرها لمراقبة الشوارع العامة ومواقف السيارات ومراكز النقل وغيرها من الأماكن العامة، شائعة في العديد من البلدان. ومن المتوقع أن يتجاوز عدد كاميرات المراقبة المستخدمة عالميا مليار كاميرا في عام 2021[67]. وتشغّل 10 مدن في العالم كثافة من حيث استخدام المراقبة بالفيديو بين حوالي 39 إلى أكثر من 115 كاميرا مراقبة لكل 000 1 نسمة[68].

31- وبالإضافة إلى نظم المراقبة التي تديرها الدولة، لدى بعض الشركات أدوات مراقبة متكاملة للاستخدام الخاص، مع ميزات مخصصة للإبلاغ عن الحوادث إلى السلطات أو حتى منحها إمكانية الوصول المباشر إلى تدفقات البيانات الخاصة بها[69]. وهذا يوسع إلى حد كبير الفضاء العام الخاضع للمراقبة، بينما يقوض الشفافية والرقابة والمساءلة.

32- وفي السنوات الأخيرة، زادت قدرات كاميرات المراقبة بشكل كبير نتيجة لإضافة قدرات متطورة لتحليل الفيديو. وتشير التقديرات إلى أن أقل من 2 في المائة من كاميرات الشبكة المبيعة في عام 2010 تتمتع بخصائص تحليلات فيديو مضمنة، ولكن هذه النسبة زادت إلى أكثر من 40 في المائة بحلول عام 2016 ومن المرجح أن تستمر في الزيادة [70]. وتعتمد ميزات التحليلات بشكل متزايد على الذكاء الاصطناعي. وتعد القدرات الإضافية لتنفيذ التعرف على الوجه وتحديد السلوك المشبوه من بين أكثر الخصائص المميزة إشكالية بالنسبة لنظم المراقبة بالفيديو المتطورة[71]. وبالإضافة إلى ذلك، تم تطبيع استخدام الطائرات بدون طيار لأغراض المراقبة في العديد من البلدان، حيث يتم استخدامها لمراقبة الاحتجاجات وغيرها من التجمعات[72].

33- وتحت مظلة مصطلح "المدن الذكية"، يجري حالياً عدد متزايد من المبادرات القائمة على البيانات لإعادة تشكيل المساحات الحضرية. وتركز مشاريع المدن الذكية على جمع البيانات ومعالجتها لإثراء إدارة مرافق المدينة، والتي يتم تمكينها من خلال تقنيات الاستشعار الأكثر قدرة من أي وقت مضى. ومع أن الكثير من البيانات التي يتم جمعها ومعالجتها في هذه السياقات تتعلق بقضايا مثل البيانات المتعلقة بتدفقات حركة المرور أو التلوث أو الضوضاء بصرف النظر عن مجال البيانات الشخصية، يمكن ربط البيانات الأخرى التي يتم جمعها بسهولة بالأفراد، مثل لوحات ترقيم السيارات وبيانات العدادات الذكية لأماكن توقف السيارات. وعلاوة على ذلك، يمكن في كثير من الأحيان إلغاء إخفاء هوية البيانات التي تبدو مجهولة المصدر[73]، ويمكن إعادة استخدام البنية التحتية، مثل الكاميرات المثبتة لمراقبة تدفقات بيانات حركة المرور، لتتبع حركة الأفراد[74].

(67) انظر https://venturebeat.com/2022/06/18/how-ml-powered-video-surveillance-could-improve-security/.

(68) انظر https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; https://surfshark.com/surveillance-cities.

(69) انظر https://www.accessnow.org/amazon-ring-privacy-review/.

(70) انظر https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf.

(71) انظر submissions by Derechos Digitales and the International Network of Civil Liberties Organizations.

(72) انظر submissions by Amnesty International and CIVICUS.

(73) انظر https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

(74) لمزيد من المعلومات عن آثار المدن الذكية على حقوق الإنسان، انظر https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/; and https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

34- وغالباً ما تحدث هذه التطورات على خلفية نظم الهوية الجديدة وقواعد البيانات البيومترية الموسعة. وفي طائفة من البلدان، ترتبط نظم الهوية بالتخزين المركزي المكثف للبيانات الشخصية، بما في ذلك المعلومات البيومترية مثل بصمات الأصابع وهندسة الوجه ومسح قزحية العين والحمض النووي. وعلاوة على ذلك، كثيراً ما تكون قواعد البيانات مترابطة ومتاحة للبحث من جانب الوكالات الأخرى. ونتيجة لذلك، أصبح تحديد هوية الأفراد أينما كانوا أسهل فأسهل.

باء- المراقبة عبر الإنترنت

35- في موازاة ذلك، أصبحت مراقبة الخطاب العام عبر الإنترنت واسعة الانتشار. وعلى الصعيد العالمي، تقوم العديد من السلطات بجمع وتحليل منشورات وسائل التواصل الاجتماعي والشبكات الخاصة والمهنية المبنية على منصات الاتصالات المتاحة للجمهور. وتتراوح معلومات وسائل التواصل الاجتماعي هذه من التحقيق في مستخدمين محددين إلى جمع كميات هائلة من البيانات وتخزينها وتحليلها. وقد تتضمن البيانات التي تم الحصول عليها: الأسماء؛ الأعمار؛ الصور والقوالب الرقمية ذات الصلة؛ العناوين; المشاركات وردود الفعل على مشاركات الآخرين؛ الاتصالات الاجتماعية والمهنية والشبكات المرتبطة بها؛ بيانات الموقع الجغرافي؛ الاهتمامات؛ الميل الجنسي؛ تحديد الهوية الجنسانية؛ الانتماء السياسي والأنشطة؛ المعتقدات الدينية; والمعلومات الصحية.

36- وفي كثير من الأحيان، تشكل أنواع مختلفة من التحليلات التنبؤية جزءا من ممارسات استخبارات وسائل التواصل الاجتماعي، بما في ذلك محاولات تحديد النقاط الساخنة المحتملة للجريمة. ومع ذلك، يمكن أيضاً استخدام هذه التحليلات لتقييم السلوك السابق والحاضر والمستقبلي للأفراد وتحديد درجات المخاطر المتعلقة باحتمال أن يصبحوا مجرمين أو يشكلوا تهديداً أمنياً[75]. ويستخدم ذكاء وسائل التواصل الاجتماعي أيضاً للتنبؤ باحتمال حدوث اضطرابات اجتماعية[76].

37- ويمكن لهذه الأنشطة أن تخدم أهدافا مشروعة وغير مشروعة متعددة، من التحقيق في الجرائم ومنعها إلى فحص المتقدمين للحصول على الاستحقاقات الاجتماعية، ورصد الاحتجاجات، وقياس المشاعر العامة، وتحديد ملامح السلوك الاجتماعي للناس[77].

جيم- الآثار المترتبة على حقوق الإنسان

38- تعمل التقنيات الحديثة القائمة على البيانات على تحويل ميزان القوى بشكل كبير بين الكيان الذي يقوم بالمراقبة والجهات التي تتم مراقبتها. وقبل ظهور أدوات المراقبة الآلية وتحليل البيانات على نطاق واسع، كانت هناك قيود عملية على المراقبة توفر مستوى معيناً من الحماية للأفراد، حتى عندما يكونون في الأماكن العامة[78]. والأدوات الرقمية المتطورة تجعل تلك الحماية "الطبيعية" السابقة موضع نقاش. واليوم، يمكن لضابط واحد مراقبة حسابات وسائل التواصل الاجتماعي لعشرات الأشخاص، وبمساعدة البرامج المتقدمة وتحليلات البيانات الضخمة، يمكن للفرق الصغيرة مراقبة آلاف الحسابات وتصنيفها[79].

39- وتعزز تطورات مماثلة فعالية تدابير المراقبة الأخرى في الأماكن العامة وتوسع نطاقها. فعلى سبيل المثال، أدى ظهور تكنولوجيا التعرف على الوجه إلى جانب تقنيات التعرف البيومترية الأخرى إلى

(75) انظر https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, p. 152.

(76) انظر https://dx.doi.org/10.2139/ssrn.2702426, p. 1.

(77) انظر https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

(78) A/HRC/44/24, para. 34.

(79) انظر https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

إحداث تحول جذري في الممارسات التقليدية للمراقبة السمعية البصرية، حيث زاد بشكل كبير من القدرة على تحديد هوية الأفراد في الأماكن العامة، بما في ذلك المشاركين في التجمعات. وتسمح تقنية التعرف المباشر على الوجه بتحديد هوية الأفراد بصورة آنية، بالإضافة إلى مراقبتهم وتتبعهم لأغراض محددة. ومن المحتمل أن يؤدي تحديد الأشخاص بأثر رجعي إلى زيادة نطاق مصادر البيانات، مما يؤدي إلى تأثيرات يمكن أن تكون تدخلية بنفس القدر[80] إذا لم يتم نشرها بأقصى قدر من ضبط النفس.

40- ويتفاقم تأثير المراقبة العامة على حقوق الإنسان بسبب تزايد دمج مصادر البيانات، على سبيل المثال من خلال الجمع بين خلاصات المراقبة بالفيديو المجهزة بتقنيات التعرف على الوجه مع بيانات وسائل التواصل الاجتماعي وقواعد البيانات الحكومية[81]، بما في ذلك المعلومات المتعلقة بالضمان الاجتماعي والهجرة والمشتبه في ارتكابهم أعمالا إرهابية والاعتقالات أو حتى قوائم الأفراد الذين تم الإبلاغ عنهم لأسباب سياسية.

41- وبالإضافة إلى ذلك، تعتمد الدول على مجموعات واسعة من البيانات التي تجمعها مجموعة متنوعة من الشركات الخاصة. وفي تقارير سابقة، سلطت المفوضة السامية والمقررون الخاصون الضوء على مسألة طلب الحكومات الوصول إلى البيانات التي يجمعها مقدمو خدمات الاتصالات السلكية واللاسلكية والإنترنت، وغالباً ما يكون ذلك على خلفية القوانين الإلزامية للاحتفاظ بالبيانات[82]. ويزداد عدد الشركات التي تتلقى مثل هذه الطلبات باطراد. وتجبر بعض الدول الشركات على تمكينها من الوصول المباشر إلى تدفقات البيانات التي تمر عبر شبكاتها. وتثير نظم الوصول المباشر هذه قلقا بالغا، لأنها معرضة بشكل خاص لإساءة الاستخدام وتميل إلى الالتفاف على الضمانات الإجرائية الرئيسية[83].

42- وعلاوة على ذلك، تعتمد الدول بشكل متزايد على خدمات المراقبة التي تقدمها مؤسسات الأعمال، مثلا عن طريق الحصول على البيانات من سماسرة البيانات وغيرهم من الشركات التي تجمع البيانات الشخصية وتبيعها[84]. ويمكن لهذه الممارسات أن تتحايل على القيود والضمانات الإجرائية الحاسمة، مما يسمح للدول بالوصول بصورة غير مباشرة إلى أدوات لم يكن بوسعها أن تستغلها بنفسها دون الإخلال بالتزاماتها في مجال حقوق الإنسان. على سبيل المثال، تم استخدام أداة التعرف على الوجه التي طورتها شركة Clearview AI من قبل الآلاف من وكالات إنفاذ القانون، على الرغم من حقيقة أنه تم بناؤها عن طريق كشط صور مليارات الأشخاص من الإنترنت، وهو تدخل هائل في حقوق الخصوصية[85].

---

(80) انظر submission by Amnesty International.

(81) انظر submission by the International Network of Civil Liberties Organizations.

(82) A/HRC/27/37، الفقرة 26؛ A/HRC/39/29، الفقرة 18؛ A/HRC/23/40 وA/HRC/23/40/Corr.1، الفقرات 65-67؛ وA/69/397، الفقرات 53-55.

(83) A/HRC/39/29، الفقرة 19.

(84) انظر على سبيل المثال https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances; and https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, p. 25.

(85) سلطات حماية البيانات المختلفة، التي قررت أن Clearview AI قد انتهكت قانون حماية البيانات، وفرضت غرامات باهظة و/أو أمرت بمحو البيانات الشخصية التي تم الحصول عليها، انظر https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; see also https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy; https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en; and https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. Data protection authorities have held that police forces, by using the tool, had violated data protection law, see https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en; and https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

43- وتشكل المراقبة المنهجية للأشخاص في الفضاء العام على شبكة الإنترنت وخارجها، ولا سيما عندما تقترن بطرق إضافية لتحليل المعلومات التي تم الحصول عليها وربطها بمصادر البيانات الأخرى، تدخلا في الحق في الخصوصية ويمكن أن تكون لها آثار ضارة للغاية على التمتع بحقوق الإنسان الأخرى[86]. وقد تشكل تهديداً لحرية التعبير والتجمع السلمي والمشاركة والديمقراطية، ولذلك ينبغي التعامل معها بأقصى قدر من الحذر وبالتقيد الصارم حصراً بمتطلبات حقوق الإنسان. وهذا هو الحال على الرغم من أن الأنشطة التي يتم رصدها تحدث في الأماكن العامة، أو على منصات التواصل الاجتماعي المفتوحة، حيث يجب أن يكون للأفراد مساحة خالية من المراقبة والاقتحام المنهجي، ولا سيما من قبل الكيانات الحكومية. وكما لاحظت المفوضة السامية من قبل، فإن حماية الحق في الخصوصية تتسع لتشمل الأماكن العامة والمعلومات المتاحة للجمهور[87]. وقد رفضت اللجنة المعنية بحقوق الإنسان الفكرة القائلة بأن البيانات التي تجمع في الأماكن العامة تكون تلقائيا في الملك العام ويمكن الوصول إليها بحرية[88]. وقد أقرت المحكمة الأوروبية لحقوق الإنسان بأن المعلومات المتاحة للجمهور أو التي يمكن أن يستشفّها قد تقع ضمن نطاق الحق في الخصوصية، ولا سيما عندما تسجل البيانات الشخصية بصورة منهجية أو دائمة[89].

44- ويتعلق أحد الشواغل الخاصة في مجال المراقبة العامة بتسجيل الصور الفوتوغرافية. وتجسد صور الأشخاص السمات الرئيسية لشخصيتهم وتكشف عن خصائص فريدة تميزهم عن غيرهم من الأشخاص. ويشكل تسجيل صور الوجه للأفراد وتحليلها والاحتفاظ بها دون موافقتهم تدخلا في حقهم في الخصوصية. ومن خلال نشر تكنولوجيا التعرف على الوجه في الأماكن العامة، وهو ما يتطلب جمع ومعالجة صور الوجه لجميع الأشخاص الذين تم التقاط صورهم بالكاميرا، يحدث هذا التدخل على نطاق واسع وعشوائي[90].

45- وعلاوة على ذلك، يمكن أن تؤدي تدابير المراقبة العامة إلى تدابير تؤثر تأثيراً مباشراً على الأفراد والمجتمعات، بما في ذلك التدابير القسرية، وغالباً ما تكون أساساً لها. وتشمل هذه التدابير زيادة الرصد وحفظ الأمن في بعض الأحياء أو الجماعات أو الأفراد، مما يؤدي أحياناً إلى استجواب الأفراد واعتقالهم واحتجازهم. ويمكن أيضاً تصنيف بعض الجماعات والأفراد على أنهم يشكلون تهديدات أو مخاطر محتملة، على سبيل المثال كإرهابيين أو مجرمين محتملين، وغالباً ما يكون ذلك دون أساس قوي في الواقع. وتستخدم عدة حكومات نتائج مجموعة متنوعة من تدابير المراقبة العامة لتحديد هوية منتقديها أو الأشخاص الذين لا يتفقون مع التوقعات الاجتماعية، مما قد يؤدي إلى المضايقة أو الاحتجاز أو الحرمان من الخدمات الأساسية[91].

(86) انظر CCPR/C/NGA/CO/2، الذي أعربت فيه اللجنة المعنية بحقوق الإنسان عن قلقها إزاء رصد وسائط التواصل الاجتماعي، الفقرة 40.

(87) A/HRC/39/29، الفقرة 6.

(88) CCPR/C/COL/CO/7، الفقرة 32.

(89) انظر European Court of Human Rights, *Rotaru v. Romania*, para. 43, judgment of 4 May 2000; *Peck v. the United Kingdom*, judgment of 28 January 2003, para. 59; *Perry v. the United Kingdom*, judgment of 17 July 2003, para. 38; and *Vukota-Bojić v. Switzerland*, judgment of 18 January 2017, para. 55.

(90) A/HRC/44/24، الفقرة 33.

(91) انظر https://privacyinternational.org/explainer/55/social-media-intelligence.

46- وتميل عمليات المراقبة إلى استهداف الأقليات والمجتمعات المهمشة بشكل غير متناسب[92]. وينطوي استخدام الذكاء الاصطناعي على خطر إدامة أنماط التمييز هذه[93]، بما في ذلك استخدام تكنولوجيات التعرف على الوجه في التنميط العرقي والإثني[94]. وقد تبين أن النظم التنبؤية المستخدمة في أعمال الشرطة ولأغراض إقامة العدل تؤثر بشكل غير متناسب في الأقليات[95].

47- وبالإضافة إلى ذلك، فإن المراقبة لها آثار مخيفة كبيرة على كيفية ممارسة الناس لحقوقهم، ولا سيما الحق في حرية التعبير والتجمع السلمي[96]. وتوضح دراسات مختلفة مدى هذه الآثار. وكشفت دراسة استقصائية أجريت عام 2015 أن 25 في المائة من المشاركين الذين كانوا على علم بحالة إدوارد سنودن قد غيروا استخدامهم لمنصات التكنولوجيا المختلفة[97]. ووجدت دراسة أخرى أن ما بين 34 في المائة و61 في المائة من الكتاب (حسب البلد المعني) تجنبوا أو على الأقل فكروا في تجنب مواضيع معينة في عملهم بسبب الخوف من المراقبة الحكومية[98]. وفي دراسة استقصائية أجراها المجلس النرويجي للتكنولوجيا، ذكر 39 في المائة من المجيبين أنهم سيتجنبون استخدام الكلمات والعبارات التي ترصدها الشرطة[99]. وكما أشارت المفوضة السامية من قبل، فإن هذه الآثار المرعبة تمتد إلى التجمعات، بما في ذلك الاحتجاجات السلمية[100].

(92) انظر CERD/C/CHN/CO/14-17; and https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media.

(93) انظر the conference room paper of the High Commissioner on the promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers, paras. 93 and 94. Available from https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session47/list-reports.

(94) A/HRC/41/35، الفقرة 12، and A/HRC/44/57، الفقرة 39.

(95) لجنة القضاء على التمييز العنصري، التوصية العامة رقم 36(2020) بشأن منع ومكافحة التنميط العنصري من جانب الموظفين المكلفين بإنفاذ القوانين، الفقرات 33-34؛ A/HRC/44/57، الفقرة 43؛ conference room paper of the High Commissioner on the promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers, para. 93; A/HRC/48/31، الفقرة 24؛ https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/; https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf; and https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

(96) A/HRC/27/37، الفقرة 20؛ انظر، فيما يتعلق بالاحتجاجات: A/HRC/44/24، الفقرات 29 و35 و52؛ European Court of Human Rights, Big Brother Watch and Others v. the United Kingdom, judgment of 25 May 2021 (58170/13, 62322/14 and 24960/15), para. 495; http://dx.doi.org/10.15779/Z38SS13; https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; and https://pen.org/research-resources/global-chilling/.

(97) انظر https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

(98) انظر https://pen.org/research-resources/global-chilling/.

(99) انظر https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Online-with-the-public.pdf.

(100) A/HRC/44/24، الفقرتان 35 و53.

دال- متطلبات حقوق الإنسان

48- مما لا شك فيه أن المراقبة العامة تنطوي على مخاطر كبيرة في مجال حقوق الإنسان ويمكن أن تقوض إلى حد كبير الحق في الخصوصية. وبالتالي، من الضروري أن تقوم الدول التي تلجأ إلى استخدام المراقبة العامة بتقييم الآثار المحتملة لأعمالها على حقوق الإنسان وأن تكفل بدقة الامتثال للقانون الدولي لحقوق الإنسان، الذي يتطلب أن يستند أي تدخل أو تقييد من هذا القبيل إلى القانون، وهو أمر ضروري لتحقيق هدف مشروع ومتناسب. وغالباً ما تفشل تدابير المراقبة العامة الحالية في تلبية هذه المتطلبات.

49- الشرعية: على الرغم من الآثار بعيدة المدى لمختلف أشكال المراقبة العامة، فإن الأطر القانونية المناسبة القابلة للتطبيق مفقودة إلى حد كبير في العديد من البلدان. وغالباً ما تكون قوانين حماية البيانات مفقودة أو غير كافية أو تقدم استثناءات واسعة النطاق لأجهزة إنفاذ القانون والاستخبارات[101]. وعلاوة على ذلك، ففي كثير من الأحيان، لا توفر القوانين العامة لخصوصية البيانات إرشادات مفصلة أو تضمن قيوداً كافية على استخدام أدوات مراقبة محددة. وفي هذا الصدد، يلزم وضع صكوك قانونية مخصصة، ولا سيما للمراقبة التي تتم في سياق إنفاذ القانون والأمن الوطني[102]. يوجب أن يكون للقوانين واللوائح قيود محددة وصارمة واضحة على الوصول إلى قواعد البيانات الحكومية ودمجها. ومما يؤسف له أن هناك علامات قليلة تشير إلى أن الدول تتجه نحو تنظيم استخدام تقنيات وتكنولوجيات وأدوات الاستخبارات على وسائل التواصل الاجتماعي. ومع أن هناك جهوداً متزايدة من قبل المنظمين والمشرعين على المستوى المحلي والوطني والإقليمي لتنظيم تقنية التعرف على الوجه وغيرها من أدوات المراقبة البيومترية[103]، تواصل معظم السلطات تشغيل نظم المراقبة البيومترية بالرغم من عدم وجود أساس قانوني لمثل هذا النشاط.

50- الأهداف المشروعة: ليس هناك شك في أن المراقبة العامة يمكن أن تخدم مجموعة واسعة من الأهداف المشروعة، على سبيل المثال حماية حياة الناس أو سلامتهم الجسدية وأمن البنية التحتية الحيوية. ومما يؤسف له أن المراقبة العامة تجري بصورة روتينية لأغراض لا يسمح بها القانون الدولي لحقوق الإنسان. وقد استخدمت المراقبة العامة دون مبرر، في جملة أمور، لتحديد وتتبع المعارضين السياسيين، ولتنفيذ التنميط العنصري والإثني، واستهداف مجتمعات المثليات والمثليين ومزدوجي الميل الجنسي ومغايري الهوية الجنسانية وحاملي صفات الجنسين، وتقييم مدى امتثال الناس للمعايير الاجتماعية.

51- الضرورة والتناسب: مع أن المراقبة العامة قد تكون مسموحا بها، يجب على الدول أن تثبت أن التدابير ضرورية ومتناسبة على حد سواء. بيد أن فعالية تدابير المراقبة كثيراً ما تكون موضع شك، مما يثير تساؤلات جدية بشأن ضرورتها أو تناسبها. والأدلة على تأثير المراقبة بالفيديو على السلامة ومنع الجريمة مختلطة. وتشير معظم الدراسات في أحسن الأحوال إلى حدوث تخفيضات متواضعة في بعض أنواع الجرائم (مثل الجرائم المتصلة بالمركبات والممتلكات) في المناطق التي ترصدها كاميرات المراقبة،

(101) A/HRC/39/29، الفقرة 34.

(102) سبق للمفوضة السامية أن حددت المتطلبات الدنيا لقوانين المراقبة، انظر A/HRC/27/37 وA/HRC/39/29.

(103) انظر the proposed European Union Artificial Intelligence Act; the European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en; see also law in Washington State, United States of America, relating to the use of facial recognition, available at https://www.securityindustry.org/report/washington-facial-recognition-law-faq/; and bans and moratoriums adopted by local and regional legislatures.

في حين لا يبدو عموما أن جرائم العنف تتأثر بوجود كاميرات مراقبة[104]. وعلاوة على ذلك، فإن المقارنة بين العديد من البلديات في مختلف الولايات القضائية تظهر ارتباطا ضئيلا أو معدوما بين عدد كاميرات المراقبة العامة والجريمة أو السلامة في بلدية بأكملها[105]. وفيما يتعلق بالكشف الآلي عن التهديدات، وهو نظام تستخدمه قوات الشرطة على نطاق واسع للكشف عن الطلقات النارية لتحديد مسارح الجريمة المحتملة، فقد تبين أنه يخطئ في التعرف على الأصوات ويصنفها على أنها طلقات نارية في 89 في المائة من الحالات[106]. وأخيراً، أنهت العديد من إدارات الشرطة التي اشتركت في خدمات الشرطة التنبؤية تعاونها في هذا المجال معللة ذلك بفائدته المحدودة[107].

52- والمراقبة العامة للأشخاص في الأماكن العامة غير متناسبة دائما تقريبا. وينبغي استهداف تدابير المراقبة في الأماكن العامة وينبغي أن تعالج هدفا مشروعا ملموسا، مثل تجنب تهديد محدد للسلامة العامة أو الأمن العام يكون كبيراً بما يكفي ليتجاوز آثارها السلبية على حقوق الإنسان. وينبغي أن تكون هذه التدابير محدودة، وأن تركز على مواقع وأوقات محددة، على سبيل المثال، عندما تشير الأدلة إلى احتمال وقوع جريمة أو إلى احتمال ظهور تهديدات للسلامة والأمن العامين. وينبغي عندئذ ألا يكون هناك أي بديل آخر أقل انتهاكاً للخصوصية. ومن الضروري فرض قيود صارمة على مدة تخزين البيانات التي تم التقاطها والأغراض المرتبطة بها التي سيتم استخدام هذه البيانات من أجلها. وتثير نظم المراقبة البيومترية عن بعد، على وجه الخصوص، شواغل جدية فيما يتعلق بتناسبها، نظراً لطبيعتها المتطفلة للغاية وتأثيرها الواسع النطاق على أعداد كبيرة من الناس[108]. ومن هذا المنطلق، رحبت المفوضة السامية بالجهود التي بذلت مؤخراً للحد من استخدام تكنولوجيات التعرف عن بعد باستخدام البيانات البيومترية أو حظرها، ودعت إلى وقف اختياري لاستخدامها في الأماكن العامة، على الأقل إلى أن يتم وضع ضمانات رئيسية[109]. وإذا ما استخدمت هذه التكنولوجيات على الإطلاق، فلا ينبغي نشرها إلا للاستجابة لحالات مثل الجرائم الخطيرة والتهديدات الخطيرة للسلامة العامة، إذا أمكن استبعاد الآثار التمييزية وإخضاعها لرقابة كافية وفعالة، بما في ذلك الإذن المستقل والمساءلة المستقلة المنتظمة بشأن قضايا حقوق الإنسان.

رابعاً- استنتاجات وتوصيات

53- يقدم هذا التقرير لمحة عن العديد من المجالات الرئيسية التي يتعرض فيها الحق في الخصوصية في المجال الرقمي حالياً للتهديد. ويثير التبني السريع للتكنولوجيات الرقمية مجموعة من التحديات الإضافية التي لم يغطها هذا التقرير ولكنها تستحق مزيداً من الاهتمام. فعلى سبيل المثال، لا تزال المراقبة الجماعية السرية، التي نوقشت في التقارير السابقة للمفوضة السامية، تمثل مشكلة خطيرة[110]. وبالمثل، فإن الآثار

(104) انظر https://academicworks.cuny.edu/jj_pubs/256/; and https://doi.org/10.1080/01924036.2021.1879885.

(105) انظر https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

(106) انظر https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/; and https://igchicago.org/2021/08/24/oig-finds-that-shotspotter-alerts-rarely-lead-to-evidence-of-a-gun-related-crime-and-that-presence-of-the-technology-changes-police-behavior/.

(107) انظر https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

(108) A/HRC/48/31، الفقرتان 26-27؛ A/HRC/44/24، الفقرات 38-33.

(109) A/HRC/48/31، الفقرتان 27 و59(د).

(110) انظر A/HRC/27/37 وA/HRC/39/29.

المترتبة على نُظُم الهوية الرقمية في مجال حقوق الإنسان وحالات الاستخدام المختلفة للبيانات البيومترية ليست مفهومة إلا قليلا، بالرغم من نشر هذه النظم في جميع أنحاء العالم. ويتطلب التتبع الواسع النطاق لمستخدمي الإنترنت من قبل عدد لا يحصى من الشركات، مثل المعلنين والمؤسسات المالية وسماسرة البيانات، اهتماما أكبر بكثير في المنتديات الدولية لحقوق الإنسان. ويمكن أن تشكّل جائحة مرض فيروس كورونا (كوفيد-19) والمجموعة المذهلة من الاستجابات الرقمية لها موضوعا لتقرير قائم بذاته. ويجب استكشاف الطرق التي تؤثر بها انتهاكات الخصوصية والتجاوزات في الأشخاص المهمشين والأشخاص الذين هم في أوضاع هشة وفهمها بشكل أكثر تعمقا. وينبغي السعي عن كثب إلى متابعة الظواهر الناشئة، مثل الدفع نحو اعتماد واسع النطاق للكتل المتسلسلة، وتقنيات الواقع الافتراضي الموسعة، وتطوير تكنولوجيا عصبية متزايدة القوة.

54- ومع ذلك، فحتى في الوقت الذي يركز فيه هذا التقرير على عدد قليل من التطورات الرئيسية، فإنه يعرض صورة مقلقة عن كيفية تقويض الحق في الخصوصية بشكل مطرد في العصر الرقمي. وينبغي ألا يفهم هذا التحليل على أنه ينكر الفوائد الهائلة التي تجلبها التقنيات الرقمية للمجتمعات – بل على العكس من ذلك، يجب على المجتمعات أن تتبنى بالكامل التقدم التكنولوجي الذي يمكّن للناس، ويحسن الحياة، ويقوي العدالة ويعزز الإنتاجية. لكن الطرق المتعددة التي تهدد بها المراقبة المنتشرة حقوق الإنسان وسيادة القانون وقد تؤدي إلى تقويض الديمقراطيات التعددية النابضة بالحياة تثير قلقاً عميقاً. ويمكن أن تصبح التكنولوجيات الرقمية الحديثة المتصلة بالشبكات أدوات هائلة للسيطرة والقمع بفضل ما تتميز به من خصائص: فكل عمل في الفضاء الرقمي يترك أثراً بيانياً. وتسهل تكنولوجيا الحوسبة السحابية دمج وتحليل مصادر البيانات المتباينة. وتعزز الأتمتة النطاق المحتمل للمراقبة وفعاليتها؛ ومن الصعب كشف المراقبة الرقمية من قبل أولئك الذين يخضعون لها. وعلاوة على ذلك، ترتبط المراقبة الرقمية ارتباطاً وثيقاً بالافتقار إلى الشفافية بشكل أعم. وغالباً ما لا يعرف الجمهور إلا القليل جداً عن ممارسات المراقبة المختلفة المتشابكة في العديد من جوانب الحياة. وكثيراً ما تفشل الحكومات في نشر معلومات موثوقة عن نوع نظم المراقبة التي تستخدمها ولأي أغراض تستخدمها وغالباً ما تهمل تقديم أدلة على فعالية تلك النظم.

55- وتدابير المراقبة التي لا تتوافق مع القانون الدولي لحقوق الإنسان منتشرة بالفعل على نطاق واسع. وحتى عندما تخدم المراقبة أغراضا مشروعة، يمكن بسهولة إعادة استخدام البنية التحتية الأساسية، وغالباً ما تخدم غايات لم تكن مخصصة لها أصلاً (ما يسمى "الزحف الوظيفي") أو بعد التغيرات في المشهد السياسي. ويجب على صناع القرار أن يضعوا ذلك في الاعتبار عند النظر في مشاريع جديدة تعزز صلاحيات جمع البيانات الشخصية وتحليلها. وهناك حاجة ماسة إلى عقد مناقشات عامة بشأن حدود المراقبة. وبدون مناقشة عامة نشطة، تخاطر المجتمعات بالسير مغمضة العينين نحو الخضوع لنظم المراقبة مما يسمح لمن هم في السلطة بممارسة مستويات غير مسبوقة من السيطرة على الحياة اليومية.

56- ومع أخذ ذلك في الاعتبار، توصي المفوضية السامية لحقوق الإنسان الدول بما يلي:

(أ) ضمان أن أي تدخل في الحق في الخصوصية، بما في ذلك الاختراق الحاسوبي، والقيود المفروضة على الوصول إلى تكنولوجيا التشفير واستخدامها، ومراقبة الجمهور، يمتثل للقانون الدولي لحقوق الإنسان، بما في ذلك مبادئ الشرعية والهدف المشروع والضرورة والتناسب وعدم التمييز، ولا ينتقص من جوهر هذا الحق؛

(ب) بذل العناية الواجبة في مجال حقوق الإنسان بشكل منهجي، بما في ذلك إجراء تقييمات شاملة منتظمة للأثر على حقوق الإنسان، عند تصميم وتطوير وشراء ونشر وتشغيل نظم المراقبة؛

(ج) مراعاة البيئة القانونية والتكنولوجية الكاملة التي تدمج فيها نظم المراقبة وسلطاتها أو التي ستدمج فيها تلك النظم أو السلطات عند بذل العناية الواجبة في مجال حقوق الإنسان وتقييم مدى ملاءمة نظم وسلطات المراقبة الجديدة؛ وينبغي للدول أيضاً أن تنظر في مخاطر إساءة الاستعمال، والزحف الوظيفي، وإعادة توجيه النظم لأغراض أخرى، بما في ذلك المخاطر الناجمة عن التغيرات السياسية في المستقبل؛

(د) اعتماد تشريعات بشأن خصوصية البيانات للقطاعين العام والخاص وتنفيذها بفعالية، من خلال سلطات مستقلة ومحايدة وذات موارد جيدة، تمتثل للقانون الدولي لحقوق الإنسان، بما في ذلك الضمانات والرقابة وسبل الانتصاف لحماية الحق في الخصوصية بشكل فعال؛

(هـ) اتخاذ تدابير فورية لزيادة شفافية استخدام تكنولوجيات المراقبة بشكل فعال، بما في ذلك عن طريق إعلام الجمهور والأفراد والمجتمعات المحلية المتضررة على النحو المناسب، وتوفير البيانات ذات الصلة بالجمهور بانتظام لتقييم فعاليتها وتأثيرها على حقوق الإنسان؛

(و) تشجيع النقاش العام بشأن استخدام تكنولوجيات المراقبة وضمان المشاركة المجدية لجميع أصحاب المصلحة في القرارات المتعلقة باقتناء تكنولوجيات المراقبة ونقلها وبيعها وتطويرها ونشرها واستخدامها، بما في ذلك وضع السياسات العامة وتنفيذها؛

(ز) تنفيذ وقف اختياري لبيع واستخدام نظم المراقبة المحلية وعبر الوطنية، مثل أدوات الاختراق الحاسوبي والنظم البيومترية التي يمكن استخدامها لتحديد هوية الأفراد أو تصنيفهم في الأماكن العامة، إلى أن تتوفر ضمانات كافية لحماية حقوق الإنسان؛ وينبغي أن تشمل هذه الضمانات تدابير محلية وتدابير لمراقبة الصادرات، تمشياً مع التوصيات الواردة في هذه الوثيقة وفي التقارير السابقة المقدمة إلى مجلس حقوق الإنسان[111]؛

(ح) ضمان حصول ضحايا انتهاكات حقوق الإنسان والتجاوزات المرتبطة باستخدام نظم المراقبة على سبل انتصاف فعالة.

57- وفيما يتعلق بالمسائل المحددة المثارة في هذا التقرير، توصي المفوضية السامية لحقوق الإنسان الدول بما يلي:

الاختراق الحاسوبي

(أ) ضمان ألا تستخدم السلطات عمليات الاختراق الحاسوبي للأجهزة الشخصية إلا كملاذ أخير، وأن تستخدمها فقط لمنع فعل معين يرقى إلى مستوى تهديد خطير للأمن القومي أو جريمة خطيرة محددة أو لأغراض التحقيق في ذلك، وأن تستهدف بشكل ضيق الشخص المشتبه في ارتكابه تلك الأفعال؛ وينبغي أن تخضع هذه التدابير لرقابة مستقلة صارمة وأن تتطلب موافقة مسبقة من هيئة قضائية؛

التشفير

(ب) تعزيز وحماية التشفير القوي وتجنب جميع القيود المباشرة أو غير المباشرة والعامة والعشوائية على استخدام التشفير، مثل الحظر الشامل والتجريم وفرض معايير تشفير ضعيفة أو اشتراط المسح العام الإلزامي من جانب العميل؛ وينبغي ألا يتم التدخل في تشفير الاتصالات الخاصة للأفراد إلا

(111) انظر A/HRC/27/37، A/HRC/39/29، A/HRC/44/24 و A/HRC/48/31.

بإذن من هيئة قضائية مستقلة وعلى أساس كل حالة على حدة، مستهدفاً الأفراد إذا لزم الأمر للتحقيق في الجرائم الخطيرة أو لمنع الجرائم الخطيرة أو التهديدات الخطيرة للسلامة العامة أو الأمن القومي؛

مراقبة الأماكن العامة ومراقبة تصدير تكنولوجيا المراقبة

(ج) اعتماد أطر قانونية مناسبة لتنظيم جمع وتحليل وتبادل المعلومات الاستخبارية على وسائل التواصل الاجتماعي التي تحدد بوضوح الأسباب المسموح بها والمتطلبات المسبقة وإجراءات الترخيص وآليات الرقابة المناسبة؛

(د) تجنب المراقبة العامة للأماكن العامة التي تتطفل على الخصوصية وضمان أن تكون جميع تدابير المراقبة العامة ضرورية ومتناسبة للغاية لتحقيق أهداف مشروعة مهمة، بما في ذلك عن طريق الحد الصارم من موقعها ووقتها، فضلاً عن مدة تخزين البيانات، والغرض من استخدام البيانات والوصول إليها؛ وينبغي ألا تستخدم نظم التعرف البيومترية إلا في الأماكن العامة لمنع الجرائم الخطيرة أو التهديدات الخطيرة للسلامة العامة أو التحقيق فيها، ورهناً بتنفيذ جميع الاشتراطات المنصوص عليها في القانون الدولي لحقوق الإنسان فيما يتعلق بالأماكن العامة[112]؛

(هـ) إنشاء نظم قوية جيدة التصميم لمراقبة الصادرات تنطبق على تكنولوجيات المراقبة، والتي ينطوي استخدامها على مخاطر كبيرة على التمتع بحقوق الإنسان؛ وينبغي للدول أن تشترط إجراء تقييمات شفافة للأثر على حقوق الإنسان تأخذ في الاعتبار قدرات التكنولوجيات المعنية فضلاً عن الحالة في الدولة المتلقية، بما في ذلك الامتثال لحقوق الإنسان، والتقيد بسيادة القانون، ووجود القوانين المنطبقة التي تنظم أنشطة المراقبة وإنفاذها تنفيذاً فعالاً، ووجود آليات رقابة مستقلة؛

(و) الحرص على أن تحترم الشراكات بين القطاعين العام والخاص، لدى توفير تكنولوجيات المراقبة واستخدامها، معايير حقوق الإنسان وتكفل إدماجها الصريح، وتحرص على ألا يكون ذلك سبباً في التخلي عن مساءلة الحكومة عن حقوق الإنسان.

---

(112) بما في ذلك المتطلبات المبينة في الفقرة 53(ي)(‘1’-‘5’) من الوثيقة A/HRC/44/24، والفقرة 59(د) من الوثيقة A/HRC/48/31.