الأمم المتحدة

A/69/397

الجمعية العامة

Distr.: General
23 September 2014
Arabic
Original: English

الدورة التاسعة والستون
البند ٦٨ (أ) من جدول الأعمال
تعزيز حقوق الإنسان وحمايتها: تنفيذ الصكوك الدولية المتعلقة بحقوق الإنسان

تعزيز حقوق الإنسان والحريات الأساسية وحمايتها في سياق مكافحة الإرهاب*

مذكرة من الأمين العام

يتشرف الأمين العام بأن يحيل إلى الجمعية العامة تقرير السيد بن إمرسون، المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، المقدم عملاً بقرار الجمعية العامة ١٧٨/٦٨ وقرار مجلس حقوق الإنسان ١٥/١٥.

* تأخر تقديم هذه الوثيقة.

141014 141014 14-61490 (A)

تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب

ملخص

هذا التقرير هو التقرير السنوي الرابع، يقدمه إلى الجمعية العامة السيد بن إمرسون، المقررُ الخاص الحالي المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب.

ويرد في الفرع الثاني من التقرير بيانُ الأنشطة الرئيسية التي اضطلع بها المقرر الخاص في الفترة من ١٧ كانون الأول/ديسمبر ٢٠١٣ إلى ٣١ تموز/يوليه ٢٠١٤. وفي الفرع الثالث يبحث المقرر الخاص في استخدام المراقبة الرقمية الجماعية لغرض مكافحة الإرهاب ويتناول انعكاسات تكنولوجيا الوصول إلى البيانات بالجملة على الحق في الخصوصية في إطار المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

أولا – مقدمة

١ – يقدم السيد بن إمرسون، المقررُ الخاص الحالي المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب هذا التقرير إلى الجمعية العامة عملاً بقرار الجمعية العامة ١٧٨/٦٨ وقرارات مجلس حقوق الإنسان ١٥/١٥، و ١٩/١٩، و ٨/٢٢، و ٧/٢٥. ويرد في الفرع الثاني من التقرير بيانُ الأنشطة الرئيسية التي اضطلع بها المقرر الخاص في الفترة من ١٧ كانون الأول/ديسمبر ٢٠١٣ إلى ٣١ تموز/يوليه ٢٠١٤. وفي الفرع الثالث يبحث المقرر الخاص في استخدام المراقبة الرقمية الجماعية لغرض مكافحة الإرهاب ويتناول انعكاسات تكنولوجيا الوصول إلى البيانات بالجملة على الحق في الخصوصية في إطار المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

ثانيا – الأنشطة المتصلة بالولاية

٢ – في ١٣ شباط/فبراير ٢٠١٤، شارك المقرر الخاص متحدثاً في حلقة نقاش عن الحكم الثاني بحق ياسين القاضي تحت عنوان: Debating Kadi II "United Nations Ombudsperson v judicial review in Security Council "sanctions decision-making في كلية لندن للاقتصاد.

٣ – من ٢٣ إلى ٢٥ شباط/فبراير ٢٠١٤، شارك المقرر الخاص في حلقة دراسية للخبراء عن الحق في الخصوصية في العصر الرقمي، استضافتها بعثات ألمانيا والبرازيل وسويسرا وليختنشتاين والمكسيك والنرويج والنمسا الدائمة في جنيف، ونظمتها أكاديمية جنيف للقانون الدولي الإنساني وحقوق الإنسان في جنيف.

٤ – في ١١ آذار/مارس ٢٠١٤، قدم المقرر الخاص تقريره إلى مجلس حقوق الإنسان في دورته الخامسة والعشرين، عن استخدام الطائرات الموجهة عن بُعد أو الطائرات المقاتلة بلا طيار في عمليات لمكافحة الإرهاب توقع قتلى خارج الحدود الإقليمية، بما في ذلك في إطار النزاعات المسلحة غير المتكافئة، وآثارها على المدنيين (A/HRC/25/59). وعقد حواراً مع المجلس بشأن التقريرين اللذين قدمهما عن زيارتيه إلى بوركينا فاسو (A/HRC/25/59/Add.1) وشيلي (A/HCR/25/59/Add.2).

٥ – وفي ١٢ آذار/مارس ٢٠١٤، شارك المقرر الخاص، كعضو في فريق الخبراء، في اجتماع جانبي تناول موضوع حقوق الإنسان والطائرات المقاتلة بلا طيار وعقد مؤتمراً صحافياً خلال الدورة الخامسة والعشرين لمجلس حقوق الإنسان.

ثالثا – مكافحة الإرهاب والمراقبة الرقمية الجماعية

ألف – لمحة عامّة

٦ – أدىّ التطوّر الكبير الذي شهدته القدرات التكنولوجية للدول خلال العقد الماضي، إلى تحسّن قدرة أجهزة المخابرات وهيئات إنفاذ القانون على مراقبة الأفراد والمؤسسات في حال الاشتباه. ويوفر اعتراض الاتصالات مصدراً قيماً للمعلومات تستطيع الدول الاستعانة به للتحقيق في أعمال الإرهاب والجرائم الخطيرة الأخرى وإحباطها وملاحقتها. واليوم، تمتلك غالبية الدول قدرة على اعتراض الاتصالات التي تجرى عبر الهواتف الثابتة أو النقالة ورصدها، تمكنها من تحديد موقع أفراد معينين، ورصد تحركاتهم عبر تحليل المواقع الخلوية، وقراءة الرسائل وتسجيلها. والمراقبة الموجهة تمكّن أجهزة المخابرات وهيئات إنفاذ القوانين من رصد نشاط هؤلاء الأشخاص على الإنترنت، واختراق قواعد البيانات ووسائل التخزين السحابي، والحصول على المعلومات المخزنة فيها. ويزداد عدد الدول التي تعتمد نظم البرمجيات الخبيثة التي يمكن استخدامها لاختراق حاسوب الفرد المستهدف أو هاتفه الذكي، وتجاوز إعداداته، ورصد أنشطته. وأساليب المراقبة هذه توفر معاً مجموعة بيانات متعددة المصادر تتيح معلومات مخابراتية قيمة عن أفراد معينين أو منظمات محددة.

٧ – والسمة المشتركة بين تقنيات المراقبة هي اعتمادها جميعاً على اشتباه مسبق بالفرد أو المؤسسة موضع المراقبة. وفي هذه الحالات، تعتمد معظم الدول عرفاً شبه ثابت إذ تطلب الحصول على إذن مسبق (قضائي أو تنفيذي)، وفي بعض الدول هناك شرط إضافي وهو إجراء مراجعة مستقلة لاحقة. لذا، في معظم البلدان هناك على الأقل فرصة واحدة (وأحياناً أكثر من فرصة) للتدقيق في المعلومات المزعم أن تثير الشكوك ولتقييم شرعية تدابير المراقبة وتناسبها بالاستناد إلى الوقائع المرتبطة بقضية محددة. وتتيح المراقبة الموجهة إجراء تقييم موضوعي لضرورة المراقبة وتناسبها، ودراسة مستوى التدخل المقترح على أساس النتيجة المتوقعة منه في مجريات تحقيق معين.

٨ – ولكن وتيرة التقدم التكنولوجي السريعة أتاحت لبعض الدول تأمين إمكانية الوصول بالجملة إلى بيانات الاتصالات والمحتويات من دون ضرورة وجود اشتباه مسبق. واليوم، أصبح بإمكان السلطات المعنية في هذه الدول تطبيق حلول حسابية آلية لاستخراج البيانات لتطويق عالم من حركة الاتصالات قد لا يكون له حدود. وقد تسنّى للدول إجراء عمليات مراقبة جماعية لمحتوى الاتصالات والبيانات الفوقية، وذلك بوضع صنابير على كابلات الألياف البصرية التي يمر عبرها معظم الاتصالات الرقمية، فأتاحت لأجهزة المخابرات

وهيئات إنفاذ القوانين الفرصة لرصد اتصالات الأفراد وتسجيلها، ليس فقط من مواطنيها، بل من المقيمين في دول أخرى أيضاً. ويتم عادةً تعزيز هذه القدرة مع إصدار قوانين للاحتفاظ الإلزامي بالبيانات تفرض على الجهات المقدمة لخدمات الاتصالات السلكية واللاسلكية والإنترنت الاحتفاظ ببيانات الاتصالات لاستخدامها في عمليات التفتيش والتحليل. واستخدام برامج المسح، ومعايير تحديد ملف التعريف، ومصطلحات محددة للبحث، يمكّن السلطات المعنية من فرز الكميات الهائلة من المعلومات المخزنة لتحديد أنماط الاتصالات بين الأفراد والمؤسسات. وتربط العمليات الحسابية الآلية لاستخراج البيانات بين أسماء التعريف والمواقع والأرقام وعناوين بروتوكول الإنترنت، وتبحث عن أي علاقات ترابط، والتقاء جغرافي بين بيانات الموقع، وأنماط العلاقات الاجتماعية وغيرها من العلاقات على الإنترنت[1].

٩ - وهكذا تستطيع الدول التي تسجل ارتفاعاً في معدلات انتشار الانترنت الوصول إلى محتويات الهاتف والبريد الإلكتروني لعدد غير محدود من المستخدمين ويمكنها تعقب النشاط الذي يجري على مواقع إلكترونية معينة على شبكة الإنترنت. وكل ذلك ممكن من غير أيّ اشتباه مسبق بفرد محدد أو مؤسسة معينة. ومن المحتمل إذاً أن تكون الاتصالات التي يجريها كل فرد يستخدم الإنترنت مفتوحة أمام أجهزة المخابرات وهيئات إنفاذ القوانين في الدول المعنية. والواقع أن هذه العملية تصل إلى حد التدخل المنهجي في الحق في احترام خصوصية الاتصالات، وتستلزم مبرراً وافياً لاستخدامها.

١٠ - ومن منظور إنفاذ القانون، تستمدّ تقنية المراقبة الجماعية قيمتها المضافة من قدرتها على مراقبة اتصالات أفراد ومؤسسات لم يسبق أن لفتت إنتباه السلطات. وتُعزى المنفعة العامة في تكنولوجيا الوصول بالجملة إلى أنها لا تتطلب اشتباهاً مسبقاً بجهة معينة. وهذا المنطق يدور في حلقة متواصلة، لا يمكن الخروج منها إلا بوضع ممارسات الدول في هذا الإطار موضع التحليل بمقتضى ما تنص عليه المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

١١ - وتنص المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية على أن أي تدخل بالاتصالات الشخصية ينبغي أن يكون منصوصا عليه بموجب القانون وأن يكون وسيلة ضرورية ومتناسبة لتحقيق هدف مشروع في السياسة العامة (كما هو وارد أدناه في الفقرات ٢٨-٣١). ومكافحة الإرهاب هي حتماً هدف مشروع لهذا الغرض

(١) http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf.

(كما هو وارد أدناه في الفقرات ٣٣ و ٣٤)، على أن تتقيّد أنشطة أجهزة المخابرات وهيئات إنفاذ القوانين في هذا المجال بالقانون الدولي لحقوق الإنسان[٢]. ومجرد التأكيد، من دون تخصيص، أن تقنية المراقبة الجماعية يمكن أن تساهم في منع أعمال الارهاب وملاحقتها لا يعطي مبرراً وافياً لهذه المراقبة وفقاً لأحكام قانون حقوق الإنسان. فالجدوى التقنية لأي خيار وفائدته في الحصول على معلومات مخابراتية قيمة، لا تكفي بحد ذاتها لتبريره من الناحية المنطقية أو القانونية (وفقاً لأحكام القانون الدولي أو المحلي) (A/HRC/27/37 الفقرة ٢٤).

١٢ - ويفرض القانون الدولي لحقوق الإنسان على الدول تقديم مبرر واضح وافي الأدلة لأي تدخل في الحق في الخصوصية أكان ذلك على صعيد فردي أم جماعي. وحسب مبدأ التناسب، كلما ارتفعت درجة التدخل في حقوق الإنسان التي يحميها القانون، ازدادت الحاجة إلى مبررات وافية، إذا أريد للتدخل أن يمتثل لشروط العهد الدولي. والحقيقة التي لا لبس فيها أن استخدام تقنية المراقبة الجماعية لا يلتقي بالفعل مع الحق في خصوصية الاتصالات على الإنترنت. وهذه التكنولوجيا، إذ تتيح الوصول بالجملة إلى جميع حركات الاتصالات الرقمية، تتنافى مع إمكانية تحليل التناسب حسب كل حالة على حدة. وهي تسمح باعتراض الاتصالات الشخصية من دون الحاجة إلى أي ترخيص مستقل (أو أي ترخيص مسبق) يُعطى استناداً إلى اشتباه بفرد معين أو مؤسسة معينة. وهكذا يكون التدقيق المسبق ممكناً على أعلى مستويات العموم فقط.

١٣ - وفي حين لا يتوفر مبرر خاص بجهة مستهدفة معينة لاتخاذ تدابير المراقبة الجماعية، يتحتم على الدول المعنية تبرير الممارسة العامة المتعلقة بالسعي إلى الوصول بالجملة إلى الاتصالات الرقمية. وبذلك ينتقل تحليل التناسب من المستوى الجزئي (تقييم مبرر اختراق خصوصية أفراد أو مؤسسات معينة) إلى المستوى الكلي (تقييم مبرر اعتماد نظام يشمل التدخل بالجملة بالحق في الخصوصية الفردية والجماعية لجميع مستخدمي الإنترنت). وضخامة التدخل في الحق في الخصوصية تستدعي في المقابل تبريراً في السياسة العامة يضاهي حجم التدخل.

١٤ - وفي حد أدنى، تفرض المادة ١٧ على الدول التي تستخدم تقنية المراقبة الجماعية أن تقدم كشفاً علنياً مقنعاً بالفوائد الملموسة المتأتية عن استخدام هذه التقنية. ومن دون هذا المبرر ما من وسيلة لقياس مدى امتثال هذه الممارسة الناشئة للأحكام التي ينص عليها العهد الدولي. ويتطلب تقييم التناسب في هذا السياق نوعاً من التوازن بين المصلحة الاجتماعية في

(٢) يمكن الاطلاع على تجميع للممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية لأجهزة المخابرات والرقابة على هذه الأجهزة، الصادرة عن المقرر الخاص (A/HRC/14/46، الفقرات ٩-٥٠).

حماية الخصوصية على الإنترنت، والمستلزمات الحتمية لمكافحة الإرهاب وإنفاذ القوانين بطريقة فعالة. ويتطلب تحديد مواضع هذا التوازن إجراء نقاش عام مستنير بين الدول وضمن الدولة الواحدة. ويحتاج المجتمع الدولي إلى التصدي مباشرةً للتحول الجذري في مفهومنا الجماعي للعلاقة بين الفرد والدولة[٣]. والشرط الأساسي لتقييم قانونية التدابير المتخذة هو أن تتوخى الدول التي تستخدم هذه التقنية الشفافية في المنهجية والتبرير[٤]. وفي غياب هذه الشفافية، يطرح خطر الانتشار المتزايد للتدخل المنهجي في أمن الاتصالات الرقمية من دون النظر بجدية إلى الآثار المترتبة على الإهدار الجماعي للحق في الخصوصية على الإنترنت. وإذا استمرت الدول التي تستخدم هذه التقنية باحتكار المعلومات حول تأثيرها، فسيسود نوع من الرقابة، يفرض قيوداً على المفاهيم الأساسية ويحول دون إجراء نقاش مستنير.

١٥ - ويفترض البعض عدم وجود منطق يستند إليه مستخدمو الإنترنت في توقع حماية خصوصيتهم على الإنترنت، وعلى معظمهم أن يتوقعوا أن ما يجرونه من اتصالاتهم متاح للرصد من شركات خاصة وأجهزة الدولة على حد سواء. ويجري مناصرو هذا الرأي مقارنة تقليدية، إذ يشبهون إرسال بريد إلكتروني غير مشفر بإرسال بطاقة بريدية. ولكن هذه المقارنة، ومهما كانت قيمتها، لا تجيب عن الأسئلة المتعلقة بالقانونية والضرورة والتناسب. والغاية الأساسية من الشرط الذي ينص عليه العهد الدولي بشأن وضع تشريعات واضحة ومتاحة للاطلاع عليها ترعى تدخل الدولة في الاتصالات، هي تمكين الأفراد من معرفة مدى الحقوق العائدة لهم في الخصوصية وتوقع الظروف التي قد تخضع فيها اتصالاتهم للمراقبة (الفقرات ٣٥-٣٩). غير أن قيمة هذه التكنولوجيا كأداة لمكافحة الإرهاب وإنفاذ القانون تكمن في أن مستخدمي الإنترنت يفترضون أن اتصالاتهم سرية (وإلا لما كان هناك أي غرض من التدخل بها). وهذا ما أكده أعضاء في الوكالات الاستخبارية في الولايات المتحدة الأمريكية والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية على أثر الإفصاح عن برامج

---

(٣) As the United States Privacy and Civil Liberties Oversight Board has observed: "[P]ermitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens"; "Report on the Telephone Records Program and on the Operations of the Foreign Intelligence Surveillance Court".

(٤) تشير مفوضة الأمم المتحدة السامية لحقوق الإنسان في تقريرها عن الحق في الخصوصية في العصر الرقمي (A/HRC/27/37، الفقرة ٤٨) إلى أن "الغياب المزعج للشفافية الحكومية المرتبطة بسياسات وقوانين وممارسات المراقبة، الذي يعيق أي جهود لتقييم اتساقها مع القانون الدولي لحقوق الإنسان ولضمان المساءلة".

المراقبة الجماعية التي تعمل بها الدولتان، إذ أفيد بأن الإفصاح عن المعلومات أخلّ بالأمن القومي لأنه نبه الإرهابيين المحتملين إلى أن اتصالاتهم خاضعة للمراقبة[٥].

١٦ - وأي تقييم للتناسب ينبغي ألا يغفل على الإطلاق أن شبكة الإنترنت هي اليوم وسيلة الاتصال التي تخترق كل مكان، ويستخدمها الملايين في العالم. وقد أحدثت الثورة في التكنولوجيا الرقمية تحولاً هائلاً في طريقة التواصل بين الناس وأصبحت تكنولوجيا الاتصالات الرقمية التي تستخدم الإنترنت (بما فيها الأجهزة المحمولة والهواتف الذكية) في صلب الحياة اليومية (A/HRC/27/37، الفقرة ١). وكل من يريد المشاركة في تبادل المعلومات والأفكار في عالم الاتصالات الحديث أصبح اليوم مضطراً لاستخدام تكنولوجيا الاتصالات العابرة للحدود الوطنية. وكثيراً ما تعبر حركة الإنترنت في دولة معيّنة خوادم تقع ضمن ولايات دول أخرى. وما من مبرر وافٍ للزعم بأن مستخدمي الإنترنت تنازلوا طوعاً عن حقهم (المرجع نفسه، الفقرة ١٨). فمن المبادئ العامة للقانون الدولي لحقوق الإنسان أن أي شخص لا يعتبر متخلياً عن حق من حقوق الإنسان التي يحميها هذا القانون إلا بموجب تنازل يصدر عنه طوعاً وصراحة، وعن اطّلاع لا لبس فيه. وفي العالم الرقمي الحديث، لا يمكن أن يشكل مجرد استخدام الإنترنت كوسيلة اتصالات خاصة تنازلاً عن اطّلاع عن الحق في الخصوصية وفقاً للمادة ١٧ من العهد الدولي.

١٧ - وشبكة الإنترنت ليست مساحة عامة وحسب، بل تختزن، إلى جانب المجالات الاجتماعية والعامة، الكثير من النطاقات الخاصة[١]. ومن البديهي ألا يكون لدى الأشخاص الذين يستخدمون عن اطّلاع مواقع التواصل الاجتماعي حيث تنشر الرسائل على العموم، أي توقعات منطقية بالحفاظ على الخصوصية على هذه المواقع. وإذا كان تشبيه نشر المعلومات عبر المواقع العامة مثل فيسبوك وتويتر أو النشر عبر المواقع العامة بالبطاقة البريدية تشبيه في محله، فما من وجه شبه بين قراءة بطاقة بريدية واعتراض الرسائل الخاصة التي تبعث بالبريد الإلكتروني أكانت مشفرة أم غير مشفرة.

١٨ - ويضمن القانون الحق في احترام الخصوصية في الاتصالات الرقمية (وهو حق غير قابل للنقاش) (يمكن الاطلاع على قرار الجمعية العامة ١٦٧/٦٨)، واعتماد تكنولوجيا المراقبة الجماعية يمس فعلاً بجوهر هذا الحق (الفقرات ٥١ و ٥٢ أدناه) ويتعارض مع المبدأ الأساسي الذي ينص على ضرورة اعتماد الدول للوسائل المتوفرة الأقل اقتحاماً لترسيخ

(٥) http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388 and www.itv.com/news/2013-10-09/the-damage-of-edward-snowdens-revelations.

حقوق الإنسان المحمية (الفقرة ٥١ أدناه) ولا يتيح أي تقييم للتناسب على الصعيد الفردي (الفقرة ٥٢ أدناه) وتحيطه مطالبات بالحفاظ على السرية تجعل أي شكل آخر من تحليل التناسب غايةً في الصعوبة (الفقرتان ٥١ و ٥٢ أدناه). ولم تنجح الدول التي تعتمد المراقبة الجماعية حتى الآن في تقديم تبرير علني مفصل ووافي الأدلة يثبت ضرورة استخدام هذه التقنية ولم تسن أي دولة تقريباً تشريعات محلية لتنظيم عملية السماح بهذا الاستخدام (الفقرة ٣٧ أدناه). وانطلاقاً من المادة ١٧ من العهد الدولي، تبقى هذه الممارسة أقرب إلى التعارض مع الحق في خصوصية الاتصالات الشخصية بالمجمل. ولهذه الأسباب، تطرح المراقبة الجماعية للمحتوى الرقمي وبيانات الاتصالات تحدياً كبيراً أمام قاعدة راسخة من قواعد القانون الدولي. ويعتبر المقرر الخاص أن اعتماد برامج المراقبة الجماعية هو على الأرجح تدخل غير متناسب في الحق في الخصوصية[٦]. وهذا التحليل يتعارض مع المفاهيم السائدة بشأن خصوصية الدول في جمع الاتصالات أو البيانات الفوقية كلّها في أي وقت ومن دون تمييز، لأن جوهر الحق في خصوصية الاتصالات يكمن في وجوب أن يكون التدخل في هذا الحق استثنائياً ومبرراً وفقاً لكل حالة على حدة (الفقرة ٥١ أدناه).

١٩ - وقد يكون في مكافحة الإرهاب تبرير وافٍ لإعادة تقييم حقوق الخصوصية على الإنترنت حسب ما تتطلبه هذا الممارسات. ولكن الحجج الداعمة لإبطال الحق في الخصوصية على الإنترنت لم تقدّم بعد من الدول المعنية، ولم تخضع إلى تدقيق معمّق أو نقاش مطّلع. وحتى يتوفر في خطر الإرهاب التبرير المقنع للمراقبة الجماعية، لا بد من أن تتمكن الدول التي تستخدم تقنية المراقبة الجماعية من تبيان المزايا الفريدة والملموسة التي حققتها باستخدامها هذه التقنية في مكافحة الإرهاب. ولا ينبغي على الإطلاق استغلال التدابير المبررة بواجب الدولة في الحماية من خطر الإرهاب، كذريعة لتوسيع صلاحيات المراقبة لأهداف لا تمتّ بصلة للوظائف الحكومية. وهناك خطر دائم في أن تتسلل أغراض أخرى إلى الغرض الأساسي بحيث تستخدم السلطات العامة التدابير المبررة بمكافحة الإرهاب لأغراض أخرى أقل أهمية للمصلحة العامة (الفقرة ٥٥ أدناه). وفي هذا التقرير يستند المقرر الخاص إلى أعمال سلفه (A/HRC/13/37) وأعمال المقرر الخاص السابق المعني بتعزيز وحماية الحق في حرية الرأي والتعبير (A/HRC/23/40). ويعتبر المقرر الخاص أن تقديم شرح فوري ودقيق وعلني عن سبب تبرير الاقتحام بالجملة للخصوصية الجماعية لمكافحة الإرهاب أو أي جريمة خطيرة أخرى، بات مسؤولية الدول التي تعتمد تكنولوجيا مراقبة الوصول إلى البيانات بالجملة.

(٦) يمكن أيضاً الاطلاع على وجهة نظر مفوضة الأمم المتحدة السامية لحقوق الإنسان، A/HRC/27/37، الفقرتان ٢٠ و ٢٥.

باء - المعلومات التي جرى مؤخراً الإفصاح عنها والمتعلقة بنوع المراقبة الرقمية لدى الدول ومداها

٢٠ - في ٥ حزيران/يونيه ٢٠١٣، نشرت إحدى الصحف المحلية في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية محتوى أمر قضائي سري صادر عن محكمة مراقبة المخابرات الأجنبية الأمريكية بموجب الفرع ٢١٥ من قانون مكافحة الإرهاب. وأوردت الصحيفة أن هذا الأمر يتضمن طلباً إلى إحدى أكبر شركات الاتصالات السلكية واللاسلكية في الولايات المتحدة الأمريكية بتسليم جميع ''البيانات الفوقية الهاتفية'' إلى وكالة الأمن القومي، وذلك بشكل يومي ولمدة ثلاثة أشهر، ويحظر على الشركة الكشف عن وجود هذا الطلب أو الأمر. وفي ٦ حزيران/يونيه ٢٠١٣، نشرت صحيفة أمريكية خبراً آخر يكشف عن استخدام وكالة الأمن القومي لبرنامج مراقبة رقمي سري يعرف ببرنامج PRISM. وقيل إن عمل هذا البرنامج، الذي أجيز اعتماده بموجب الفرع ٧٠٢ من قانون مراقبة المخابرات الأجنبية الأمريكية حسبما أفيد، يشمل تجميع بيانات المحتويات من الخوادم المركزية لتسع من الشركات الرائدة في التكنولوجيا في الولايات المتحدة الأمريكية.

٢١ - وحسب تقارير صادرة عن الصحيفتين، أصبحت المواد التي عثر عليها برنامج PRISM متاحة أمام أجهزة مخابرات أخرى منها مقر الاتصالات الحكومية في المملكة المتحدة (GCHQ). وأفادت معلومات لاحقة عن استخدام برنامج آخر لجمع بيانات هو برنامج Upstream، وهو حسبما أفيد يترصّد الاتصالات التي تجرى عبر الهاتف والإنترنت على حد سواء وتمر عبر كابلات الألياف البصرية ومنشآت البنى التحتية المملوكة من مزوّدي الخدمات في الولايات المتحدة الأمريكية. والواقع أن نسبة كبيرة من حركة الانترنت في العالم تمر عبر خوادم تقع في الولايات المتحدة.

٢٢ - وذكرت وسائل الإعلام لاحقاً أن مديرية المخابرات الخاصة بنظم الاتصالات (Systems Intelligence Directorate) في وكالة الأمن القومي تضم فرعاً مختصاً بالبحث عن ثغرات في التطبيقات لاختراقها ''application vulnerabilities branch''، وهو يعمل على جمع البيانات من نظم الاتصالات في العالم. ويقال إن الوكالة تدير آلية لاستخدام الانترنت هي نظام Quantum الذي يسمح لها بكشف حاسوب الطرف الثالث من خلال التحكم السري بخوادم (أو امتلاكها) في مواقع رئيسية على الجزء الأهم من الإنترنت. ويقوم النظام بمحاكاة مواقع معينة (بما فيها المواقع الأكثر شيوعاً مثل صفحة البحث في موقع جوجل) ويُدخل من دون أي إذن برنامج تحكم عن بعد إلى الحاسوب أو الجهاز العامل بالاتصال اللاسلكي بالإنترنت للمستخدم الذي يزور الموقع المستنسخ (والذي لن يشك في صحة الموقع

المستنسخ). ويعتبر خبراء التكنولوجيا أن هذه المنهجية تكشف حاسوب المستخدم بشكل دائم وتضمن توفير معلومات مخابراتية لوكالة الأمن القومي في الولايات المتحدة الأمريكية إلى أجل غير مسمّى.

٢٣ - لاحقاً، اتخذت السلطات التنفيذية والتشريعية في الولايات المتحدة الأمريكية عدداً من الخطوات رداً على كشف هذه المعلومات. ومن القضايا التي برزت مع هذه التطورات هو الفرق في التعامل مع المواطنين الأمريكيين والمواطنين غير الأمريكيين (حتى المقيمين ضمن الأراضي الإقليمية للولايات المتحدة الأمريكية). وفي ما يلي ملخص عن التطورات الرئيسية:

(أ) في ٩ آب/أغسطس ٢٠١٣، أعلن الرئيس باراك أوباما أنه طلب إلى مجلس الرقابة على الخصوصية والحريات المدنية[٧] إجراء مراجعة للجهود المبذولة حالياً لمكافحة الإرهاب[٨]. وفي أواخر آب/أغسطس ٢٠١٣، طلب المجلس إلى مدير المخابرات الوطنية والنيابة العامة تحديث إجراءات أجهزة المخابرات المتعلقة بجمع المعلومات وحفظها ونشرها[٩]؛

(ب) في ١٢ كانون الأول/ديسمبر ٢٠١٣، أصدر فريق المراجعة التابع للرئيس تقريره عن الحرية والأمن في العالم المتغيّر وقدم فيه عدداً من التوصيات الهامة بشأن الإصلاح. وعلى ضوء هذا التقرير، اقترح الرئيس في ١٧ كانون الثاني/يناير ٢٠١٤ سلسلة من التغييرات التشريعية والإدارية[١٠]. وبالتزامن مع ذلك أصدرت الحكومة توجيهاً رئاسياً جديداً بشأن السياسة العامة "PPD-28" لتفعيل الرقابة في أنشطة مخابرات الإشارات التي تقوم بها أجهزة المخابرات داخل الولايات المتحدة الأمريكية وخارجها على حد سواء[١١]؛

(ج) في ٢٣ كانون الثاني/يناير ٢٠١٤، أصدر مجلس الرقابة على الخصوصية والحريات المدنية التقرير الأول من تقريرين، وقد استخلصت فيه الأكثرية أن برنامج البيانات الفوقية الهاتفية لا يتفق مع القانون المحلي لأن البند ٢١٥ من قانون مكافحة الإرهاب لم يوفر

---

(٧) المجلس هو وكالة مستقلة تابعة للسلطة التنفيذية تتمتع بصلاحية استعراض عمليات مكافحة الإرهاب وتحليلها وضمان توازنها مع ضرورة حماية الخصوصية والحريات المدنية؛ www.pclob.gov.

(٨) www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

(٩) www.pclob.gov/newsroom.

(١٠) www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html

(١١) www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

مبرراً كافياً لدعمه[١٢]. وفي ٢٧ آذار/مارس أطلق الرئيس أوباما مجموعة من الاقتراحات الجديدة لإلغاء هذا البرنامج[١٣]. وفي ٢٢ أيار/مايو ٢٠١٤، اعتمد مجلس النواب قانون الحرية الأمريكي الذي تضمّن بعضاً من مقترحات الرئيس؛

(د) وفي ٢ تموز/يوليه ٢٠١٤، أصدر مجلس الرقابة على الخصوصية والحريات المدنية تقريراً ثانياً يحدد بالتفصيل كيفية تطبيق عمليات المراقبة بموجب الفرع ٧٠٢ من قانون مراقبة المخابرات الأجنبية[١٤]. وفي حين كان الشاغل الرئيسي الذي تناوله التقرير هو توافق هذه البرامج مع الأحكام التشريعية والدستورية في الولايات المتحدة الأمريكية، اعترف المجلس بأنه أثار أيضاً مسألة هامة وشائكة في الشأن القانوني والسياسة العامة، تتعلق في كيفية معاملة الأشخاص غير الأمريكيين[١٥]. ورأى المجلس أن قضية تطبيق الحق في الخصوصية على المراقبة الأمنية الوطنية في بلد معيّن وتأثيرها على سكان بلد آخر، غير ''محسومة'' بين الدول الأطراف في العهد الدولي الخاص بالحقوق المدنية والسياسية، وهذا ما يتبيّن من خلال ''المناقشات الحامية الجارية''[١٦].

٢٤ - وأجريت عملية مراجعة أيضاً في المملكة المتحدة ورداً على الإدعاءات الموجهة إلى مقر الاتصالات الحكومية بالتحايل على قانون المملكة المتحدة بسبب استخدامه برنامج المراقبة PRISM للوصول إلى محتوى اتصالات لا يجيز القانون المحلي الوصول إليها، أدلى وزير الخارجية في ١٠ حزيران/يونيه ٢٠١٣ ببيان في البرلمان أشار فيه إلى أن البيانات المأخوذة من الولايات المتحدة الأمريكية والتي تعني مواطنين من المملكة المتحدة ''تخضع للضوابط والضمانات القانونية الخاصة بالمملكة'' بما فيها الأحكام ذات الصلة في قانون أجهزة المخابرات لعام ١٩٩٤، وقانون حقوق الإنسان لعام ١٩٩٨، والقانون المتعلق بتنظيم سلطات التحقيق لعام ٢٠٠٠[١٧].

---

(١٢) "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court".

(١٣) www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

(١٤) "Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA", www.pclob.gov/meetings-and-events/2014meetingsevents/02-july-2014-public-meeting.

(١٥) Ibid., p. 98.

(١٦) Ibid., p. 100.

(١٧) www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq.

٢٥ - وفي ٢١ حزيران/يونيه ٢٠١٣، نشر الإعلام معلومات عن استخدام مقر الاتصالات الحكومية لبرنامج آخر ('Tempora') قضى بوضع أجهزة على كابلات الألياف البصرية التي تعمل بين المملكة المتحدة والولايات المتحدة الأمريكية تسهل اعتراض البيانات الفوقية ومعلومات المحتويات. وطرحت التساؤلات داخل برلمان المملكة المتحدة وخارجه عما إذا كانت التشريعات السارية تمنح مقر الاتصالات الحكومية السلطة القانونية للقيام بهذه العمليات وما إذا كانت تحترم الحق في الخصوصية الذي تضمنه المادة ٨ من الإتفاقية الأوروبية لحقوق الإنسان[١٨]. لاحقاً جرى الإفصاح عن معلومات ركزت على دور فريق المخابرات المشترك للبحث في التهديدات (Joint Threat Intelligence Group) التابع لمقر الاتصالات الحكومية. وقيل إن الوكالة نشرت فيروساً حاسوبياً يعرف باسم Ambassador's Reception لإجراء أعمال خفية على الإنترنت. ويقال إن هذا الفيروس يقوم بتشفير نفسه ويعمل على تقليد اتصالات مستخدمين آخرين على الإنترنت.

٢٦ - وأجرت لجنة المخابرات والأمن (وهي لجنة برلمانية مسؤولة عن الإشراف على أجهزة المخابرات)[١٩] تحقيقاً أولياً في عملية وصول مقر الاتصالات الحكومية إلى بيانات الاتصالات والمحتويات. وفي ١٧ تموز/يوليه ٢٠١٣، أصدرت بيانها بهذا الشأن وقد وضعت في عين الاعتبار الإطار القانوني الذي يحكم ترتيبات تبادل المعلومات بين مقر الاتصالات الحكومية ونظرائه في الخارج، وخلصت إلى أنه لم يحدث أي انتهاك لأي قانون من قوانين المملكة المتحدة وأن إجراءات مقر الاتصالات الحكومية تتفق مع واجباته القانونية بموجب قانون أجهزة المخابرات لعام ١٩٩٤. ولكن اللجنة استنتجت أن من المجدي إجراء المزيد من التحقيقات لدراسة مدى ملاءمة الإطار القانوني الحالي الذي يحكم الوصول إلى الاتصالات الخاصة وذلك بالنظر إلى ''التداخل المتشعّب'' بين قانون أجهزة المخابرات لعام ١٩٩٤، والقانون المتعلق بتنظيم سلطات التحقيق لعام ٢٠٠٠. وفي ١٧ تشرين الأول/أكتوبر ٢٠١٣، أعلنت لجنة المخابرات والأمن أنها ستوسع نطاق استقصاءاتها بدافع قلقها حيال حجم قدرات أجهزة المخابرات وتأثير العمليات التي تقوم بها على الحق في الخصوصية[٢٠].

٢٧ - وفي ٨ نيسان/أبريل ٢٠١٤، أصدرت محكمة العدل التابعة للاتحاد الأوروبي حكمها في قضية الحقوق الرقمية في أيرلندا وأعلنت فيه أن توجيهات الاتحاد الأوروبي المتعلقة

---

(١٨) www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance
www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm

(١٩) http://isc.independent.gov.uk.

(٢٠) http://isc.independent.gov.uk/news-archive/17october2013.

بالاحتفاظ بالبيانات تتضارب مع الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية اللذين يضمنهما ميثاق الحقوق الأساسية للاتحاد الأوروبي[٢١]. وهذه التوجيهات تلزم مزوّدي خدمات الاتصالات بالاحتفاظ ببيانات حركة الاتصالات وإتاحتها للسلطات الوطنية المختصة بهدف منع حدوث الجرائم الخطيرة بما فيها أعمال الإرهاب، والتحقيق فيها وكشفها وملاحقتها. ومع اعتبار المحكمة أن الاحتفاظ بهذه البيانات والوصول إليها يشكل تدخلاً خطيراً للغاية في الحقين المذكورين، رأت أن التوجيهات لم تستوفِ مبدأ التناسب. واستناداً إلى هذا الحكم، وضعت حكومة المملكة المتحدة في ١٠ تموز/يوليه ٢٠١٤، مسودة قانون بشأن الاحتفاظ بالبيانات وسلطات التحقيق. وصنفت الحكومة مسودة القانون، الذي اتخذ اليوم صيغة القانون النهائي، على أنه تدبير لتوضيح طبيعة ونطاق الموجبات التي يمكن أن تفرض على مزوّدي خدمة الإنترنت والاتصالات في المملكة المتحدة[٢٢].

جيم - المراقبة الجماعية، مكافحة الإرهاب، والحق في الخصوصية

١ - الحق في الخصوصية بموجب المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية

٢٨ - يمكن تعريف الخصوصية بافتراض ضرورة إتاحة المجال للأفراد للنمو المستقل والتفاعل والحرية، من دون تدخل الدولة والتدخل المفرط غير المطلوب من أفراد دخلاء (A/HRC/23/40، الفقرة ٢٢؛ و A/HRC/13/37، الفقرة ١١). وواجب احترام خصوصية الاتصالات وأمنها يعني حق الأفراد في تبادل المعلومات والأفكار من دون تدخل من الدولة (أو جهة خاصة)، وكفالة معرفتهم بأن اتصالاتهم ستصل فقط إلى الجهات المقصودة ولن يقرأها أحد سواها[٢٣]. ويشمل الحق في الخصوصية حق الأفراد في معرفة من يحتفظ بالمعلومات المتعلقة بهم وكيف تستخدم هذه المعلومات[٢٤].

٢٩ - والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية هي أهم حكم ملزم قانوناً تنصّ عليه معاهدة على الصعيد العالمي بشأن الحق في الخصوصية. وتنص هذه المادة على أنه ”لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في

---

(٢١) Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014.

(٢٢) www.gov.uk/government/speeches/communications-data-and-interception.

(٢٣) Human Rights Committee General Comment No. 16, para. 8.

(٢٤) Ibid., para. 10; see A/HRC/23/40, para. 22.

خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته'' وأن ''من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس''. وتتضمن صكوك دولية أخرى متعلقة بحقوق الإنسان أحكاماً مماثلة وتكرس القوانين على الصعيدين الإقليمي والوطني أيضاً حق جميع الأشخاص في أن تُحترم حياتهم الخاصة وحياتهم العائلية وسكنهم ومراسلاتهم.

٣٠ - ولكن الحق في الخصوصية ليس حقاً مطلقاً. ومتى أصبح فرد مشتبهاً به وبدأ التحقيق معه رسمياً من أجهزة المخابرات وهيئات إنفاذ القوانين، يمكن أن يخضع للمراقبة لأغراض مشروعة حقاً، من قبيل مكافحة الإرهاب وإنفاذ القوانين (A/HRC/13/37، الفقرة ١٣). ولا تتضمن المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية بنداً مقيداً محدداً يبين الظروف التي يمكن فيها أن تتوافق إجراءات التدخل في الحق في الخصوصية مع العهد، ولكن من المعروف عالمياً أنه يسمح بهذه الإجراءات شرط (أ) أن يسمح بها القانون المحلي الذي ينبغي أن يكون متاحاً ودقيقاً ويتماشى مع أحكام العهد[٢٥]، (ب) أن يكون لها هدف مشروع، (ج) أن تستوفي إختبارات الضرورة والتناسب[٢٦].

٣١ - وقد دفع التنبّه إلى أن جزءاً كبيراً من حركة الإنترنت في العالم توجه عبر الولايات المتحدة الأمريكية، عدداً من الدول إلى الإعراب عن القلق حيال استخدام برنامج PRISM من احتمال انتهاك حق مواطنيها في الخصوصية. وفي كانون الأول/ديسمبر ٢٠١٣، اتخذت الجمعية العامة القرار ١٦٧/٦٨ بشأن الحق في الخصوصية في العصر الرقمي، الذي اشتركت في تقديمه ٥٧ دولة عضواً وأقرّ من دون تصويت. وفي هذا القرار، أكدت الجمعية العامة وجوب حماية الحق في الخصوصية على الإنترنت وأهابت بجميع الدول أن تستعرض إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجمع البيانات الشخصية، مشددةً على الحاجة إلى ضمان تنفيذ التزامات الدول بموجب القانون الدولي لحقوق الإنسان تنفيذاً كاملاً وفعالاً.

---

(٢٥) Human Rights Committee general comment No. 16, para. 3.

(٢٦) A/HRC/27/37، الفقرات ٢٢-٢٥؛ وA/HRC/23/40، الفقرتان ٢٨ و٢٩؛ A/HRC/13/37، الفقرات ١٣-١٧؛ ومبادئ سيراكيوزا المتعلقة بأحكام التقييد وعدم التقيد الواردة في العهد الدولي الخاص بالحقوق المدنية والسياسية، E/CN.4/1985/4، المرفق؛ Human Rights Committee general comments Nos. 16, 27, 29, 34 and 31; Human Rights Committee, Van Hulst v. Netherlands, Communication No. 903/2999, 2004; Madafferi v. Australia, Communication No. 1011/2001, 2004; Toonen v. Australia, Communication No. 488/1992, para. 8.3; MG v. Germany, Communication No. 1482/2006, 2008; and CCPR/C/USA/CO/4.

٣٢ - وفي هذا القرار، طلبت الجمعية العامة إلى مكتب المفوض السامي لحقوق الإنسان تقديم تقرير إلى مجلس حقوق الإنسان والجمعية العامة عن حماية الخصوصية وتعزيزها في سياق المراقبة الداخلية والخارجية و/أو اعتراض الاتصالات الرقمية وجمع البيانات الشخصية، بما في ذلك على نطاق جماعي. وفي الفقرة ٤٧ من التقرير السنوي لمفوضة الأمم المتحدة السامية لحقوق الإنسان الصادر في ٣٠ حزيران/يونيه ٢٠١٣ (A/HRC/27/37)، استنتجت المفوضة السامية أن القانون الدولي لحقوق الإنسان يوفر إطاراً واضحاً وعالمياً لتعزيز الحق في الخصوصية وحمايته، بما في ذلك في سياق المراقبة الداخلية والخارجية، واعتراض الاتصالات الرقمية وجمع البيانات الشخصية. وأشارت أيضاً إلى أن الممارسات في العديد من الدول كشفت عدم وجود تشريعات و/أو وسائل إنفاذ وطنية كافية، ووجود ضمانات إجرائية ضعيفة ورقابة غير فعالة، وكل ذلك أسهم في انعدام المساءلة عن التدخل التعسفي أو غير القانوني في الحق في الخصوصية. وشددت على أننا نجهل الكثير عن طبيعة عمليات المراقبة ومداها وأعربت عن قلقها بشأن ”الغياب المزعج للشفافية الحكومية المرتبطة بسياسات وقوانين وممارسات المراقبة، الذي يعيق أي جهود لتقييم اتساقها مع القانون الدولي لحقوق الإنسان ولضمان المساءلة“. (المرجع نفسه، الفقرة ٤٨). ودعت الدول إلى استعراض قوانينها وممارساتها الوطنية لضمان مطابقتها التامة للقانون الدولي لحقوق الإنسان وإلى إجراء التعديلات اللازمة حسب الاقتضاء. وأهابت بالمجتمع الدولي إجراء المزيد من الدراسات المعمقة للقضايا ذات الصلة (المرجع نفسه، الفقرتان ٤٩ و ٥١).

٢ - مكافحة الإرهاب هدف مشروع

٣٣ - على خلاف عدد من الحقوق المشروطة التي يحميها العهد، لا تعداد في المادة ١٧ للأهداف المشروعة في السياسة العامة التي يمكن أن تشكل أساساً لتبرير التدخل في الحق في الخصوصية. ولكن منع الأعمال الإرهابية وقمعها والتحقيق فيها هي بلا شك من الأهداف المشروعة لأغراض المادة ١٧. فالإرهاب يزعزع استقرار المجتمعات، ويهدد التنمية الاجتماعية والاقتصادية والسلامة الإقليمية للدول، ويقوّض السلام والأمن الدوليين. وبموجب المادة ٦ من العهد، تلتزم الدول التزاماً إيجابياً بحماية المواطنين وغيرهم ضمن ولايتها ضد الأعمال الإرهابية. ومن جوانب هذا الالتزام واجب إنشاء آليات فعالة لرصد المخاطر الإرهابية المحتملة قبل أن تصبح أفعالاً. وتقوم الدول بهذا الواجب من خلال تجميع المعلومات ذات الصلة وتحليلها من المخابرات ووكالات إنفاذ القانون وتحليلها.

٣٤ - ويُزعم أن تحسين قدرة الدول على رصد كامل الحركة عبر الإنترنت يكتسب أهمية خاصة في سياق مكافحة الإرهاب، لأن التواصل عبر الإنترنت كان له دور كبير في تمويل

أعمال الإرهاب الدولي وارتكابها؛ ولأن شبكة الإنترنت استخدمت لأغراض تجنيد المنظمات الإرهابية؛ وتحديد المتورطين في التخطيط أو التحريض على الإرهاب مقدماً يمكن عرقلته من خلال القيود المخابراتية. وبما أن الإرهاب هو نشاط عالمي، لا بد أن يتخطى تعقب المتورطين الحدود الوطنية. فمنع الإرهاب وقمعه هو واجب بالغ الأهمية للمصلحة العامة، ويمكن أن يشكل في المبدأ أساساً لتبرير مقنع للمراقبة الجماعية للإنترنت.

٣ - المراقبة الجماعية ونوعية الشروط القانونية

٣٥ - تنص المادة ١٧ من العهد صراحة على أن لكل فرد الحق في الحماية من التدخل غير المشروع أو التعسفي في خصوصيته. وهذا يفرض مواصفات ''لنوعية القانون'' ترتبط بثلاثة شروط: (أ) ينبغي للإجراء أن يستند إلى أساس في القانون المحلي؛ (ب) ينبغي للقانون المحلي أن يكون متوافقاً مع سيادة القانون ومقتضيات العهد؛ (ج) ينبغي أن تكون الأحكام ذات الصلة في القانون المحلي متاحة وواضحة ودقيقة. ولكن التدخل المسموح بموجب القانون المحلي يمكن أن يكون ''غير مشروع'' و/أو ''تعسفياً'' لأغراض المادة ١٧ إذا كان القانون المحلي لا يلبي الشروط الأساسية أي أنه غير متاح وغير دقيق ولا يمكن التنبّؤ بآثاره[٢٧]، لم يستوفِ القانون معايير الضرورة والتناسب[٢٨]. وينبغي للقانون المحلي إذاً أن يتضمن أحكاماً تكفل أن تكون القوى المراقبة المتدخلة مصمّمة لأغراض مشروعة ومحددة (انظر A/HRC/13/37، الفقرة ٦٠؛ و A/HRC/27/37، الفقرة ٢٨)، وتحمل ضمانات فعالة ضد الإساءة[٢٩]. ولا بد أيضاً من تقييد ممارسة السلطة التنفيذية التقديرية بوضوح معقول بموجب القانون المعمول به أو المبادئ التوجيهية المنشورة الملزمة[٣٠].

٣٦ - وليصير القانون المحلي متاحاً لا يكفي نشره، بل ينبغي أن يلبّي أيضاً معايير الوضوح والدقة الكافية لتمكين المتضررين من تنظيم سلوكهم على ضوء الظروف التي يمكن فيها أن تجري المراقبة التدخلية. وشددت اللجنة المعنية بحقوق الإنسان في الفقرة ٨ من تعليقها العام رقم ١٦، على أنه يجب للتشريعات التي تجيز بالتدخل في الاتصالات الخاصة ''أن تحدد

(٢٧) اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ١٦، الفقرة ٣.

(٢٨) المرجع نفسه، الفقرة ٨.

(٢٩) CCPR/C/USA/CO/4, para. 22; Malone v. United Kingdom, Application No. 8691/79, Judgment of 2 August 1984, paras. 67-68; and Weber and Saravia v. Germany, Application No. 54934/00, Judgment of 29 June 2006.

(٣٠) A/HRC/27/37, para. 29; and Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (see E/CN.4/1985/4, annex), paras. 16 and 18.

بالتفصيل الظروف التي يجوز السماح فيها بهذا التدخل''. وقبل إطلاق برامج المراقبة الجماعية المشار إليها في هذا التقرير، كان المفهوم من هذا النص أنه يتطلب تشريعات محلية تبيّن بوضوح الظروف التي في ظلها، والإجراءات التي بموجبها، يمكن أن يؤذن بأي تدخل؛ وفئات الأشخاص الذين يمكن اعتراض اتصالاتهم؛ وحدود مدة المراقبة؛ والإجراءات المتعلقة باستخدام البيانات المجموعة وتخزينها[٢٩]. وأكدت المحكمة الأوروبية لحقوق الإنسان الحاجة إلى القواعد المفصلة والواضحة بشأن هذا الموضوع[٣١].

٣٧ - وتشكل برامج المراقبة الجماعية تحدياً كبيراً لشروط الشرعية بموجب المادة ١٧ من العهد. وفي حين تستخدم برامج الوصول إلى البيانات بالجملة، لا قواعد تحدد فئات الأشخاص الذين يمكن أن يخضعوا للمراقبة، ولا حدود لمدة هذه المراقبة. ولذلك لا يمكن تحديد هذه الشروط في القوانين. وتبقى الأطر القانونية والإدارية المفصلة للمراقبة الجماعية في الكثير من الأحيان سريّة، ولا يعرف بشكل عام سوى القليل عن كيفية معالجة البيانات المسجلة. وعدد قليل جداً من الدول قام حتى الآن بسن التشريعات الأولية التي تسمح صراحة بمثل هذه البرامج. بدلاً من ذلك، طبقت قوانين محلية عفا عنها الزمن مصممة لمعالجة أشكال أولية من المراقبة على التكنولوجيا الرقمية الجديدة من دون أي تعديل لإدراج الإمكانات الكبيرة المتزايدة التي تستخدمها بعض الدول اليوم. وما يذكر أن بعض الدول ''تسعى عن قصد إلى تطبيق نظم ضمانات أقدم وأضعف على معلومات أكثر حساسية'' (انظر A/HRC/13/37، الفقرة ٥٧).

٣٨ - ويعتبر المقرر الخاص أنه من الضروري أن تعمل الدول على مراجعة القوانين الوطنية التي تنظم الأشكال الحديثة من المراقبة لضمان اتساقها مع القانون الدولي لحقوق الإنسان. وينبغي تحديث القوانين المحلية التي تنظم مراقبة الاتصالات بحيث تشمل الأشكال الحديثة للمراقبة الرقمية الأوسع نطاقاً، والتي تقتضي تدخلاً أعمق في المجال الخاص، مقارنة بما كان سائداً عند سن التشريعات المحلية السارية. ويؤدي غياب قوانين واضحة وحديثة إلى بيئة مهيأة لاحتمال حدوث أي تدخل تعسفي في الحق في الخصوصية من دون ضمانات مناسبة. والقوانين الواضحة والمفصلة ضرورية لكفالة الشرعية والتناسب في هذا الإطار، وهي سبيل لا غنى عنه لتمكين الأفراد من توقّع ما إذا كانت اتصالاتهم ستخضع للمراقبة، وفي أي ظروف.

٣٩ - وتتيح عملية تشريعية عامة فرصة لتبرر الحكومات تدابير المراقبة الجماعية للسكان. ويتيح النقاش المفتوح للرأي العام فهم التوازن بين الخصوصية والأمن (المرجع نفسه،

(٣١) Weber and Saravia v. Germany, Application No. 54934/00, Judgment 29 June 2006; Uzun v. Germany (2012) 54 EHRR 121 para. 35.

الفقرة ٥٦). وينبغي اعتماد نهج شفاف لوضع القوانين يحدّد مواطن الضعف الكامنة في نظم الاتصالات الرقمية، فيمكّن المستخدمين من اتخاذ القرارات استناداً إلى معلومات كافية. وهذا عنصر أساسي لضمان اليقين القانوني بموجب المادة ١٧ من العهد، بل إنه أيضاً وسيلة قيّمة لإشراك الرأي العام في المناقشات بشأن المواضيع التي تلقى اهتماماً على الصعيدين الوطني والدولي (انظر A/HRC/27/37، الفقرة ٢٩؛ و A/HRC/14/46). وحسب المقرر الخاص، عندما تكون الحقوق في الخصوصية للمجتمع الرقمي ككل خاضعة للتدخل المنهجي، فمن الشروط الأساسية التي لا غنى عنها تضمين التشريعات الأولية أحكاماً واضحة بهذا الشأن للوفاء بمبدأ الشرعية.

٤٠ - وعلى خلاف ذلك، أتاح استخدام التشريعات المفوّضة (صكوك نصتها السلطات التنفيذية بموجب صلاحيات مفوّضة لها) اعتماد أطر قانونية سرية للمراقبة الجماعية، ما قوّض قدرة السلطة التشريعية والقضائية والرأي العام على التدقيق في استخدام الصلاحيات الجديدة (انظر A/HRC/13/37، الفقرة ٥٤). وهذه الأحكام لا تستوفي المقتضيات القانونية في المادة ١٧ من العهد الدولي لأنها غير متاحة بما يكفي للجمهور (انظر CCPR/C/USA/CO/4) وقد تبرر بعض الأسباب المشروعة للمصلحة العامة الحفاظ على سريّة المواصفات الفنية والتشغيلية، غير أنها لا تبرر إخفاء المعلومات العامة بشأن طبيعة تدخل الدولة في الإنترنت ومدى هذا التدخل عن الرأي العام. ومن دون هذه المعلومات، من المستحيل تقدير مشروعية هذه التدابير وضرورتها وتناسبها. ولذلك ينبغي أن تتوخى الدول الشفافية إزاء طبيعة ونطاق المراقبة الجماعية للاتصالات (انظر A/HRC/23/40، الفقرة ٩١).

٤ - برامج المراقبة الجماعية التي تتجاوز الحدود الإقليمية

٤١ - يتمتع بعض الدول بالقدرة الفنية على المراقبة الجماعية للاتصالات بين الأفراد غير المقيمين في نطاق ولايتها، وقد أنشأت لذلك ترتيبات للمراقبة تتجاوز آثارها الحدود الإقليمية. وبعض هذه الأنشطة يجري مادياً في إقليم الدولة المعنية وتقوم بذلك على مبادئ الولاية القضائية الإقليمية بموجب العهد. ولا تقتصر هذه الحالة على الوكالات الحكومية التي تعترض البيانات عبر وضع أجهزة على كابلات الألياف الضوئية التي تمر ضمن ولايتها القضائية، بل تشمل أيضاً الحالات التي تمارس فيها الدولة سلطة تنظيمية على الاتصالات اللاسلكية أو تراقب الجهات المقدّمة لخدمات الإنترنت والتي تتحكم بالبيانات فعلياً (A/HRC/27/37، الفقرة ٣٤). وفي كلتا الحالتين، لا بد من توسيع نطاق حماية حقوق الإنسان لتشمل الذين يجري التدخل في خصوصيتهم، أكانوا موجودين فعلياً في البلد حيث مقدمو الخدمات أم لم يكونوا. وينطبق الأمر نفسه على الحالات التي يفرض فيها الاحتفاظ

الإلزامي بالبيانات التزامات على مقدمي الخدمات الموجودين ضمن إقليم الدولة أو ولايتها القضائية. وحتى عندما تخرق الدولة البنى التحتية الواقعة كلياً خارج الولاية القضائية الإقليمية، تبقى السلطات المعنية ملزمة بالتزامات الدولة بموجب العهد (المرجع نفسه، الفقرات من ٣٢ إلى ٣٥ والمصادر المذكورة فيها).

٤٢ - وتطرح عمليات المراقبة خارج الحدود الإقليمية تحديات خاصة على تطبيق ''نوعيّة القانون'' في المادة ١٧ من العهد. والتشريعات المحلية التي تحكم عمليات اعتراض الاتصالات الخارجية (الدولية) تؤمن عادة قدراً أقل من الحماية مقارنة بالأحكام التي تقتصر حمايتها على الاتصالات المحلية[٣٢]. وما يثير المزيد من القلق استمرار بعض الدول (بما فيها الولايات المتحدة الأمريكية) بالسماح بنظم الحماية غير المتكافئة للمواطنين وغير المواطنين. ويؤثر هذا الفرق في المعاملة على جميع الاتصالات الرقمية بما أن الرسائل عادة تحوّل عبر خوادم في ولايات قضائية أخرى. غير أن لذلك تشعبات مهمة خاصة باختراق الحوسبة السحابية[٣٣].

٤٣ - وأي شكل من أشكال المعاملة التفضيلية يتعارض مع مبدأ عدم التمييز بموجب المادة ٢٦ من العهد، وهو مبدأ في صلب مفهوم التناسب[٣٤]. ويثير استخدام برامج المراقبة الجماعية لمراقبة اتصالات الأشخاص من خارج ولاية دولة معيّنة تساؤلات جدية عن إمكانية الوصول إلى القانون الذي يحكم التدخل في حقوق الخصوصية والتنبؤ بآثاره، وعدم قدرة الأفراد على معرفة أنه يمكن أن يخضعوا للمراقبة أو اعتراض اتصالاتهم ضمن ولايات دول أخرى. ويعتبر المقرر الخاص أن الدول ملزمة قانوناً بتأمين الحماية نفسها للمواطنين وغير المواطنين، والموجودين ضمن حدود ولايتها أو خارجها.

---

(٣٢) حددت المفوضة السامية في تقريرها عدداً من هذه الأحكام مثل قانون مراقبة المخابرات الأجنبية، S1881(a) في الولايات المتحدة؛ والقانون المتعلق بتنظيم سلطات التحقيق لعام ٢٠٠٠، S8(4) في المملكة المتحدة؛ والقانون المتعلق بمكتب الأمن الحكومي لعام ٢٠٠٣، S.15A في نيوزيلندا؛ وقانون أجهزة المخابرات S.9 في أستراليا، وقانون الدفاع الوطني S.273.64(1) في كندا (انظر A/HRC/27/37، الفقرة ٣٥، الحاشية ٣٠).

(٣٣) European Parliament Directorate General for Internal Policies and Casper Bowden, "The US surveillance programmes and their impact on EU citizens' fundamental rights", 2013.

(٣٤) شددت اللجنة المعنية بحقوق الإنسان على أهمية ''اتخاذ تدابير لضمان توافق أي تدخل في حق الخصوصية مع مبادئ الشرعية والتناسب والضرورة، بصرف النظر عن جنسية أو موقع الأفراد الذين تخضع اتصالاتهم لمراقبة مباشرة''، CCPR/C/USA/CO/4، الفقرة ٢٢ (أ).

٥ - التعاون الدولي بين أجهزة المخابرات

٤٤ - تنشأ شواغل مماثلة متعلقة بترتيبات تبادل المعلومات المخابراتية على الصعيد الدولي. وقد ترك غياب القوانين المنظمة لتبادل المعلومات بين الدول الباب مفتوحاً لتتخذ أجهزة المخابرات ترتيبات ثنائية ومتعددة الأطراف سرية خارج نطاق إشراف أي سلطة مستقلة (انظر A/HRC/13/37). ويمكن تبادل المعلومات المتعلقة باتصالات فرد معيّن مع وكالات مخابراتية أجنبية خارج حماية أي إطار قانوني متاح علناً ومن دون ضمانات كافية. وعقب مشاورات موسّعة، وجدت المفوضة السامية لحقوق الإنسان مؤخراً معلومات موثوقة توحي بأن بعض الحكومات وجّهت بانتظام مهام جمع البيانات ومهام تحليلية عن طريق سلطات لديها ضمانات أضعف للخصوصية (انظر A/HRC/27/37، الفقرة ٣٠). ومثل هذه الممارسات، إذ تجعل عملية نظام المراقبة غير واضحة للمتأثرين بها، تتنافى بذلك مع المادة ١٧ من العهد.

٦ - الضمانات والإشراف

٤٥ - من أشكال الحماية الرئيسية التي تضمنها المادة ١٧ ارتباط نظم المراقبة السرية بالضمانات الإجرائية الكافية للحماية من التجاوزات[٢٩]. ويمكن أن تأخذ هذه الضمانات أشكالاً عدة، ولكنها عادة تشمل إذناً مسبقاً مستقلاً و/أو استعراضاً لاحقاً مستقلاً. وتتطلب أفضل الممارسات مشاركة السلطات التشريعية والتنفيذية والقضائية، إضافة إلى رقابة مدنية مستقلة (انظر A/HRC/27/37). ويمكن أن يؤدي غياب الضمانات الكافية إلى نقص في المساءلة حول التدخلات التعسفية أو غير القانونية في الحق في الخصوصية على الإنترنت (المرجع نفسه).

٤٦ - وحيث تستخدم برامج المراقبة المحددة الأهداف، تفرض الدول الحصول على إذن قضائي مسبق. والتدخل القضائي بموجب المعايير الدولية يشكّل ضمانة مهمة، على الرغم من وجود أدلة على أن درجة هذا التدقيق وفعاليته قد تراجعت في بعض البلدان بسبب الإحالة القضائية إلى السلطة التنفيذية (المرجع نفسه، الفقرة ٣٨). وفي دول أخرى مثل المملكة المتحدة، يعطي وزراء الحكومة أوامر التدخل الموجهة إلى أهداف محددة من دون إذن قضائي مسبق. ويقال إن هذا الأمر يبرره خضوع الوزراء للمساءلة القانونية من الناخبين. واستخدام الصلاحيات التنفيذية لهذه السلطات خاضع للمراجعة من مفوّض مستقل مختص بمراجعة اعتراض الاتصالات، ويمكن أن يقدم الأفراد شكاوى إلى هيئة قضائية، هي محكمة سلطات التحقيق، يخوّلها اختصاصها النظر في المعلومات السرية في مداولات مغلقة.

٤٧ - وفي إطار المراقبة المحددة الأهداف، أياً كانت طريقة الحصول على الإذن المسبق (قضائية أو تنفيذية)، ثمة فرصة على الأقل لاستعراض سابق لضرورة المراقبة التدخلية وتناسبها بالنظر إلى الظروف الخاصة بالحالة أو الفرد أو المنظمة التي ستخضع اتصالاتها للاعتراض. ولا تتاح هذه الفرص في خطط المراقبة الجماعية بما أنها لا تعتمد على الاشتباه بالفرد. ويقتصر الاستعراض السابق في هذه الحالة على الإذن بمواصلة العملية ككل، بدلاً من تطبيقه على فرد محدد. ويعتبر المقرر الخاص أن الدول التي تستخدم تكنولوجيا المراقبة الجماعية يجب أن تنشئ هيئات رقابة قوية ومستقلة تتمتع بما يكفي من الموارد ومكلفة بإجراء استعراضات سابقة لاستخدام تقنيات المراقبة التدخلية في ضوء شروط الشرعية والضرورة والتناسب بموجب المادة ١٧ من العهد (A/HRC/13/37، الفقرة ٦٢).

٤٨ - ويرتبط البعد الإجرائي الآخر للمادة ١٧ بشرط الاستعراض اللاحق لتدابير المراقبة التدخلية. وتفرض بعض الدول قيام مراجع مستقل برصد عملية المراقبة فيحلّل طريقة استخدامها ونطاقها ومبرراتها. وينبغي لمثل هذه الاستعراضات أن تشمل دائماً تحليلاً لمدى اتساق ممارسات الدولة مع شروط العهد الدولي.

٤٩ - وبالإضافة إلى هذا النوع من الاستعراض العام، يتوجب على الدول بشكل خاص التعويض للأفراد الذين يدعون أن الحقوق التي يكفلها لهم العهد الدولي قد انتهكت. وتلزم الفقرة ٣ (ب) من المادة ٢ من العهد الدول الأطراف بأن تكفل لكل فرد يطالب بالتعويض حقاً قابلاً للتنفيذ تحدده سلطة محلية قضائية أو إدارية أو تشريعية مختصة. وليصبح هذا الحق نافذاً، ينبغي أن ينص القانون المحلي على آلية مستقلة قادرة على إجراء استعراض شامل ومحايد، مع الوصول إلى جميع المواد ذات الصلة بمراعاة الأصول القانونية، يكون لها السلطة لفرض سبل الانتصاف الملزمة (بما في ذلك، عند الاقتضاء، أمر بوقف المراقبة أو تدمير المنتج) (انظر A/HRC/14/46؛ و A/HRC/27/37، الفقرة ٣٩).

٥٠ - ومن أجل الاحتجاج بالحق في التعويض، من الضروري أن يثبت الفرد أنه كان ضحية انتهاك. وفي إطار تدابير المراقبة السرية، قد يكون من الصعب أو من المستحيل الوفاء بهذا الشرط. فقليلة هي الدول التي وضعت أحكاماً تتطلب تزويد المشتبه به بإخطار لاحق بالمراقبة. وبناء على ذلك، خففت المحكمة الأوروبية لحقوق الإنسان من شرط أن يثبت الفرد أنه كان خاضعاً للمراقبة السرية. وقد ميّزت بين الشكاوى الموجهة ضد نظام يُزعم أنه لا يفي بشروط الاتفاقية الأوروبية لحقوق الإنسان، والشكاوى المتعلقة بحالات محددة من الأنشطة غير القانونية المرتكبة من الدولة. وفي الحالة الأولى، كُلّفت المحكمة بالنظر في

الأحكام المطعون فيها في الظاهر[٣٥]، أما في الحالة الثانية، فيطلب من مقدمي الدعاوى عادة إثباتهم ''احتمالاً معقولاً'' بأنهم تعرضوا للمراقبة غير القانونية[٣٦]. وفي ظل نظم المراقبة الجماعية، يرى المقرر الخاص أن مستخدمي الإنترنت ينبغي أن يكون لهم صفة للطعن في شرعية وضرورة وتناسب التدابير المتخذة.

٧ - الضرورة والتناسب في برامج المراقبة الجماعية

٥١ - ينبغي للدول أن تثبت أن أي تدخل في الحق في الخصوصية الذي تنص عليه المادة ١٧ من العهد هو وسيلة ضرورية لتحقيق غاية مشروعة. وينبغي في هذا الإطار وجود علاقة منطقية بين الوسيلة المعتمدة والهدف المنشود. كما ينبغي أن تكون الوسيلة المعتمدة الأقل تدخلاً من بين الوسائل التي يمكن أن تحقق النتيجة المنشودة (انظر CCPR/C/21/Rev.1/Add.9؛ و A/HRC/13/37 الفقرة ٦٠). ومبدأ التناسب في هذا الإطار يعني تحقيق التوازن بين مدى التدخل في حقوق الخصوصية على الإنترنت والفائدة المحددة التي ستعود على المصلحة العامة من التحقيقات التي تجريها أي سلطة عامة. ومع ذلك، تفرض قيود على مدى التدخل المسموح به في أي حق من الحقوق المشمولة بالعهد. وقد شددت لجنة حقوق الإنسان على أنه ''لا يجوز بأي حال من الأحوال فرض القيود أو الاحتجاج بها بطريقة تمسّ جوهر أي حق من الحقوق المشمولة بالعهد''[٣٧]. وفيما يتعلق بعمليات المراقبة السرية، شددت اللجنة على أن أي قرار باللجوء إلى التدخل في الاتصالات يجب أن تتخذه السلطة التي يسميها القانون، ''على أساس كل حالة على حدة''[٣٨]. وأي تدخل في الحق في الخصوصية يجب أن يكون معقولاً بالنسبة للظروف التي يحدث فيها[٣٩].

٥٢ - ولا ينسجم أي من هذه المبادئ مع استخدام الدول لتكنولوجيا المراقبة الجماعية. ولا شك في أن القدرة التقنية على تشغيل برامج لجمع كم كبير من المعلومات وتحليلها تؤمن وسيلة إضافية لمواصلة التحقيقات في مجال مكافحة الإرهاب وإنفاذ القانون. لكن يجب أن تُحسب أيضاً الأضرار التبعية التي تلحق بالحقوق في الخصوصية الجماعية عند تقييم مدى تناسب هذه البرامج. وبرامج جمع البيانات على نطاق جماعي تتنافى مع الشرط الذي يلزم

(٣٥) Klass v. Germany (1979-80) 2 EHRR 214.

(٣٦) Halford v. United Kingdom (1997) 24 EHRR 523.

(٣٧) لجنة حقوق الإنسان، التعليقان العامان رقم ٢٧ و ٣١.

(٣٨) لجنة حقوق الإنسان، التعليق العام رقم ١٦، الفقرة ٨.

(٣٩) لجنة حقوق الإنسان، التعليق العام رقم ١٦، الفقرة ٤. Van Hulst v. The Netherlands, Communication No. 903/1999, 2004, para 7.3; Toonen v. Australia, Communication No. 488/1992, para. 8.3.

أجهزة المخابرات باختيار الوسيلة الأقل تدخلاً في حقوق الإنسان (إلا إذا كانت الدول المعنية قادرة على إثبات أنها بحاجة إلى الوصول إلى جميع الاتصالات الجارية عبر الإنترنت لتأمين الحماية من تهديد الإرهاب وغيره من الجرائم الخطيرة). وبسبب عدم إمكانية إجراء تقييم للتناسب حسب كل حالة من الحالات قبل اختيار الأساليب التي ستعتمد، يمكن القول إن هذه البرامج تتنافى مع جوهر الحق في الخصوصية. فهي لا تترك مجالاً لإجراء التحليل ''على أساس كل حالة على حدة'' الذي اعتبرته لجنة حقوق الإنسان أساسياً، ويمكن بالتالي اعتبارها تعسفية، حتى لو كانت تخدم هدفاً مشروعاً واعتُمدت على أساس نظام قانوني في المتناول (انظرA/HRC/27/37 الفقرة ٢٥). وخلص المقرر الخاص، بناءً على ما تقدم، إلى أن هذه البرامج لا يمكن أن تتوافق مع المادة ١٧ من العهد إلا إذا كانت الدول المعنية قادرة على إثبات أن التدخل في حقوق الخصوصية على الإنترنت لعدد غير محدد من الناس الأبرياء في أي مكان في العالم ضروريٌّ للتصدي للخطر المحدد ومتناسب معه(٤٠).

٨ - قانون الاحتفاظ الإلزامي بالبيانات والاستخراج التلقائي لبيانات الاتصال والجهات المقدمة لخدمات الإنترنت

٥٣ - لا ينحصر استخدام برامج المراقبة الجماعية باعتراض محتوى الاتصالات. فالاتصالات الرقمية تضع في التداول كميات كبيرة من البيانات. وتتضمن بيانات الاتصال هذه (أو البيانات الفوقية) معلومات شخصية عن أفراد، وعن أماكنهم، ونشاطاتهم على شبكة الإنترنت. وقد اعتمدت العديد من الدول تشريعات تلزم الجهات المقدمة لخدمات الاتصالات والإنترنت بجمع بيانات الاتصال والاحتفاظ بها لإمكانية تحليلها في مرحلة لاحقة. وتتطلب هذه القوانين من الجهات المقدمة لهذه الخدمات تزويد السلطات بسجلات تخصيص عناوين بروتوكول الإنترنت، ما يمكّنها في أي وقت من تحديد هوية مستخدم عنوان محدد لبروتوكول الإنترنت. وقد أصبح الحصول على بيانات الاتصال تقنية قيّمة جداً في مجال المراقبة بالنسبة إلى الدول. ويسهل تخزين بيانات الاتصال والبحث فيها، ويمكن استخدامها في تجميع ملامح الأفراد التي تعتبر شديدة الخصوصية تماماً كمحتوى الاتصالات (انظر A/HRC/27/37، الفقرة ١٩). ومن خلال جمع وتصنيف المعلومات المستخلصة من بيانات الاتصال، يمكن تحديد مكان الفرد المعني وعلاقاته وأنشطته (انظر A/HRC/23/40، الفقرة ١٥). وفي غياب أي ضمانات خاصة، لن يسلم أي بعد سري من حياة الأفراد من

(٤٠) انظر A/HRC/27/37 الفقرة ٢٥، حيث بيّنت المفوضة السامية لحقوق الإنسان أنه ''لن يكون كافياً أن توجّه التدابير للبحث عن بعض الإبر في كومة من التبن؛ فالقياس المناسب هو أثر التدابير على كومة التبن، بالنسبة إلى الضرر الذي يهدّد بالوقوع؛ خاصةً ما إذا كان التدبير ضرورياً ومتناسباً''.

تحليل البيانات الفوقية[١]. لذلك، يمكن القول إن للاستخراج التلقائي للبيانات أثر سلبي على الخصوصية.

٥٤ - ولدى عدد كبير من الهيئات العامة في دول عدة إمكانية للوصول إلى بيانات الاتصال لأهداف متنوعة، وغالباً من دون توفر إذن قضائي أو رقابة مستقلة. ففي المملكة المتحدة على سبيل المثال، يسمح لأكثر من ٢٠٠ وكالة بالحصول على بيانات الاتصال بموجب قانون عام ٢٠٠٠ بشأن تنظيم السلطات المسؤولة عن التحقيق[٤١]، وقد بلغ عدد طلبات السلطات الرسمية على بيانات الاتصال ٦٠٨ ٥١٤ طلباً في عام ٢٠١٣ فقط[٤٢]. واعترفت المحاكم في فترة من الفترات بأن تسليم البيانات الفوقية لسلطة رسمية يشكل تدخلاً في الحق في الخصوصية، كما أشارت محكمة العدل الأوروبية مؤخراً إلى أن الاحتفاظ بالبيانات الفوقية المتعلقة بالحياة الشخصية لشخص ما واتصالاته يشكل بحد ذاته تدخلاً في هذا الحق[٤٣] (وإعطاء الإذن بالحصول على البيانات الفوقية المحفوظة بهدف تحليلها يشكل تدخلاً إضافياً مختلفاً)[٤٤]. وشددت محكمة العدل الأوروبية عندما توصلت إلى هذا الاستنتاج على أن البيانات الفوقية للاتصال تسمح بالتوصل إلى استنتاجات في غاية الدقة بشأن الحياة الخاصة للأشخاص الذين يُحتفظ ببياناتهم[٤٥].

٥٥ - وعند تطبيق النهج المعتمد لدى محكمة العدل الأوروبية، يصبح جمع بيانات الاتصال والاحتفاظ بها تدخلاً في الحق في الخصوصية، سواء أوصلت البيانات إلى سلطة عامة وحُلّلت أم لا. ولا يتطلب جمع بيانات الاتصال بموجب قانون الاحتفاظ الإلزامي بالبيانات ولا الكشف عنها لاحقاً للسلطات الرسمية (وتحليلها على يد هذه السلطات) وجود اشتباه أولي ضد أي فرد أو جماعة. وفي هذا الإطار، يشاطر المقرر الخاص التحفظات التي أعربت عنها المفوضة السامية في ما يتعلق بالضرورة والتناسب في قوانين الاحتفاظ الإلزامي بالبيانات (انظر A/HRC/27/37، الفقرة ٢٦).

---

(٤١) تتضمن قائمة الوكالات المخولة بالبحث في بيانات الاتصال السلطات الضريبية والوكالات الحكومية المحلية، ويمكن توسيعها بموجب التشريعات المفوضة (أوامر تنفيذية).

(٤٢) انظر www.intelligencecommissioners.com.

(٤٣) Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, para. 34.

(٤٤) المرجع نفسه، الفقرة ٣٥.

(٤٥) المرجع نفسه، الفقرات ٢٦ و ٢٧ و ٣٧.

٩ - تحديد الهدف

٥٦ - تفتقر العديد من الدول إلى أحكام ''تحديد الهدف'' التي تمنع استخدام المعلومات التي جمعت لهدف معين في أهداف أخرى لا علاقة للحكومة بها. ونتيجةً لذلك، يمكن تبادل البيانات التي جمعت لأهداف تتعلق ظاهرياً بالأمن القومي بين أجهزة المخابرات، وهيئات إنفاذ القانون، وغيرها من أجهزة الدولة، بما في ذلك السلطات الضريبية، والمجالس المحلية، وهيئات الترخيص(٤٦). وتستثنى وكالات الأمن القومي وإنفاذ القانون عادة من أحكام قانون حماية البيانات الذي يفرض قيوداً على تبادل البيانات الشخصية. ونتيجةً لذلك، يصعب على الأفراد معرفة متى يمكن أن يتعرضوا للمراقبة وأي وكالة حكومية يمكن أن تراقبهم. والخطر القائم في هذا اللغط هو احتمال انتهاك المادة ١٧ من العهد الدولي، إذ لا يمكن التكهن بآثار القوانين ذات الصلة، وتدابير المراقبة التي قد تكون ضرورية ومتناسبة لهدف واحد مشروع قد لا تكون كذلك لأغراض هدف آخر (المرجع نفسه، الفقرة ٢٧). وبناءً على ما تقدم، يؤيد المقرر الخاص توصية سلفه بضرورة إلزام الدول بتوفير أساس قانوني من أجل إعادة استخدام المعلومات الشخصية، وذلك وفقاً لمبادئ حقوق الإنسان (انظر A/HRC/13/37، الفقرة ٥٠ و ٦٦). ويعتبر ذلك ذا أهمية خاصة عندما يجري تبادل المعلومات عبر الحدود أو بين الدول.

١٠ - القطاع الخاص

٥٧ - يزداد اعتماد الدول على القطاع الخاص لتيسير المراقبة الرقمية. ولا يقتصر ذلك على تطبيق قانون الاحتفاظ الإلزامي بالبيانات. فالشركات تواطأت أيضاً وبشكل مباشر في تطوير وتطبيق تكنولوجيا الوصول إلى المعلومات من خلال تصميم هياكل أساسية للاتصالات تيسّر المراقبة الجماعية. وطُلب إلى الجهات المقدمة لخدمات الاتصالات والإنترنت ترك ثغرات في تكنولوجياتها للتأكد من جهوزيتها للتنصت. وقد رأت المفوضة السامية لحقوق الإنسان أن هذه الممارسات هي ''تفويض لعملية إنفاذ القانون ومسؤوليات شبه قضائية إلى وسطاء في مجال الإنترنت تحت ستار التنظيم الذاتي أو التعاون'' (انظر A/HRC/27/37، الفقرة ٤٢). ويوافق المقرر الخاص على هذا التقييم. ولتضمن الجهات المقدمة للخدمات أنها ليست شريكة في تجاوزات تتعلق بحقوق الإنسان، عليها أن تتأكد من

(٤٦) لتحليل الطرق التي جرى فيها استخدام المعلومات التي جمعت لغرض معيّن في تحقيق غرض آخر في المملكة المتحدة، انظر www.whatdotheyknow.com/request/127491/response/315758/attach/html/2Summay%20of%20Counsels%20advice.pdf.html

أن عملها يمتثل للمبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان التي أيدها مجلس حقوق الإنسان في عام ٢٠١١ (المرجع نفسه، الفقرات ٤٣-٤٦).

رابعا - الاستنتاجات والتوصيات

٥٨ - من التزامات الدول بموجب المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية احترام خصوصية الاتصالات الرقمية وأمنها. ويعني هذا الالتزام من حيث المبدأ أنه يحق للأفراد تبادل المعلومات والأفكار من دون تدخل من الدولة، ليقينهم أن اتصالهم سيصل إلى المرسل إليهم وحسب. والتدابير التي تتعارض مع هذا الحق يجب أن ينص عليها قانون محلي يكون دقيقاً وفي متناول الجميع، ولا يتعارض مع شروط العهد الدولي. كذلك يجب أن يكون اتخاذ هذه التدابير لتحقيق هدف مشروع وأن تستوفي معايير الضرورة والتناسب.

٥٩ - ويشكل منع الإرهاب وقمعه ضرورة قصوى تحتمها المصلحة العامة، ويمكن الاحتجاج به لتبرير عمليات المراقبة الجماعية للإنترنت. إلا أن النطاق التقني للبرامج الحالية واسع للغاية، ولا يتوافق مع المادة ١٧ من العهد إلا إذا كانت الدول المعنية قادرة على إثبات أن التدخل في حقوق الخصوصية على الإنترنت لعدد غير محدد من الناس الأبرياء في أي مكان في العالم ضروري للتصدي للخطر المحدد ومتناسب معه. وتكنولوجيا الوصول إلى البيانات بالجملة تمسّ بخصوصية الجميع على الإنترنت من دون تمييز، وتنتهك جوهر الحق الذي تضمنه المادة ١٧. وفي غياب أي إعفاء رسمي من التزامات الدول بموجب العهد، تبقى هذه البرامج انتهاكاً مباشراً ومتواصلاً لقاعدة راسخة من قواعد القانون الدولي.

٦٠ - ويتفق المقرر الخاص مع المفوضة السامية لحقوق الإنسان على الحاجة الملحة إلى قيام الدول التي تستخدم هذه التكنولوجيا بمراجعة تشريعاتها الوطنية وتحديثها، لضمان اتساقها مع القانون الدولي لحقوق الإنسان. وليس الهدف من ذلك الالتزام بالمادة ١٧ وحسب، بل أيضاً إتاحة فرصة هامة لإجراء نقاش مستنير يساهم في توعية الرأي العام ويمكّن الأفراد من اتخاذ خيارات مدروسة. وعندما تكون حقوق الخصوصية للمجتمع الرقمي بكامله مهددة، لا يمكن القبول بأقل من تشريع أولي مفصل وصريح. وينبغي فرض قيود ملائمة على الاستخدام الممكن للبيانات التي تم الحصول عليها، بحيث يطلب إلى السلطات العامة ذات الصلة تقديم أساس قانوني لإعادة استخدام المعلومات الشخصية.

٦١ - وعلى الدول إنشاء هيئات رقابة قوية ومستقلة وتزويدها بالتمويل وبالصلاحية لإجراء استعراضات مسبقة، من خلال النظر في طلبات الحصول على تراخيص ليس فقط على ضوء مقتضيات القانون المحلي، بل أيضاً على ضوء مقتضيات الضرورة والتناسب التي ينص عليها العهد. ويجب أن يحظى الأفراد بحق التماس وسيلة انتصاف فعالة في حال انتهاك حقوقهم في الخصوصية على الإنترنت. ويتطلب ذلك استحداث وسيلة يمكن من خلالها للأفراد المتضررين تقديم شكوى إلى آلية مستقلة قادرة على إجراء استعراض شامل وحيادي، وعلى الوصول إلى جميع المواد ذات الصلة، ومدعومة بضمانات كافية للقيام بالاجراءات القانونية الواجبة. ويمكن أن تتخذ آليات المساءلة أشكالاً عدة، لكن لا بد من أن يكون لديها الصلاحية لفرض سبل انتصاف ملزمة. وينبغي ألا تفرض الدول شروطاً تقوّض الحق في الانتصاف الفعلي.

٦٢ - ويتفق المقرر الخاص مع المفوضة السامية لحقوق الإنسان على أن الدول التي تخترق الهياكل الأساسية في مكان خارج ولايتها الإقليمية، تبقى مقيدة في هذا المكان بالتزاماتها بموجب العهد. وتحظر المادة ٢٦ من العهد أي تمييز لأي سبب، كالجنسية والمواطنة. وعلى ضوء ذلك، يرى المقرر الخاص أن الدول ملزمة قانوناً بتأمين المستوى نفسه من حماية الخصوصية للمواطنين وغير المواطنين، وللموجودين ضمن ولايتها وخارجها. وتشكل النظم غير المتماثلة في حماية الخصوصية انتهاكاً لشروط العهد.

٦٣ - ويدعو المقرر الخاص جميع الدول التي تستخدم تكنولوجيا المراقبة الرقمية الجماعية إلى أن تقدم للرأي العام تبريراً مفصلاً ومدعوماً بالأدلة لتدخلها المنهجي في الحق في الخصوصية للجماعات المستخدمة للإنترنت، بناءً على شروط المادة ١٧ من العهد. ويجب أن تعتمد الدول الشفافية في الإفصاح عن طبيعة ومدى اختراقها للإنترنت، والمنهجية التي تتبعها، وفي تبريرها لذلك، وأن تقدم للرأي العام بياناً مفصلاً بالفوائد الملموسة الناتجة من هذا الاختراق.

٦٤ - ويتفق المقرر الخاص مع سلفه (انظر **A/HRC/13/37**، الفقرة ١٩) ومع المقرر الخاص السابق المعني بتعزيز وحماية الحق في حرية الرأي والتعبير (انظر **A/HRC/23/40**، الفقرة ٩٨) على أنه ينبغي للجنة المعنية بحقوق الإنسان صياغة تعليق عام جديد بشأن الحق في الخصوصية على الإنترنت، يأخذ في الاعتبار التطورات في مراقبة الاتصالات الرقمية منذ اعتماد التعليق العام رقم ١٦ في عام ١٩٨٨.