الأمم المتحدة

A/HRC/27/37

الجمعية العامة

Distr.: General
30 June 2014
Arabic
Original: English

مجلس حقوق الإنسان

الدورة السابعة والعشرون

البندان ٢ و٣ من جدول الأعمال

التقرير السنوي لمفوضة الأمم المتحدة السامية لحقوق الإنسان وتقارير المفوضية 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

طلبت الجمعية العامة في قرارها ١٦٧/٦٨ إلى مفوضية الأمم المتحدة السامية لحقوق الإنسان أن تقدم إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين تقريراً عن حماية الخصوصية وتعزيزها في سياق المراقبة الداخلية والخارجية و/أو اعتراض الاتصالات الرقمية وجمع البيانات الشخصية، بما في ذلك على نطاق جماعي، وأن تدرج فيه آراء وتوصيات، لتنظر فيه الدول الأعضاء. ويُقدَّم هذا التقرير بناء على ذلك الطلب. وستقدم المفوضية أيضاً التقرير إلى الجمعية العامة في دورتها التاسعة والستين بناء على طلب الجمعية.

(A) GE.14-06869 050814 050814

1406869

المحتويات

أولاً- مقدمة

١- لقد أصبحت تكنولوجيا الاتصالات، مثل الإنترنت والهواتف الذكية النقالة والأجهزة العاملة بالاتصال اللاسلكي بالإنترنت، جزءاً من الحياة اليومية. وبإدخال تحسينات جذرية على إمكانية الوصول إلى المعلومات والاتصال الفوري، عززت الابتكارات في مجال تكنولوجيا الاتصالات حرية التعبير ويسرت النقاش العالمي ووطدت المشاركة الديمقراطية. وبتضخيم أصوات المدافعين عن حقوق الإنسان وتزويدهم بأدوات جديدة لتوثيق التجاوزات وكشفها، تَعِدُ هذه التكنولوجيات القوية بتحسين التمتع بحقوق الإنسان. وفي الوقت الذي أصبحت فيه وقائع الحياة المعاصرة تدور في الفضاء الإلكتروني أكثر من أي وقت مضى، أصبحت الإنترنت، في الوقت نفسه، موجودة في كل مكان وحميمية بشكل متزايد.

٢- وفي العصر الرقمي، عززت تكنولوجيا الاتصالات أيضاً قدرات الحكومات والمؤسسات والأفراد على القيام بأعمال المراقبة واعتراض الاتصالات وجمع البيانات. وكما لاحظ المقرر الخاص المعني بالحق في حرية التعبير والرأي، تعني أوجه التقدم التكنولوجي أن فعالية الدولة في القيام بعمل المراقبة لم تعد محدودة من حيث النطاق والمدة. وأدى انخفاض تكاليف التكنولوجيا وتخزين البيانات إلى القضاء على الروادع المالية والعملية للقيام بعمل المراقبة. وتملك الدول حالياً من القدرات أكثر من أي وقت مضى للقيام بعمل مراقبة متزامن واقتحامي ومحدد الهدف وواسع النطاق[(١)]. وبعبارة أخرى، فإن المنصات التكنولوجية التي تعتمد عليها الحياة السياسية والاقتصادية والاجتماعية العالمية بشكل متزايد ليست غير حصينة أمام المراقبة الجماعية فحسب، بل يمكن في الحقيقة أن تيسر هذه المراقبة.

٣- وقد أُعرِب عن قلق بالغ عند كشف سياسات وممارسات تستغل عدم حصانة تكنولوجيا الاتصالات الرقمية أمام المراقبة الإلكترونية واعتراض الاتصالات في جميع بلدان العالم. وتكاثرت أمثلة المراقبة الرقمية العلنية والسرية في ولايات قضائية حول العالم، وظهرت المراقبة الحكومية الجماعية كعادة خطيرة وليس تدبيراً استثنائياً. وتفيد التقارير بأن الحكومات هددت بحظر شركات خدمات الاتصالات والمعدات اللاسلكية ما لم تحصل على إمكانية الوصول المباشر إلى حركة الاتصالات، وتنصتت على كبلات الألياف البصرية لأغراض المراقبة، وطلبت من الشركات أن تكشف بانتظام معلومات بكميات كبيرة عن الزبائن والموظفين. وعلاوة على ذلك، تفيد التقارير بأن بعض هذه الحكومات استخدمت مراقبة شبكات الاتصالات لاستهداف أعضاء المعارضة السياسية و/أو المنشقين السياسيين. وتفيد بعض التقارير بأن السلطات في بعض الدول تسجل بشكل روتيني جميع المكالمات الهاتفية وتحتفظ بها لتحليلها، بينما أُبلِغ عن رصد حكومات مضيفة للاتصالات أثناء الأحداث

(١) A/HRC/23/40، الفقرة ٣٣.

العالمية. وتفيد التقارير بأن السلطات في إحدى الدول تشترط تجهيز جميع الحواسيب الشخصية التي تُباع في البلد ببرامجيات ترشيح يمكن أن تنطوي على قدرات مراقبة أخرى. وحتى الجماعات المسلحة غير الحكومية أصبحت الآن فيما يبدو تستحدث قدرات مراقبة رقمية متطورة. وقد بدأت تكنولوجيا المراقبة الجماعية حالياً تدخل السوق العالمية، مما يزيد من خطر إفلات المراقبة الرقمية من الضوابط الحكومية.

٤- وتضخمت بواعث القلق عقب ما كُشِف عنه في عامي ٢٠١٣ و٢٠١٤ من معلومات تفيد بأن وكالة الأمن القومي في الولايات المتحدة ومقر الاتصالات العامة في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية طورا معاً تكنولوجيات تسمح بالوصول إلى الكثير من حركة الإنترنت العالمية، وسجلات المكالمات في الولايات المتحدة، ودفاتر العناوين الإلكترونية للأفراد، وأحجام هائلة من محتوى الاتصالات الرقمية الأخرى. وتفيد التقارير بأن هذه التكنولوجيات نُشِرت عن طريق شبكة غير وطنية تشمل العلاقات الاستخباراتية الاستراتيجية بين الحكومات، والمراقبة التنظيمية للشركات الخاصة، والعقود التجارية.

٥- وبعد أن أعربت الدول الأعضاء وغيرها من الجهات ذات المصلحة عن قلقها إزاء الأثر السلبي لهذه الممارسات الرقابية على حقوق الإنسان، اعتمدت الجمعية العامة في كانون الأول/ديسمبر ٢٠١٣، دون تصويت، القرار ١٦٧/٦٨ بشأن الحق في الخصوصية في العصر الرقمي. وأكدت الجمعية في هذا القرار، الذي اشتركت في تقديمه ٥٧ دولة عضواً، أن حقوق الأشخاص خارج الفضاء الإلكتروني يجب أن تحظى بالحماية أيضاً في الفضاء الإلكتروني، وأهابت بجميع الدول أن تحترم وتحمي الحق في الخصوصية في الاتصالات الرقمية. وأهابت كذلك بجميع الدول أن تستعرض إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجمع البيانات الشخصية، مشددة على حاجة الدول إلى ضمان تنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان تنفيذاً كاملاً وفعالاً.

٦- وطلبت الجمعية العامة أيضاً، في قرارها ١٦٧/٦٨، إلى مفوضية الأمم المتحدة السامية لحقوق الإنسان أن تقدم إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين تقريراً عن حماية الخصوصية وتعزيزها في سياق المراقبة الداخلية والخارجية و/أو اعتراض الاتصالات الرقمية وجمع البيانات الشخصية، بما في ذلك على نطاق جماعي، وأن تدرج فيه آراء وتوصيات، لتنظر فيه الدول الأعضاء. ويُقدَّم هذا التقرير بناء على ذلك الطلب. وحسب التكليف الصادر بموجب القرار ١٦٧/٦٨، ستقدم المفوضية أيضاً التقرير إلى الجمعية العامة في دورتها التاسعة والستين.

ثانياً- المعلومات الأساسية والمنهجية

٧- شاركت المفوضية في عدد من الأحداث وجمعت معلومات من مجموعة واسعة من المصادر، مراعية في ذلك القرار ١٦٧/٦٨. وفي ٢٤ شباط/فبراير ٢٠١٤، قدمت المفوضة السامية عرضاً رئيسياً في حلقة دراسية للخبراء بشأن "الحق في الخصوصية في العصر الرقمي"، شاركت في رعايتها ألمانيا والبرازيل وسويسرا وليختنشتاين والمكسيك والنرويج والنمسا ويسرتها أكاديمية جنيف للقانون الدولي الإنساني وحقوق الإنسان.

٨- وفي الفترة من تشرين الثاني/نوفمبر ٢٠١٣ إلى آذار/مارس ٢٠١٤، أشركت المفوضية جامعة الأمم المتحدة في مشروع بحثي عن تطبيق القانون الدولي لحقوق الإنسان على النظم الوطنية التي تشرف على المراقبة الرقمية الحكومية. وتعرب المفوضية عن امتنانها للجامعة، وتقر بمساهمتها الموضوعية الرئيسية في إعداد هذا التقرير من خلال المشروع البحثي.

٩- وفي إطار مشاورة مفتوحة، وجهت المفوضية، في ٢٧ شباط/فبراير ٢٠١٤، استبياناً إلى الدول الأعضاء عن طريق بعثاتها الدائمة في جنيف ونيويورك؛ والمنظمات الدولية والإقليمية؛ والمؤسسات الوطنية لحقوق الإنسان؛ والمنظمات غير الحكومية؛ وكيانات الأعمال التجارية. ودعت المفوضية في بيانها إلى تقديم إسهامات بشأن القضايا التي تناولتها الجمعية العامة في قرارها ١٦٧/٦٨. وأُنشئت صفحة شبكية مكرسة تابعة للمفوضية لإتاحة الاستبيان وجميع الإسهامات ليطلع عليها الجمهور، وكذلك لإتاحة فرصة إضافية لتقديم الإسهامات. ووردت الإسهامات من ٢٩ دولة عضواً من جميع المناطق، ومن خمس منظمات دولية و/أو إقليمية، وثلاث مؤسسات وطنية لحقوق الإنسان، و١٦ منظمة غير حكومية، ومبادرتين من مبادرات القطاع الخاص[٢].

١٠- وأشار العديد من الإسهامات بالتفصيل إلى الأطر التشريعية الوطنية القائمة وإلى تدابير أخرى اتُّخِذت لضمان احترام الخصوصية في العصر الرقمي وحمايتها، وكذلك إلى مبادرات لإنشاء وتنفيذ ضمانات إجرائية ورقابة فعالة. وأشارت بعض الإسهامات إلى التحديات المواجهة في تنفيذ الحق في الخصوصية في العصر الرقمي، وقدمت اقتراحات لاتخاذ مبادرات على الصعيد الدولي. وتضمنت تشجيعاً للجنة المعنية بحقوق الإنسان لتحديث تعليقاتها العامة ذات الصلة، ولا سيما بشأن المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية؛ وقيام مجلس حقوق الإنسان بإنشاء ولاية إجراءات خاصة بشأن الحق في الخصوصية؛ و/أو إشراك المكلفين بولايات في إطار الإجراءات الخاصة الحالية ذات الصلة في مبادرات مشتركة أو فردية لمعالجة القضايا المتصلة بالحق في الخصوصية في سياق المراقبة الرقمية وتقديم توجيهات بشأن الممارسة الجيدة.

---

(٢) جميع الإسهامات متاحة على العنوان التالي: www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

١١- وبناء على الطلب الوارد في قرار الجمعية العامة ١٦٧/٦٨، يقدم هذا التقرير أفكاراً وتوصيات تستند إلى تقييم للمعلومات المتاحة وقت الصياغة، وتعتمد أيضاً على المواد الوافرة التي وردت في المجموعة المختلفة من الإسهامات المتلقاة.

ثالثاً- القضايا المتصلة بالحق في الخصوصية في العصر الرقمي

١٢- كما أشارت الجمعية العامة في قرارها ١٦٧/٦٨، يوفر القانون الدولي لحقوق الإنسان الإطار العالمي الذي يجب أن يُقيَّم على ضوئه أي تدخل في حقوق الخصوصية الفردية. وتنص المادة ١٢ من الإعلان العالمي لحقوق الإنسان على أنه "لا يُعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات." ووفقاً للمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، الذي صدقت عليه حتى تاريخه ١٦٧ دولة، "لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته." وتشير هذه المادة، علاوة على ذلك، إلى أن "من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس."

١٣- وتتضمن صكوك دولية أخرى لحقوق الإنسان أحكاماً مماثلة. وتعكس القوانين على الصعيدين الإقليمي والوطني أيضاً حق جميع الأشخاص في أن تُحترم حياتهم الخاصة وحياتهم العائلية وسكنهم ومراسلاتهم أو الحق في الاعتراف بكرامتهم أو سلامتهم الشخصية أو سمعتهم واحترامها. وبعبارة أخرى، هناك اعتراف عالمي بالأهمية الأساسية والصلة الوطيدة للحق في الخصوصية والحاجة إلى ضمان حماية هذا الحق في القانون والممارسة.

١٤- ورغم أن الولاية الخاصة بهذا التقرير ركزت على الحق في الخصوصية، فإن من الضروري التشديد على أن حقوقاً أخرى يمكن أيضاً أن تتأثر بالمراقبة الجماعية، واعتراض الاتصالات الرقمية، وجمع البيانات الشخصية. وتشمل هذه الحقوق الحق في حرية الرأي والتعبير، وفي التماس المعلومات وتلقيها وإذاعتها؛ والحق في حرية التجمع السلمي وتكوين الجمعيات؛ والحق في الحياة العائلية - وهي حقوق كلها ترتبط ارتباطاً وثيقاً بالحق في الخصوصية وتُمارس بشكل متزايد عن طريق الوسائط الرقمية. ويمكن أن تتأثر أيضاً بممارسات المراقبة الرقمية حقوق أخرى، مثل الحق في الصحة، مثلاً عندما يحجم أحد الأفراد عن التماس أو إبلاغ معلومات حساسة تتعلق بالصحة خوفاً من كشف هويته. وهناك دلالات موثوقة توحي بأن التكنولوجيا الرقمية استُخدِمت لجمع معلومات أدت بعد ذلك إلى التعذيب وغيره من سوء المعاملة. وتشير التقارير أيضاً إلى أن بيانات توصيفية مستمدة من المراقبة الإلكترونية جرى تحليلها لتحديد موقع أهداف ضربات فتاكة شنتها طائرات بدون طيار. ولا تزال هذه الضربات تثير مخاوف شديدة بشأن الامتثال للقانون الدولي لحقوق

الإنسان والقانون الدولي الإنساني، والمساءلة عن أي انتهاك لهما. ورغم أن الصلات بين المراقبة الجماعية وهذه الآثار على حقوق الإنسان تخرج عن نطاق هذا التقرير، فإنها تستحق مزيداً من الدراسة.

ألف- الحق في الحماية من التدخل التعسفي أو غير القانوني في الخصوصيات أو العائلة أو السكن أو المراسلات

١٥- شددت عدة إسهامات على أن مراقبة بيانات الاتصالات الإلكترونية يمكن أن تكون تدبيراً ضرورياً وفعالاً لإنفاذ القانون بصورة مشروعة أو لأغراض الاستخبارات عندما تُجرى بطريقة تمتثل للقانون، بما في ذلك القانون الدولي لحقوق الإنسان. غير أن المعلومات التي كُشِفت عن المراقبة الرقمية الجماعية أثارت أسئلة بشأن مدى اتساق هذه التدابير مع المعايير القانونية الدولية وما إذا كانت ثمة حاجة إلى ضمانات أقوى في مجال المراقبة للحماية من انتهاكات حقوق الإنسان. وبالتحديد، يجب ألا تتدخل تدابير المراقبة بطريقة تعسفية أو غير قانونية في خصوصية الفرد أو عائلته أو سكنه أو مراسلاته؛ ويجب أن تتخذ الحكومات تدابير محددة لضمان الحماية القانونية من هذا التدخل.

١٦- وكشف استعراض لمختلف الإسهامات الواردة أن معالجة هذه الأسئلة يتطلب تقييماً لما يشكل تدخلاً في الخصوصية في سياق الاتصالات الرقمية؛ ولمعنى "بطريقة تعسفية وغير قانونية"؛ ولمسألة من تحظى حقوقه بالحماية بموجب القانون الدولي لحقوق الإنسان وأين يتم ذلك. وتتناول الأجزاء التالية القضايا التي شددت عليها مختلف الإسهامات.

١- التدخل في الخصوصية

١٧- قدم كل من هيئات المعاهدات الدولية والإقليمية لحقوق الإنسان والمحاكم واللجان والخبراء المستقلين إرشادات ذات صلة فيما يخص نطاق ومحتوى الحق في الخصوصية، بما في ذلك معنى "التدخل" في خصوصية الفرد. وشددت اللجنة المعنية بحقوق الإنسان، في تعليقها العام رقم ١٦، على أن الامتثال للمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية يقتضي ضمان سلامة المراسلات وسريتها بحكم القانون وبحكم الواقع. وينبغي أن تُقدم المراسلات إلى الجهة المرسَل إليها دون أن يعترضها أحد ودون أن يفتحها أو يقرأها بطريقة أخرى"[(٣)].

١٨- وقد اقترح البعض أن نقل المعلومات الشخصية وتبادلها عن طريق الوسائل الإلكترونية جزء من تسوية واعية يقدم الأفراد بموجبها طواعية معلومات عن أنفسهم

(٣) *الوثائق الرسمية للجمعية العامة، الدورة الثالثة والأربعون، الملحق رقم ٤٠* (A/43/40)، المرفق السادس، الفقرة ٨.

وعلاقاتهم مقابل الوصول الرقمي إلى السلع والخدمات والمعلومات. ولكن تُثار أسئلة خطيرة عن مدى معرفة المستهلكين حقاً لأي بيانات يتقاسمونها، وكيف ومع من يتقاسمونها، وكيف ستُستخدَم. ووفقاً لأحد التقارير، "من حقائق البيانات الكبيرة أنها بمجرد أن تُجمع، يمكن أن يكون من الصعب جداً أن يبقى مصدرها مجهولاً. ورغم أن هناك جهوداً بحثية واعدة جارية لطمس المعلومات التي يمكن التعرف على هوية أصحابها شخصياً ضمن مجموعات كبيرة من البيانات، فإن جهوداً أكثر تقدماً بكثير تُبذل حالياً لتحدد من جديد هوية البيانات التي تبدو "مجهولة المصدر". والاستثمار الجماعي في القدرة على صهر البيانات أكبر بكثير من المرات من الاستثمار في التكنولوجيات التي ستعزز الخصوصية." وعلاوة على ذلك، لاحظ أصحاب التقرير أن "التركيز على مراقبة جمع البيانات الشخصية والاحتفاظ بها، مع أنه مهم، لا يمكن أن يبقى كافياً لحماية الخصوصية الشخصية"، وذلك جزئياً لأن "البيانات الضخمة تمكن من استخدامات جديدة وغير بديهية وقوية وغير متوقعة للبيانات"[٤].

١٩- وعلى نفس المنوال، اقتُرح أن اعتراض أو جمع البيانات المتعلقة باتصال ما، بالمقارنة مع محتوى الاتصال، لا يشكل لوحده تدخلاً في الخصوصية. وليس هذا التمييز مقنعاً من وجهة نظر الحق في الخصوصية. ويمكن أن يعطي تجميع المعلومات المشار إليه عادة بتسمية "البيانات التوصيفية" نظرة عن سلوك الفرد وعلاقاته الاجتماعية وأفضلياته الخاصة وهويته تتجاوز حتى تلك التي ينقلها الوصول إلى محتوى اتصال خاص. والبيانات التوصيفية للاتصالات، كما لاحظت محكمة العدل الأوروبية مؤخراً، "إذا أُخِذت ككل، يمكن أن تسمح بالتوصل إلى استنتاجات دقيقة بشأن الحياة الخاصة للأشخاص الذين احتُفِظ ببياناتهم"[٥]. وقد دفع الاعتراف بهذا التطور إلى مبادرات تدعو إلى إصلاح السياسات والممارسات القائمة لضمان حماية أقوى للخصوصية.

٢٠- ويستتبع ذلك أن أي التقاط لبيانات الاتصالات تدخل محتمل في الخصوصية، ويستتبع علاوة على ذلك أن جمع بيانات الاتصالات والاحتفاظ بها يُعد بمثابة تدخل في الخصوصية سواء أتم الاطلاع على تلك البيانات واستخدامها لاحقاً أم لا. وحتى مجرد احتمال التقاط معلومات الاتصالات ينشئ تدخلاً في الخصوصية[٦]، مع احتمال وجود أثر

---

(٤) المكتب التنفيذي لرئيس الولايات المتحدة الأمريكية، "البيانات الضخمة: اغتنام الفرص، والحفاظ على القيم"، أيار/مايو ٢٠١٤، (متاح على الموقع التالي: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)، الصفحة ٥٤.

(٥) محكمة العدل الأوروبية، الحكم الصادر في القضيتين المشتركتين C-293/12 وC-594/12، الحقوق الرقمية في أيرلندا وسايتلينغر وآخرون، الحكم المؤرخ ٨ نيسان/أبريل ٢٠١٤، الفقرات ٢٦-٢٧، و٣٧. وانظر أيضاً المكتب التنفيذي للرئيس، "Big Data and Privacy: A Technological Perspective" (متاح على الموقع الشبكي التالي: www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_may_2014.pdf)، الصفحة ١٩.

(٦) انظر المحكمة الأوروبية لحقوق الإنسان، ويبر وسارافيا، الفقرة ٧٨؛ *ومالون ضد المملكة المتحدة*، الفقرة ٦٤.

مخيف على الحقوق، بما فيها الحق في حرية التعبير والحق في تكوين الجمعيات. وهكذا فإن وجود برنامج مراقبة جماعية ينشئ في حد ذاته تدخلاً في الخصوصية. ويقع على الدولة عبء إثبات أن هذا التدخل ليس تعسفياً ولا غير قانوني.

٢- ماذا يعني مصطلح "تعسفي" أو "غير قانوني"؟

٢١- لا يجيز القانون الدولي لحقوق الإنسان التدخل في حق الفرد في الخصوصية إلا إذا لم يكن هذا التدخل تعسفياً ولا غير قانوني. وأوضحت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم ١٦ أن مصطلح "غير قانوني" يعني عدم إمكان حدوث أي تدخل "إلا في الحالات التي ينص عليها القانون. ولا يجوز أن يحدث التدخل الذي تأذن بها الدول إلا على أساس القانون، الذي يجب هو نفسه أن يكون متفقاً مع أحكام العهد ومراميه وأهدافه"[٧]. وبعبارة أخرى، فإن التدخل المسموح به بموجب القانون الوطني قد يكون مع ذلك "غير قانوني" إذا كان ذلك القانون الوطني يتضارب مع أحكام العهد الدولي الخاص بالحقوق المدنية والسياسية. ويمكن أن تتسع عبارة "التدخل التعسفي" لتشمل أيضاً التدخل المنصوص عليه بموجب القانون. وأوضحت اللجنة أن "المقصود بإدراج مفهوم التعسف هو ضمان أن يكون التدخل نفسه الذي يسمح به القانون موافقاً لأحكام العهد ومراميه وأهدافه وأن يكون، في جميع الحالات، معقولاً بالنسبة للظروف المعنية التي يحدث فيها"[٨]. وفسرت اللجنة مفهوم المعقولية على أنه يدل على أن "أي تدخل في الخصوصية يجب أن يتناسب مع الغرض المنشود، ويجب أن يكون ضرورياً في ظروف أي قضية معينة"[٩].

٢٢- وعلى خلاف بعض الأحكام الأخرى في العهد، لا تتضمن المادة ١٧ بنداً ينص على قيود صريحة. ومع ذلك، يمكن استخلاص إرشادات بشأن معنى نعتي "تعسفي أو غير قانوني" من مبادئ سيراكوزا المتعلقة بأحكام التقييد وعدم التقيّد الواردة في العهد الدولي الخاص بالحقوق المدنية والسياسية[١٠]؛ وممارسة اللجنة المعنية بحقوق الإنسان الواردة في تعليقاتها العامة، بما فيها التعليقات رقم ١٦ و٢٧ و٢٩ و٣٤ و٣١، والنتائج المتعلقة بالبلاغات الفردية[١١] والملاحظات الختامية[١٢]؛ والسوابق القضائية الإقليمية والوطنية[١٣]؛ وآراء الخبراء

---

(٧) *الوثائق الرسمية للجمعية العامة* (انظر الحاشية ٣)، الفقرة ٣.

(٨) المرجع نفسه، الفقرة ٤.

(٩) البلاغ رقم ١٩٩٢/٤٨٨، *تونان ضد أستراليا*، الفقرة ٨-٣؛ انظر أيضاً البلاغ رقم ١٩٩٩/٩٠٣، الفقرة ٧-٣ والبلاغ رقم ٢٠٠٦/١٤٨٢، الفقرتين ١٠-١ و١٠-٢.

(١٠) انظر E/CN.4/1985/4، المرفق.

(١١) مثلاً البلاغ رقم ١٩٩٩/٩٠٣، ٢٠٠٤، *فان هولست ضد هولندا*.

(١٢) CCPR /C/USA/CO/4.

(١٣) مثلاً، المحكمة الأوروبية لحقوق الإنسان، *أوزون ضد ألمانيا*، ٢ أيلول/سبتمبر ٢٠١٠، *ووبير وسورافيا ضد ألمانيا*، الفقرة ٤؛ ومحكمة البلدان الأمريكية لحقوق الإنسان، *إيشر ضد البرازيل*، الحكم، ٢٠ تشرين الثاني/نوفمبر ٢٠٠٩.

المستقلين[١٤]. وتنص اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم ٣١ بشأن طبيعة الالتزام القانوني العام الذي يقع على عاتق الدول الأطراف في العهد، مثلاً، على أن الدول الأطراف يجب أن تحجم عن انتهاك الحقوق المعترف بها في العهد، وأن "أية قيود تُفرض على تلك الحقوق يجب أن تكون مباحة بموجب الأحكام ذات الصلة من العهد. وعلى الدول، عند فرضها أية قيود من هذا القبيل، أن تقيم الدليل على ضرورتها وألا تتخذ من التدابير إلا ما يكون متناسباً مع السعي إلى تحقيق الأهداف المشروعة بغية ضمان حماية الحقوق المنصوص عليها في العهد حماية مستمرة وفعالة"[١٥]. وشددت اللجنة علاوة على ذلك على أنه "لا يجوز في أي حال فرض القيود أو التذرع بها على نحو يضر بجوهر تلك الحقوق."

٢٣- وتشير هذه المصادر الرسمية إلى المبادئ الأساسية المتمثلة في القانونية والضرورة والتناسبية، التي سُلِّط الضوء أيضاً على أهميتها في العديد من الإسهامات الواردة. وفي البداية، يجب أن ينص القانون على أي تقييد لحقوق الخصوصية الواردة في المادة ١٧ وأن يكون هذا القانون في المتناول وواضحاً ودقيقاً بما يكفي بحيث يمكن لأي فرد أن ينظر إلى القانون ويتأكد ممن يُؤذن له القيام بمراقبة البيانات وفي أي ظروف. ويجب أن يكون التقييد ضرورياً للتوصل إلى هدف مشروع، كما يجب أن يكون متناسباً مع الهدف وأن يكون أقل الخيارات اقتحاماً للحياة الخاصة[١٦]. وعلاوة على ذلك، يجب بيان أن التقييد المفروض على الحق (تدخل في الخصوصية، مثلاً، لأغراض حماية الأمن القومي أو حق الآخرين في الحياة) يحتمل أن يحقق ذلك الهدف. ويقع عبء إثبات أن للقيد علاقة بهدف مشروع على عاتق السلطات التي تسعى إلى تقييد الحق. وعلاوة على ذلك، يجب ألا يجرد أي تقييد للحق في الخصوصية جوهر الحق من معناه ويجب أن يكون متسقاً مع حقوق الإنسان الأخرى، بما فيها حظر التمييز. وعندما لا يستوفي التقييد هذه المعايير، سيكون التقييد غير قانوني و/أو يكون التدخل في الحق في الخصوصية تعسفياً.

٢٤- وغالباً ما تبرر الحكومات برامج مراقبة الاتصالات الرقمية بأسباب الأمن القومي، بما في ذلك المخاطر التي يشكلها الإرهاب. واقترحت عدة إسهامات أن المراقبة القانونية والمحددة الهدف للاتصالات الرقمية يمكن أن تشكل تدبيراً ضرورياً وفعالاً للاستخبارات و/أو هيئات إنفاذ القوانين عندما تُجرى وفقاً للقانون الدولي والمحلي ما دامت تكنولوجيات الاتصالات الرقمية يمكن أن يستخدمها الأفراد، بل استخدموها، لأهداف إجرامية (بما في ذلك تجنيد أشخاص لارتكاب أعمال إرهابية وتمويل هذه الأعمال وارتكابها). ويمكن أن تكون المراقبة لأسباب الأمن القومي أو لمنع الإرهاب أو غيره من الجرائم "هدفاً مشروعاً" لأغراض إجراء

(١٤) انظر A/HRC/13/37 وA/HRC/23/40. وانظر أيضاً المبادئ الدولية المتعلقة بتطبيق حقوق الإنسان على مراقبة الاتصالات، متاحة على الموقع الشبكي التالي: https://en.necessaryandproportionate.org/text.

(١٥) CCPR/C/21/Rev.1/Add.13، الفقرة ٦.

(١٦) CCPR/C/21/Rev.1/Add.9، الفقرات ١١-١٦. وانظر أيضاً A/HRC/14/46، المرفق، الممارسة ٢٠.

تقييم من وجهة نظر المادة ١٧ من العهد. ولكن درجة التدخل يجب أن تُقيَّم على أساس ضرورة التدبير المتخذ لتحقيق ذلك الهدف والفائدة الفعلية المتأتية منه نحو تحقيق هذا الغرض.

٢٥- وعند تقييم ضرورة تدبير معين، شددت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم ٢٧ على المادة ١٢ من العهد الدولي الخاص بالحقوق المدنية والسياسية على "عدم إعاقة جوهر الحق من جراء القيود [...]؛ ويجب ألا تُقلَب العلاقة بين الحق والقيد، بين القاعدة والاستثناء"[١٧]. وأوضحت اللجنة كذلك أنه "لا يكفي أن تخدم القيود الأغراض المسموح بها؛ فيجب أيضاً أن تكون ضرورية لحمايتها." وعلاوة على ذلك، يجب أن تكون هذه التدابير متناسبة: "أقل الوسائل تدخلاً مقارنة بغيرها من الوسائل التي يمكن أن تحقق النتيجة المنشودة"[١٨]. وعندما يكون هناك هدف مشروع وضمانات مناسبة، يمكن أن يُسمَح لدولة ما أن تباشر مراقبة اقتحامية جداً؛ ولكن يقع على الحكومة عبء إثبات أن التدخل ضروري للتصدي للخطر المحدد ومتناسب معه. ومن ثم يمكن أن تُعتبَر برامج المراقبة الجماعية أو "بالجملة" تعسفية، حتى وإن كانت تخدم هدفاً مشروعاً واعتُمِدت على أساس نظام قانوني في المتناول. وبعبارة أخرى، لن يكون كافياً أن تُوجّه التدابير للبحث عن بعض الإبر في كومة من التبن؛ فالقياس المناسب هو أثر التدابير على كومة التبن، بالنسبة إلى الضرر الذي يهدد بالوقوع؛ خاصة ما إذا كان التدبير ضرورياً ومتناسباً.

٢٦- والشواغل المتعلقة بما إذا كان الوصول إلى البيانات واستخدامها مصممين لأهداف مشروعة محددة أيضاً تثير أيضاً أسئلة بشأن زيادة اعتماد الحكومات على الجهات الفاعلة في القطاع الخاص للاحتفاظ بالبيانات "في حالة ما إذا" دعت إليها الحاجة لأغراض حكومية. ولا يبدو من الضروري ولا من المتناسب الاحتفاظ بالبيانات لدى أطراف ثالثة إلزاماً، وهي سمة متكررة لنظم المراقبة في العديد من الدول، حيث تقتضي الحكومات من شركات الهاتف ومقدمي خدمات الإنترنت أن تخزن بيانات توصيفية عن اتصالات زبائنها وموقعهم لتصل إليها في وقت لاحق هيئات إنفاذ القانون وأجهزة المخابرات[١٩].

٢٧- ويتمثل أحد العوامل التي يجب النظر فيها عند تحديد التناسبية فيما تؤول إليه البيانات بالجملة ومن يمكن أن يصل إليها بعد جمعها. ويفتقر العديد من الأطر الوطنية إلى "القيود على الاستخدام"، وتسمح هذه الأطر بدلاً من ذلك بجمع البيانات لهدف واحد مشروع، ولكنها تسمح باستخدامها لاحقاً لأهداف أخرى. وتفاقم عدم وجود قيود فعالة على الاستخدام

---

(١٧) CCPR/C/21/Rev.1/Add.9، الفقرات ١١-١٦. وانظر أيضاً المحكمة الأوروبية لحقوق الإنسان، *هانديساید ضد المملكة المتحدة*، الفقرة ٤٨، *وكلاس ضد ألمانيا*، الفقرة ٤٢.

(١٨) CCPR/C/21/Rev.1/Add.9، الفقرات ١١-١٦.

(١٩) انظر رأي المحامي العام لمحكمة العدل الأوروبية كروز فيلالون في القضيتين المشتركتين C-293/12 وC-594/12، الصادر في ١٢ كانون الأول/ديسمبر ٢٠١٣، الذي اقترح فيه أن التوجيه 2006/24/EU (بشأن الاحتفاظ بالبيانات المولدة أو المجهزة فيما يتعلق بتوفير خدمات الاتصالات الإلكترونية) ينتهك "في مجمله" ميثاق الحقوق الأساسية للاتحاد الأوروبي لأنه لا يفرض حدوداً صارمة على هذا الاحتفاظ بالمعلومات. وانظر أيضاً CCPR/C/USA/CO/4، الفقرة ٢٢.

منذ ١١ أيلول/سبتمبر ٢٠١١ إذ طُمِست الحدود بين العدالة الجنائية والأمن القومي كثيراً. والخطر القائم هو أن ما نتج عن ذلك من تقاسم للبيانات بين هيئات إنفاذ القانون وأجهزة المخابرات وغيرها من أجهزة الدولة قد ينتهك المادة ١٧ من العهد لأن تدابير المراقبة التي قد تكون ضرورية ومتناسبة لهدف واحد مشروع قد لا تكون كذلك لأغراض هدف آخر. وتبين من استعراض للممارسة الوطنية في وصول الحكومات إلى بيانات الأطراف الثالثة أن "توسيع حرية تقاسم المعلومات بين الوكالات واستخدامها لأغراض تتجاوز الأغراض التي جُمعت لأجلها يشكل إضعافاً كبيراً لتدابير الحماية التقليدية للبيانات عندما يُضاف إلى السهولة الكبيرة التي يمكن بها لوكالات الأمن القومي وهيئات إنفاذ القانون من الوصول إلى بيانات القطاع الخاص في المقام الأول"[٢٠]. وفي عدة دول، أبطلت المراجعة القضائية نظم تقاسم البيانات على هذا الأساس. واقترحت أخرى أن فرض هذه القيود على الاستخدام ممارسة جيدة لضمان فعالية وفاء الدولة بالتزاماتها بموجب المادة ١٧ من العهد[٢١]، مع فرض عقوبات هامة على انتهاكها.

باء- حماية القانون

٢٨- تنص الفقرة ٢ من المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية صراحة على أن لكل شخص الحق في أن يحميه القانون من التدخل غير القانوني أو التعسفي في خصوصيته. ويعني ذلك وجوب تطبيق أي برنامج لمراقبة الاتصالات على أساس قانون يكون بإمكان الجمهور أن يصل إليه ويجب أن يتوافق هذا القانون بدوره مع النظام الدستوري الخاص بالدولة ومع القانون الدولي لحقوق الإنسان[٢٢]. ولا تقتضي "إمكانية الوصول" نشر القانون فحسب، بل أن يكون دقيقاً بما يكفي لتمكين الشخص المتأثر من تنظيم تصرفاته، مع تبصُّر الآثار التي يمكن أن تترتب عن عمل معين. ويجب أن تضمن الدولة أن أي تدخل في الحق في الخصوصية أو العائلة أو السكن أو المراسلات جائز بموجب قوانين (أ) يمكن أن يصل إليها عامة الجمهور؛ (ب) تتضمن أحكاماً تضمن أن عمليات جمع البيانات والوصول إليها واستخدامها مصممة لأهداف مشروعة محددة؛ (ج) دقيقة بما يكفي وتحدد بالتفصيل الظروف الدقيقة التي يمكن السماح فيها بأي تدخل من هذا النوع، وإجراءات إصدار الإذن، وفئات الأشخاص الذين يمكن وضعهم تحت المراقبة، وحدود مدة

(٢٠) انظر المرجع التالي: Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, "Systematic government access to private-sector data", *International Data Privacy Law*, vol. 2, No. 4, 2012, p. 198.

(٢١) انظر A/HRC/14/46، المرفق، الممارسة ٢٣.

(٢٢) المرجع نفسه، المرفق.

المراقبة، وإجراءات استخدام البيانات المجموعة وتخزينها؛ (د) تنص على ضمانات فعالة ضد التجاوزات[٢٣].

٢٩- لذلك فإن القواعد السرية والتفسيرات السرية للقانون - حتى التفسيرات القضائية السرية - لا تتمتع بصفات "القانون" الضرورية[٢٤]. كما لا تتمتع بهذه الصفات القوانين أو القواعد التي تعطي السلطات التنفيذية، مثل الدوائر الأمنية والاستخباراتية، سلطة تقديرية مفرطة؛ ويجب الإشارة بوضوح معقول (في القانون نفسه أو في مبادئ توجيهية ملزمة منشورة) إلى نطاق وطريقة ممارسة السلطة التقديرية الرسمية الممنوحة. وأي قانون يمكن الوصول إليه ولكن لا يمكن التنبؤ بآثاره لن يكون ملائماً. وتكون الطبيعة السرية لسلطات مراقبة محددة مصحوبة بمزيد من خطر الممارسة التعسفية للسلطة التقديرية التي تقتضي بدورها مزيداً من الدقة في القاعدة التي تنظم ممارسة السلطة التقديرية ومزيداً من الرقابة. وتشترط عدة دول أيضاً أن يُنشأ الإطار القانوني عن طريق تشريعات أولية تُناقش في البرلمان بدلاً من مجرد لوائح ثانوية تسنها السلطة التنفيذية - وهو شرط يساعد على ضمان أن الإطار القانوني لا يمكن أن يصل إليه الجمهور المعني بعد اعتماده فحسب، بل أيضاً خلال إعداده، وفقاً للمادة ٢٥ من العهد الدولي الخاص بالحقوق المدنية والسياسية[٢٥].

٣٠- ويكون شرط إمكانية الوصول ذا صلة أيضاً عند تقييم الممارسة الناشئة التي تستعين فيها الدول بجهات أخرى في مهام المراقبة. وثمة معلومات موثوقة توحي بأن بعض الحكومات وجّهت بانتظام مهام جمع البيانات ومهام تحليلية عن طريق ولايات قضائية لديها ضمانات أضعف للخصوصية. وتفيد التقارير بأن بعض الحكومات شغّلت شبكة عبر وطنية لوكالات الاستخبارات من خلال ربط ثغرات قانونية، تنطوي على تنسيق ممارسة المراقبة لاجتناب تدابير الحماية التي تنص عليها النظم القانونية المحلية. ويمكن القول إن هذه الممارسة لا تجتاز اختبار المشروعية لأنها، كما أشارت إلى ذلك بعض الإسهامات في هذا التقرير، تجعل تشغيل نظام المراقبة غير قابل للتنبؤ بالنسبة لمن يتأثرون به. ويمكن أن تقوض جوهر الحق المحمي بموجب المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، ومن ثم تحظرها المادة ٥ من هذا العهد. وأخفقت الدول أيضاً في اتخاذ تدابير فعالة لحماية الأفراد داخل ولايتها القضائية من ممارسات المراقبة غير القانونية من جانب دول أو كيانات تجارية أخرى، وذلك في انتهاك لالتزاماتها في مجال حقوق الإنسان.

---

(٢٣) CCPR /C/USA/CO/4، الفقرة ٢٢. وانظر أيضاً المحكمة الأوروبية لحقوق الإنسان، *مالون ضد المملكة المتحدة*، رقم ٧٩/٨٦٩١، ٢ آب/أغسطس ١٩٨٤، الفقرتان ٦٧ و٦٨، *وويبر وسارافيا ضد ألمانيا*، الطلب رقم ٥٤٩٣٤٠٠، ٢٩ حزيران/يونيه ٢٠٠٦، الذي تعدد فيه المحكمة الضمانات الدنيا التي ينبغي تحديدها في القانون التشريعي.

(٢٤) انظر CCPR /C/USA/CO/4، الفقرة ٢٢.

(٢٥) انظر أيضاً A/HRC/14/46.

جيم- من يحظى بالحماية ومتى؟

٣١- تناول عدد من الإسهامات التي وردت مسألة تطبيق العهد الدولي الخاص بالحقوق المدنية والسياسية على المراقبة الرقمية خارج الحدود الإقليمية. ورغم أن من الواضح أن بعض جوانب برامج المراقبة التي كُشف عنها مؤخراً مثلاً ستحرك الالتزامات الإقليمية للدولة التي تقوم بالمراقبة، فقد أُعرب عن شواغل إضافية فيما يتعلق بالمراقبة خارج الحدود الإقليمية واعتراض الاتصالات.

٣٢- وتقتضي المادة ٢ من العهد الدولي الخاص بالحقوق المدنية والسياسية من كل دولة طرف أن تحترم الحقوق المعترف بها في العهد وتكفلها لجميع الأشخاص الموجودين في إقليمها والداخلين في ولايتها، دون تمييز بسبب العرق، أو اللون، أو الجنس، أو اللغة، أو الدين، أو الرأي سياسيا أو غير سياسي، أو الأصل القومي أو الاجتماعي، أو الثروة، أو النسب، أو غير ذلك من الأسباب. وأكدت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم ٣١ أن الفقرة ١ من المادة ٢ تقتضي من الدول الأطراف أن تحترم وتكفل الحقوق الواردة في العهد لجميع الأشخاص الذين قد يوجدون في إقليمها ولجميع الأشخاص الداخلين في ولايتها. ويعني ذلك أن على الدولة أن تحترم وتكفل الحقوق المنصوص عليها في العهد لأي شخص يوجد تحت سلطة تلك الدولة الطرف أو تحت مراقبتها الفعلية، حتى وإن لم يكن يوجد داخل إقليم الدولة الطرف[٢٦]. ويتسع ذلك ليشمل الأشخاص الواقعين تحت "سلطتها"[٢٧].

٣٣- وقد استرشدت اللجنة المعنية بحقوق الإنسان، كما عبرت عن ذلك حتى في آرائها السابقة، بالمبدأ القائل إنه لا يمكن لأي دولة أن تتجنب التزاماتها الدولية في مجال حقوق الإنسان باتخاذ إجراءات خارج إقليمها يكون محظوراً عليها اتخاذها "في أرض الوطن"[٢٨]. ويتوافق هذا الموقف مع آراء محكمة العدل الدولية، التي أكدت أن العهد الدولي الخاص بالحقوق المدنية والسياسية ينطبق فيما يخص الأعمال التي تقوم بها الدولة "عند ممارستها لولايتها خارج إقليمها الخاص"[٢٩]، وكذلك مع المادتين ٣١ و٣٢ من اتفاقية فيينا لقانون

---

(٢٦) CCPR/C/21/Rev.1/Add.13، الفقرة ١٠.

(٢٧) انظر *الوثائق الرسمية للجمعية العامة، الدورة السادسة والثلاثون، الملحق رقم ٤٠* (A/36/40)، المرفق التاسع عشر، الفقرة ١٢-٢؛ وانظر أيضاً المرفق العشرين. وانظر أيضاً CCPR/CO/78/ISR، الفقرة ١١، وCCPR/CO/72/NET، الفقرة ٨، وCCPR/CO/81/BEL، الفقرة ٦، ولجنة البلدان الأمريكية لحقوق الإنسان، *كورد وآخرون ضد الولايات المتحدة*، القضية رقم ١٠-٩٥١، التقرير رقم ٩٩/١٠٩، ٢٩ أيلول/سبتمبر ١٩٩٩، الفقرات ٣٧ و٣٩ و٤١ و٤٣.

(٢٨) انظر *الوثائق الرسمية للجمعية العامة، الدورة السادسة والثلاثون*، (انظر الحاشية ٢٧)، المرفق التاسع عشر، الفقرتان ١٢-٢ و١٢-٣؛ والمرفق العشرين، الفقرة ١٠-٣.

(٢٩) انظر فتوى محكمة العدل الدولية بشأن *الآثار القانونية الناشئة عن تشييد جدار في الأرض الفلسطينية المحتلة*، المؤرخة ٩ تموز/يوليه ٢٠٠٤ (A/ES-10/273 وCorr.1)، الفقرات ١٠٧-١١١. وانظر أيضاً محكمة العدل

المعاهدات. ويدل مفهوما "السلطة" و"المراقبة الفعلية" عما إذا كانت الدولة تمارس "الولاية القضائية" أو السلطات الحكومية، التي يُقصد من تدابير حماية حقوق الإنسان تقييد إساءة استعمالهما. ولا يمكن لأي دولة أن تتجنب مسؤولياتها في مجال حقوق الإنسان بمجرد الإحجام عن جعل تلك السلطات في حدود القانون. والقيام باستنتاج آخر لن يقوض عالمية وجوهر الحقوق المحمية بموجب القانون الدولي لحقوق الإنسان فحسب، بل يمكن أيضاً أن ينشئ حوافز هيكلية للدول للتعاقد الخارجي مع بعضها البعض بشأن المراقبة.

٣٤- ويُفهم من ذلك إذن أن المراقبة الرقمية يمكن أن توجب وفاء دولة ما بالتزاماتها في مجال حقوق الإنسان إذا كانت تلك المراقبة تشمل ممارسة الدولة للسلطة أو مراقبتها الفعلية فيما يتعلق بالهياكل الأساسية للاتصالات الرقمية، سواء كان ذلك مثلاً من خلال التنصت المباشر أو اختراق تلك الهياكل الأساسية. وبالمثل، عندما تمارس الدولة الولاية التنظيمية على طرف ثالث يتحكم مادياً في البيانات، يكون لتلك الدولة أيضاً التزامات بموجب العهد. وإذا سعى بلد ما إلى تأكيد ولايته على بيانات الشركات الخاصة كنتيجة لتأسيس تلك الشركات في ذلك البلد، فإن تدابير حماية حقوق الإنسان يجب أن تُوسع لتشمل أولئك الذين يتم التدخل في خصوصيتهم، سواء في بلد التأسيس أو خارجه. ويصح ذلك سواء كانت ممارسة تلك الولاية قانونية أو لم تكن كذلك في المقام الأول، أو كانت تنتهك في الحقيقة سيادة دولة أخرى.

٣٥- وهذا الاستنتاج مهم كذلك في ضوء المناقشات الجارية بشأن ما إذا كان "الأجانب" و"المواطنون" ينبغي أن يستفيدوا على قدم المساواة من تدابير حماية الخصوصية في إطار النظم الوطنية للإشراف على المراقبة الأمنية. وتميز نظم قانونية عدة بين التزامات دولة ما تجاه مواطنيها أو داخل أقاليمها والتزاماتها تجاه غير مواطنيها ومن هم في الخارج[٣٠]، أو تقدم فيما عدا ذلك اتصالات أجنبية أو خارجية ذات مستويات حماية أدنى. وإذا كان هناك شك بشأن ما إذا كانت البيانات أجنبية أو محلية، غالباً ما ستتعامل وكالات المخابرات مع البيانات على أنها أجنبية (إذ إن الاتصالات الرقمية تمر بانتظام إلى "الخارج" في لحظة من اللحظات) ومن ثم تسمح بجمعها والاحتفاظ بها. وتكون النتيجة حماية أضعف بكثير - أو حتى منعدمة - لخصوصية الأجانب وغير المواطنين، بالمقارنة مع حماية المواطنين.

٣٦- والقانون الدولي لحقوق الإنسان صريح فيما يخص مبدأ عدم التمييز. وتنص المادة ٢٦ من العهد الدولي الخاص بالحقوق المدنية والسياسية على أن "الناس جميعا سواء أمام

الدولية، قضية *الأنشطة المسلحة على إقليم الكونغو* (جمهورية الكونغو الديمقراطية ضد أوغندا)، الحكم، ٢٠٠٥، الصفحة ١٦٨.

(٣٠) انظر مثلاً، في الولايات المتحدة، قانون مراقبة المخابرات الأجنبية S1881(a)، وفي المملكة المتحدة، القانون المتعلق بتنظيم سلطات التحقيق لعام ٢٠٠٠، S8(4)؛ وفي نيوزيلندا، القانون المتعلق بمكتب الأمن الحكومي لعام ٢٠٠٣، S.15A؛ وفي أستراليا، قانون أجهزة المخابرات S.9؛ وفي كندا، قانون الدفاع الوطني، S.273.64(1).

القانون ويتمتعون دون أي تمييز بحق متساو في التمتع بحمايته. وفي هذا الصدد يجب أن يحظر القانون أي تمييز وأن يكفل لجميع الأشخاص على السواء حماية فعالة من التمييز لأي سبب، كالعرق أو اللون أو الجنس أو اللغة أو الدين أو الرأي سياسيا أو غير سياسي، أو الأصل القومي أو الاجتماعي، أو الثروة أو النسب، أو غير ذلك من الأسباب". ويجب قراءة هذه الأحكام مع المادة ١٧ التي تنص على أنه "لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته" وأن "من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"، وكذلك الفقرة ١ من المادة ٢. وفي هذا الصدد، 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"[٣١].

دال- الضمانات الإجرائية والرقابة الفعالة

٣٧- تنص الفقرة ٢ من المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية على أن لكل شخص الحق في أن يحميه القانون من التدخل في الخصوصيات أو المساس غير القانوني أو التعسفي. ويجب تفعيل "حماية القانون" من خلال ضمانات إجرائية فعالة، بما في ذلك ترتيبات مؤسسية فعالة تُرصد لها موارد كافية. ولكن من الواضح أن عدم وجود رقابة فعالة أسهم في انعدام المساءلة عن حالات الاقتحام التعسفي أو غير القانوني في الحق في الخصوصية في البيئة الرقمية. وقد أثبتت الضمانات الداخلية دون رصد خارجي مستقل على الخصوص عدم فعاليتها ضد أساليب المراقبة غير القانونية أو التعسفية. ورغم أن هذه الضمانات يمكن أن تأتي في أشكال شتى، فإن مشاركة جميع فروع الحكومة في الإشراف على برامج المراقبة، وكذلك وكالة رقابة مدنية مستقلة، أمر ضروري لضمان حماية قانونية فعالة.

٣٨- ومن شأن مشاركة قضائية تستوفي المعايير الدولية المتصلة بالاستقلالية والحياد والشفافية أن تساعد على ترجيح استيفاء النظام القانوني العام للمعايير الدنيا التي يقتضيها القانون الدولي لحقوق الإنسان. وفي الوقت نفسه، ينبغي عدم النظر إلى المشاركة القضائية في الرقابة على أنها دواء شامل؛ ففي العديد من البلدان، لم يعدُ التفويض أو الاستعراض القضائي لأنشطة المراقبة الرقمية التي تضطلع بها وكالات الاستخبارات و/أو وكالات إنفاذ القانون فعلاً عن كونه تمريناً لا يقدم ولا يؤخر في شيء. لذلك فإن الاهتمام يتجه بشكل متزايد نحو نماذج رقابة إدارية وقضائية وبرلمانية مختلطة، وهذه نقطة أبرزتها عدة إسهامات في هذا التقرير. وثمة اهتمام خاص بإنشاء مواقف "الدعوة إلى المصلحة العامة" في إطار عمليات إصدار إذن المراقبة. ونظراً للدور المتزايد الذي تضطلع به الأطراف الثالثة، مثل مقدمي

(٣١) CCPR/C/USA/CO/4، الفقرة ٢٢.

خدمات الإنترنت، فقد يستدعي الأمر أيضاً النظر في السماح لهذه الأطراف بالمشاركة في الإذن باتخاذ تدابير المراقبة التي تؤثر في مصالحها أو السماح لها بالطعن في التدابير القائمة. وقد سُلِّط الضوء بشكل إيجابي في السوابق القضائية ذات الصلة على فائدة المشورة و/أو الرصد و/أو الاستعراض من جانب أطراف مستقلة للمساعدة على ضمان تدقيق صارم للتدابير المفروضة بموجب نظام قانوني للمراقبة. وبإمكان اللجان البرلمانية أيضاً أن تضطلع بدور هام؛ ولكنها قد تفتقر أيضاً إلى الاستقلالية أو الموارد أو الرغبة في كشف التجاوزات، وقد تكون خاضعة للهيمنة التنظيمية. وقد شددت السوابق القضائية على الصعيد الإقليمي على فائدة هيئة رقابة مستقلة تماماً، خاصة لرصد تنفيذ تدابير المراقبة الموافق عليها[٣٢]. ولذلك، اقترح المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، في عام ٢٠٠٩، أنه "يجب ألا يوجد أي نظام مراقبة سري لا يخضع لاستعراض هيئة رقابة مستقلة ويجب أن تحصل جميع عمليات التدخل على إذن هيئة مستقلة"[٣٣].

هاء- الحق في سبل انتصاف فعالة

٣٩- يقتضي العهد الدولي الخاص بالحقوق المدنية والسياسية من الدول الأطراف أن تضمن حصول ضحايا الانتهاكات المتعلقة بالعهد على سبيل انتصاف فعال. وتنص الفقرة ٣(ب) من المادة ٢ كذلك على أن الدول الأطراف في العهد "تكفل لكل متظلم على هذا النحو أن تبت في الحقوق التي يدّعي انتهاكها سلطة قضائية أو إدارية أو تشريعية مختصة، أو أية سلطة مختصة أخرى ينص عليها نظام الدولة القانوني، وبأن تنمي إمكانيات التظلم القضائي". ويجب أيضاً أن تضمن الدول قيام السلطات المختصة بإعمال سبل الانتصاف المذكورة متى مُنحت. وكما أبرزت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم ٣١، من شأن تقاعس دولة طرف عن التحقيق في ادعاءات حدوث انتهاكات أن يفضي، في حد ذاته، إلى حدوث إخلال منفصل بأحكام العهد[٣٤]. وعلاوة على ذلك فإن وقف انتهاك جارٍ عنصر ضروري من عناصر الحق في سبيل انتصاف فعال.

٤٠- ومن ثم يمكن أن تتجلى سبل الانتصاف الفعالة المتعلقة بحالات انتهاك الخصوصية عن طريق المراقبة الرقمية في مختلف الأشكال القضائية والتشريعية والإدارية. وتتقاسم سبل الانتصاف الفعالة عموماً بعض الخصائص. أولاً، يجب أن تكون سبل الانتصاف معروفة وفي متناول أي شخص لديه ادعاء قابل للجدال بأن حقوقه قد انتُهِكت. وهكذا يصبح الإشعار

(٣٢) انظر مثلاً المحكمة الأوروبية لحقوق الإنسان، *إيكيمدزييف ضد بلغاريا*، الطلب رقم ٠٠/٦٢٥٤٠، ٢٨ حزيران/يونيه ٢٠٠٧.

(٣٣) A/HRC/13/37، الفقرة ٦٢.

(٣٤) CCPR/C/21/Rev.1/Add.13، الفقرة ١٥.

(بوجود إما نظام عام للمراقبة أو تدابير مراقبة خاصة) والوقوف (للطعن في هذه التدابير) مسألتين حاسمتين في تحديد الوصول إلى سبيل انتصاف فعال. وتنتهج الدول نهجاً مختلفة في الإشعار: بينما يقتضي بعضها إشعار أهداف المراقبة بعد الفعل، بمجرد انتهاء التحقيقات، فإن نظماً عديدة لا تنص على الإشعار. وقد يطلب البعض أيضاً رسمياً هذا الإشعار في القضايا الجنائية؛ ولكن يبدو أن هذا التقييد يُهمَل باستمرار في الممارسة العملية. وهناك أيضاً نهج مختلفة للوقوف من أجل تقديم الطعون القضائية. فقد قضت المحكمة الأوروبية لحقوق الإنسان قضت بأن وجود نظام للمراقبة، رغم أنه قد يتدخل في الخصوصية، فإن ادعاء أن ذلك ينشئ انتهاكاً للحقوق لا يصلح لأن تنظر فيه المحكمة إلا عندما يكون هناك "احتمال معقول" بأن شخصاً ما خضع فعلاً لمراقبة غير قانونية[٣٥].

٤١- ثانياً، ستنطوي سبل الانتصاف الفعالة على تحقيق فوري وشامل ومحايد في الانتهاكات المزعومة. ويمكن توفير ذلك بإيجاد "هيئة رقابة مستقلة [...] ضمانات كافية لمراعاة الأصول القانونية ورقابة قضائية، في حدود ما هو مقبول في مجتمع ديمقراطي"[٣٦]. ثالثاً، لكي تكون سبل الانتصاف فعالة، يجب أن تكون قادرة على إنهاء الانتهاكات الجارية، مثلاً عن طريق الأمر بحذف البيانات أو غير ذلك من أشكال الجبر[٣٧]. ويجب أن يكون لهيئات الانتصاف هذه القدرة على "الوصول على نحو تام وبلا عوائق إلى جميع المعلومات ذات الصلة، والموارد والخبرات الضرورية لإجراء التحقيقات، والقدرة اللازمة لإصدار الأوامر الملزمة"[٣٨]. رابعاً، حيثما ارتقت انتهاكات حقوق الإنسان إلى مستوى الانتهاكات الجسيمة، لن تكون سبل الانتصاف غير القضائية كافية، إذ تكون ثمة حاجة إلى مقاضاة جنائية[٣٩].

---

(٣٥) انظر *إسبيستر ضد المملكة المتحدة*، الطلب رقم ٩١/١٨٦٠١، قرار اللجنة المؤرخ ٢ نيسان/أبريل ١٩٩٣؛ *وريدغريف ضد المملكة المتحدة*، الطلب رقم ٩٢/٢٠٢٧١١، قرار اللجنة المؤرخ ١ أيلول/سبتمبر ١٩٩٣؛ *وماتيوز ضد المملكة المتحدة*، الطلب رقم ٩٥/٢٨٥٧٦، قرار اللجنة المؤرخ ١٦ تشرين الأول/ أكتوبر ١٩٩٦.

(٣٦) "الإعلان المشترك بشأن برامج المراقبة وأثرها على حرية التعبير، الذي أصدره المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير والمقرر الخاص المعني بحرية التعبير في لجنة البلدان الأمريكية لحقوق الإنسان، حزيران/يونيه ٢٠١٣ (متاح على الموقع الشبكي التالي: www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1)، الفقرة ٩.

(٣٧) انظر مثلاً المحكمة الأوروبية لحقوق الإنسان، *سيغيرستيد - ويبر وآخرون ضد السويد*، الطلب رقم ٦٢٣٣٢/٠٠، ٦ حزيران/يونيه ٢٠٠٦. وانظر أيضاً CCPR/C/21/Rev.1/Add.13، الفقرات ١٥-١٧.

(٣٨) A/HRC/14/46.

(٣٩) المبادئ الأساسية والمبادئ التوجيهية بشأن الحق في الانتصاف والجبر لضحايا الانتهاكات الجسيمة للقانون الدولي لحقوق الإنسان والانتهاكات الخطيرة للقانون الإنساني الدولي (قرار الجمعية العامة ١٤٧/٦٠، المرفق).

رابعاً- ما هو دور الأعمال التجارية؟

٤٢- هناك أدلة قوية على تزايد اعتماد الحكومات على القطاع الخاص لإجراء المراقبة الرقمية وتيسيرها. وفي جميع القارات، استخدمت الحكومات آليات قانونية رسمية وأساليب سرية للوصول إلى المحتوى وكذلك إلى البيانات التوصيفية. ويُضفى على هذه العملية صبغة رسمية بشكل متزايد: مع تحول تقديم خدمات الاتصالات من القطاع العام إلى القطاع الخاص، كان هناك "تفويض لعملية إنفاذ القانون ومسؤوليات شبه قضائية إلى وسطاء في مجال الإنترنت تحت ستار "التنظيم الذاتي" أو "التعاون"[٤٠]. ويثير وضع شروط قانونية لكي تجعل الشركات شبكاتها "قابلة للتنصت على المكالمات" قلقاً خاصاً، لأسباب ليس أقلها أن ذلك ينشئ بيئة تيسر تدابير المراقبة الشاملة.

٤٣- وقد تكون ثمة أسباب مشروعة لكي تطلب دولة من شركة لتكنولوجيا المعلومات والاتصالات أن تزودها ببيانات المستعملين؛ ولكن، عندما تقدم شركة بيانات أو معلومات المستعملين إلى دولة استجابة لطلب ينتهك الحق في الخصوصية بموجب القانون الدولي، أو عندما تقدم شركة تكنولوجيا أو معدات المراقبة الجماعية إلى الدول دون وجود ضمانات كافية، أو عندما تُستخدم المعلومات بطريقة تنتهك حقوق الإنسان، فإن من المحتمل أن تكون تلك الشركة شريكة أو مشاركة بطريقة أخرى في تجاوزات تتعلق بحقوق الإنسان. وتوفر المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان، التي دعمها مجلس حقوق الإنسان في عام ٢٠١١، معايير عالمية لمنع ومواجهة الآثار الضارة على حقوق الإنسان المرتبطة بنشاط الأعمال التجارية. وتنطبق مسؤولية احترام حقوق الإنسان في جميع العمليات العالمية للشركات بصرف النظر عن مكان وجود مستعمليها، وهي توجد بشكل مستقل عما إذا كانت الدولة تفي بالتزاماتها في مجال حقوق الإنسان.

٤٤- وقد بُذِلت جهود هامة لأصحاب مصلحة متعددين لتوضيح تطبيق المبادئ التوجيهية في قطاع تكنولوجيا الاتصالات والمعلومات. فالمؤسسات التي تقدم خدمات المحتوى أو الإنترنت، أو تقدم التكنولوجيا والمعدات التي تجعل الاتصالات الرقمية ممكنة، على سبيل المثال، ينبغي أن تعتمد بياناً صريحاً للسياسات يوجز التزامها باحترام حقوق الإنسان في جميع أنشطة الشركة. وينبغي لها أيضاً أن تكون لديها سياسات مناسبة لبذل العناية الواجبة لتحديد وتقييم ومنع وتخفيف أي تأثير ضار. وينبغي أن تقيِّم الشركات ما إذا كانت شروط خدمتها أو سياساتها المتعلقة بجمع بيانات الزبائن وتقاسمها قد تسفر عن تأثير ضار على حقوق الإنسان الخاصة بمستعمليها وكيف يمكن أن يكون ذلك.

---

(٤٠) انظر المرجع التالي: European Digital Rights, "The Slide from 'Self-Regulation' to Corporate Censorship", Brussels, January 2011, available at www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

٤٥- وعندما تواجه المؤسسات طلبات حكومية للوصول إلى البيانات لا تتوافق مع المعايير الدولية لحقوق الإنسان، فإن المتوقع منها هو أن تسعى إلى الوفاء بمبادئ حقوق الإنسان إلى أبعد حد ممكن، وأن تكون قادرة على إثبات جهودها المستمرة من أجل ذلك. ويمكن أن يعني ذلك تفسير طلبات الحكومة بأضيق طريقة ممكنة، والتماس توضيح من الحكومة فيما يخص نطاق الطلب وأسسه القانونية، وطلب أمر محكمة قبل تلبية طلبات الحكومة الخاصة بالبيانات، والتواصل بطريقة شفافة مع المستعملين بشأن المخاطر والامتثال لطلبات الحكومة. وثمة أمثلة إيجابية عن إجراءات الصناعة في هذا الصدد، سواء من جانب فرادى المؤسسات أو عن طريق مبادرات أصحاب مصلحة متعددين.

٤٦- ويتمثل جزء مركزي من بذل العناية الواجبة في مجال حقوق الإنسان كما تعرفه المبادئ التوجيهية في إجراء مشاورات مجدية مع أصحاب المصلحة المتأثرين. وفي سياق شركات تكنولوجيا المعلومات والاتصالات، يشمل ذلك أيضاً ضمان تمتع المستعملين بشفافية ملموسة بشأن طريقة جمع بياناتهم وتخزينها واستخدامها وربما تقاسمها مع الآخرين، بحيث يتمكنون من إثارة الشواغل واتخاذ قرارات مستنيرة. وتوضح المبادئ التوجيهية أن على المؤسسات، عندما تحدد أنها تسببت في آثار ضار على حقوق الإنسان أو ساهمت فيه، أن تتحمل مسؤولية ضمان إصلاح الخطأ بإتاحة سبل انتصاف مباشرة أو بالتعاون مع عمليات انتصاف مشروعة. ولتمكين إصلاح الخطأ في أقرب وقت ممكن، ينبغي للمؤسسات أن تنشئ آليات للتظلم على المستوى التشغيلي. وقد تكون هذه الآليات مهمة بوجه خاص في البلدان حيث الحقوق غير محمية حماية كافية أو حيث تنعدم فرص الوصول إلى سبل انتصاف قضائية وغير قضائية. وبالإضافة إلى عناصر مثل التعويض ورد الحق، ينبغي أن تشمل سبل الانتصاف معلومات عن أي البيانات تم تقاسمها مع سلطات الدولة، وكيف تم ذلك.

خامساً- الاستنتاجات والتوصيات

٤٧- يوفر القانون الدولي لحقوق الإنسان إطاراً واضحاً وعالمياً لتعزيز الحق في الخصوصية وحمايته، بما في ذلك في سياق المراقبة الداخلية والخارجية، واعتراض الاتصالات الرقمية وجمع البيانات الشخصية. غير 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.

٤٨- وعند معالجة الثغرات الهامة في تنفيذ الحق في الخصوصية، يجوز إبداء ملاحظتين. الملاحظة الأولى هي أن المعلومات المتعلقة بسياسات وممارسات المراقبة الداخلية والخارجية ما زالت تظهر. وما زالت التحقيقات جارية بغية جمع المعلومات عن المراقبة الإلكترونية وجمع البيانات الشخصية وتخزينها، وكذلك تقييم أثرها على حقوق الإنسان. وتشارك المحاكم على

الصعيدين الوطني والإقليمي في دراسة مدى قانونية سياسات وتدابير المراقبة الإلكترونية. وأي تقييم لسياسات وممارسات المراقبة بالمقارنة مع القانون الدولي لحقوق الإنسان يجب بالضرورة أن يُجرى على ضوء الطبيعة المتغيرة لهذه المسألة. وتتعلق ملاحظة ثانية ذات صلة بالغياب المزعج للشفافية الحكومية المرتبطة بسياسات وقوانين وممارسات المراقبة، الذي يعيق أي جهود لتقييم اتساقها مع القانون الدولي لحقوق الإنسان ولضمان المساءلة.

٤٩- وستتطلب المواجهة الفعالة للتحديات المتصلة بالحق في الخصوصية في سياق تكنولوجيا الاتصالات الحديثة التزاما مستمراً ومتضافراً ومتعدد أصحاب المصلحة. وينبغي أن تتضمن هذه العملية حواراً يشمل جميع أصحاب المصلحة المعنيين، بما فيهم الدول الأعضاء والمجتمع المدني والأوساط العلمية والتقنية وقطاع الأعمال والأوساط الأكاديمية وخبراء حقوق الإنسان. ومع استمرار تطور تكنولوجيا الاتصالات، سيكون للقيادة دور حاسم لضمان استخدام هذه التكنولوجيات لتسخير إمكانياتها من أجل تحسين التمتع بحقوق الإنسان المكرسة في الإطار القانوني الدولي.

٥٠- ومع مراعاة الملاحظات السابقة، هناك حاجة واضحة وملحة لليقظة في ضمان امتثال أي سياسة أو ممارسة في مجال المراقبة للقانون الدولي لحقوق الإنسان، بما فيه الحق في الخصوصية، من خلال وضع ضمانات فعالة ضد التجاوزات. وكتدبير فوري، ينبغي أن تستعرض الدول قوانينها وسياساتها وممارساتها الوطنية الخاصة لضمان مطابقتها التامة للقانون الدولي لحقوق الإنسان. وعند وجود أوجه قصور، ينبغي للدول أن تتخذ خطوات لمعالجتها، بوسائل منها اعتماد إطار تشريعي واضح ودقيق وفي المتناول وشامل وغير تمييزي. وينبغي اتخاذ خطوات لضمان وجود نظم وممارسات رقابة فعالة ومستقلة، مع الاهتمام بحق الضحايا في سبيل انتصاف فعال.

٥١- وهناك عدد من التحديات العملية الهامة لتعزيز الحق في الخصوصية وحمايته في العصر الرقمي. واستناداً إلى الاستكشاف الأولي لبعض القضايا الواردة في هذا التقرير، ثمة حاجة إلى مزيد من المناقشة وإلى إجراء دراسة معمقة للقضايا المتصلة بالحماية القانونية الفعالة والضمانات الإجرائية والرقابة الفعالة وسبل الانتصاف. وسيساعد تحليل معمق لهذه القضايا على توفير مزيد من التوجيهات العملية، القائمة على القانون الدولي لحقوق الإنسان، بشأن مبادئ الضرورة والتناسبية والمشروعية فيما يخص ممارسات المراقبة؛ وبشأن تدابير رقابة فعالة ومستقلة ومحايدة؛ وبشأن تدابير الانتصاف. وسيساعد تحليل إضافي أيضاً كيانات الأعمال في الوفاء بمسؤولياتها لاحترام حقوق الإنسان، بما في ذلك بذل العناية الواجبة وضمانات إدارة المخاطر، كما سيساعد في دورها المتعلق بتوفير سبل انتصاف فعالة.