الأمم المتحدة

A/HRC/35/22

الجمعية العامة

Distr.: General
30 March 2017
Arabic
Original: English

مجلس حقوق الإنسان
الدورة الخامسة والثلاثون
٦-٢٣ حزيران/يونيه ٢٠١٧
البند ٣ من جدول الأعمال
تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية

تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير

مذكرة من الأمانة

تتشرف الأمانة بأن تحيل إلى مجلس حقوق الإنسان تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، دافيد كاي، الذي أُعد عملاً بقرار المجلس ٢/٢٥. وقد ركز المقرر الخاص في تقريريه السابقين إلى المجلس على حرية الرأي والتعبير في العصر الرقمي، وتناول بالتفصيل الكيفية التي يتسنى بها لأدوات التشفير وإخفاء الهوية توفير الأمن اللازم لممارسة حرية التعبير (A/HRC/29/32)، وحدد كيفية انخراط قطاع تكنولوجيا المعلومات والاتصالات في توفير مقتضيات حرية التعبير (A/HRC/32/38). ويتناول في هذا التقرير دور الجهات الفاعلة الخاصة المشاركة في توفير الوصول إلى الإنترنت والاتصالات السلكية واللاسلكية. ويبدأ التقرير ببحث التزامات الدول فيما يتعلق بحماية وتعزيز حرية التعبير على الإنترنت، ثم يقيّم دور صناعة الوصول الرقمي، ويختتم التقرير بمجموعة من المبادئ التي يمكن أن يسترشد بها القطاع الخاص في اتخاذ الخطوات اللازمة لاحترام حقوق الإنسان.

GE.17-05047(A)
1705047

الرجاء إعادة الاستعمال

تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير

المحتويات

الصفحة

أولاً – مقدمة ٣

ثانياً – التزام الدولة بحماية وتعزيز حرية التعبير على الإنترنت ٤

ألف– إيقاف شبكة الإنترنت والاتصالات السلكية واللاسلكية ٥

باء – وصول الحكومة إلى بيانات المستخدمين ٨

جيم– حياد شبكة الإنترنت ١٠

ثالثاً – مقدمو الخدمات الرقمية وحرية التعبير ١٢

ألف– الاتصالات السلكية واللاسلكية ومقدمو خدمات الإنترنت ١٣

باء – نقاط تبادل الإنترنت ١٤

جيم– شبكات إيصال المحتوى ١٥

دال – بائعو معدات الشبكات ١٦

هاء – أطراف فاعلة خاصة أخرى ١٧

رابعاً – مسؤوليات مقدمي خدمة الوصول الرقمي تجاه حقوق الإنسان ١٨

ألف– اعتبارات السياق ١٨

باء – المسؤولية عن احترام حرية المستخدمين في التعبير ١٩

خامساً – الاستنتاجات والتوصيات ٢٦

أولاً- مقدمة

١- تعتمد الدول بشكل متزايد على صناعة الوصول الرقمي من أجل مراقبة التعبير على الإنترنت أو حظره أو رصده. وغالباً ما تلتمس السلطات المساعدة من مقدمي خدمات الإنترنت عندما تسعى إلى حجب المواقع الشبكية ووسائط التواصل الاجتماعي عن المستخدمين، أو إيقاف شبكة الإنترنت تماماً. فيجري تعطيل نقاط تبادل الإنترنت التي تيسّر تدفق المعلومات إلى البلد أو داخله. وتتمكن من الوصول إلى الاتصالات الخاصة وغيرها من البيانات الشخصية التي تحتفظ بها شركات الاتصالات السلكية واللاسلكية. وفي الوقت الراهن، فإن العديد من هذه الجهات الفاعلة يملكها أو يشغلها القطاع الخاص. وغالباً ما تكون هذه الجهات الفاعلة ضرورية لفرض الرقابة والمراقبة من قِبل الدولة، وذلك مع إبداء الاحتجاج أو الموافقة الضمنية أو المشاركة برغبة منها. وما تطلبه الحكومات من هذه الجهات الفاعلة الخاصة، وكيفية استجابتها، قد يتسببان في إعاقة تبادل المعلومات؛ والحد من قدرة الصحفيين على التحقق بشكل آمن من المعلومات؛ وردع المبلغين والمدافعين عن حقوق الإنسان. وقد تعمد هذه الجهات الخاصة أيضاً إلى تقييد حرية التعبير بمبادرة منها، إذ بإمكانها تحديد أولويات محتوى أو تطبيقات الإنترنت نظير مقابل مادي أو منافع تجارية أخرى، ويمكنها تغيير كيفية تعامل المستخدمين مع المعلومات على شبكة الإنترنت. ويمكن للشركات التي تقدم خدمات ترشيح المعلومات أن تؤثر في نطاق المحتوى المتاح للمشتركين.

٢- وتؤثر الدول والجهات الفاعلة الخاصة على حد سواء في حرية التعبير. وللدول التزامات واضحة فيما يتعلق بحماية حرية التعبير، ولكن بماذا تكون الجهات الخاصة مدينة لمستخدميها؟ وكيف ينبغي لها أن تحترم حرية التعبير؟ وما هي الخطوات التي تتخذها لتقييم ومعالجة المخاطر التي قد تمس حرية التعبير والخصوصية نتيجة استجابتها للإجراءات والسياسات الحكومية؟ وما مقدار المعلومات التي ينبغي أن تتقاسمها مع عملائها بشأن طلبات الدولة ومطالبها؟ ومتى تكون متورطة أو مشاركة بصورة مباشرة في الانتهاكات، وما هي المعالجات التي ينبغي أن تكون متاحة للأفراد أو عامة الجمهور الذين تتعرض مصالحهم للخطر؟

٣- إن الجهات الخاصة التي تتيح الوصول الرقمي هي وسيط يمكن من ممارسة حرية التعبير. ومن المؤكد أن الدول تكون وراء معظم عمليات الرقابة والمراقبة. وبما أن الدول تعتمد عادة، ولكن ليس دائماً، على موفري الخدمات من أجل اتخاذ الإجراءات التي تمكنها من فرض الرقابة، فإننا كمستخدمين - ومستفيدين من التطورات الكبيرة التي يشهدها العصر الرقمي - ينبغي أن نفهم كيفية تفاعل هذه الجهات الفاعلة مع بعضها البعض، وكيفية تأثرنا بهذه التفاعلات والإجراءات المستقلة، وما هي مسؤوليات موفري الخدمات فيما يخص احترام الحقوق الأساسية.

٤- وهذا التقرير هو ثمرة أكثر من سنة من البحث والتشاور بدأت بالقيام في عام ٢٠١٦ بتحديد معالم قطاع تكنولوجيا المعلومات والاتصالات (انظر A/HRC/32/38)[(١)] واستجابة للنداء المتعلق بتقديم تقارير، تلقى المقرر الخاص ٢٥ تقريراً مقدمة من الدول[(٢)]؛ و٣ تقارير من الشركات؛ و٢٢ تقريراً من المجتمع المدني والدوائر الأكاديمية ومن جهات أخرى؛ وتقريراً واحداً

(١) أود أن أتقدم بالشكر للسيد آموس توه، المستشار القانوني للولاية وزميل مؤسسة فورد في جامعة كاليفورنيا، كلية إيرفن للحقوق، لما قدمه من بحوث وتحليلات دقيقة، وكذلك على تنسيق البحوث الجوهرية والأساسية التي أجراها طلبة القانون في جامعة كاليفورنيا، كلية إيرفن، مركز العدالة الدولية.

(٢) انظر الرابط https://freedex.org/new-call-for-submissions-freedom-of-expression-and-the-telecommunications-and-internet-access-sector/.

يتسم بالسرية. وبالإضافة إلى ذلك، نظم المقرر الخاص جلسة تبادل أفكار استضافتها منظمة المادة ١٩ في لندن في تموز/يوليه ٢٠١٦، واجتماعاً لخبراء من معهد حقوق الإنسان التابع لجامعة كونيتيكت، الولايات المتحدة الأمريكية، في تشرين الأول/أكتوبر ٢٠١٦، ومشاورة إقليمية مع المقرر الخاص المعني بحرية التعبير التابع للجنة الأمريكية لحقوق الإنسان، في غوادالاخارا، المكسيك، في كانون الأول/ديسمبر ٢٠١٦، ومشاورة إقليمية في بيروت في شباط/فبراير ٢٠١٧[٣].

ثانياً- التزام الدولة بحماية وتعزيز حرية التعبير على الإنترنت

٥- ينص القانون الدولي لحقوق الإنسان على حق كل إنسان في اعتناق الآراء دون مضايقة، وفي التماس الأنباء والأفكار وتلقِّيها ونقلها بأيَّة وسيلة ودونما اعتبار للحدود (انظر الإعلان العالمي لحقوق الإنسان، المادة ١٩؛ والمادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية). وقد كرر مجلس حقوق الإنسان والجمعية العامة تأكيد أن حرية التعبير والحقوق الأخرى تنطبق على شبكة الإنترنت (انظر قراري المجلس ١٣/٢٦ و١٣/٣٢؛ وقرار الجمعية العامة ١٦٧/٦٨؛ والوثيقة A/HRC/32/38). وقد بُحثت التزامات الدول بموجب المادة ١٩ من العهد من جانب اللجنة المعنية بحقوق الإنسان والمكلفين بولايات سابقاً والمقرر الخاص. وباختصار، لا يجوز للدول أن تتدخل، أو أن تقيد، اعتناق الآراء (انظر المادة ١٩(١) من العهد؛ والفقرة ١٩ من الوثيقة A/HRC/29/32). وتنص المادة ١٩(٣) من العهد على أنه يجوز للدول فرض قيود على حرية التعبير شريطة أن تكون محددة بنص القانون وأن تكون ضرورية من أجل احترام حقوق الآخرين أو سمعتهم، أو لحماية الأمن الوطني أو النظام العام أو الصحة العامة أو الآداب العامة (انظر تعليق اللجنة المعنية بحقوق الإنسان رقم ٣٤(٢٠١١)؛ والوثيقة A/71/373؛ والوثيقة A/HRC/29/32).

٦- وعلى الدول أيضاً التزامات باتخاذ خطوات لحماية الأفراد من أي تدخل لا مسوغ له في حقوق الإنسان المتعلقة بهم من قِبل جهات فاعلة خاصة (انظر المادة ٢(٢) من العهد؛ والفقرة ١٨ من التعليق العام رقم ٣١(٢٠٠٤) للجنة المعنية بحقوق الإنسان). ويوفر قانون حقوق الإنسان الحماية للأفراد من الانتهاكات التي ترتكبها الدولة فضلاً عن التجاوزات التي يرتكبها أشخاص أو كيانات خاصة (انظر الفقرة ٨ من التعليق العام رقم ٣١)[٤]. إن المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون "الحماية والاحترام والانتصاف" الذي أقره مجلس حقوق الإنسان في عام ٢٠١١، يوضح أن الدول مطالبة باتخاذ خطوات مناسبة لمنع وقوع انتهاكات من جانب الجهات الفاعلة الخاصة والتحقيق فيها والمعاقبة عليها وإتاحة سبل الانتصاف (انظر A/HRC/17/31، المرفق، المبدأ ١). وتشمل الخطوات من هذا القبيل اعتماد وتنفيذ تدابير تشريعية وقضائية وإدارية وتربوية وغيرها من التدابير المناسبة التي تقتضي احترام الأعمال التجارية لحرية التعبير، وتتيح الوصول إلى سبيل

(٣) يمكن الاطلاع على التقارير على موقع الولاية. ويمكن الاطلاع على موجز عن المشاورات التي عقدت والمساهمات المستلمة من أجل إعداد هذا التقرير، في مرفق تكميلي متاح أيضاً على الموقع الشبكي للولاية.

(٤) انظر أيضاً "اللجنة الأفريقية لحقوق الإنسان والشعوب، التعليق العام رقم ٣(٢٠١٥) بشأن الحق في الحياة، الفقرة ٣٨؛ ومحكمة البلدان الأمريكية لحقوق الإنسان، قضية *فيلاسكيز رودريغيز*، الحكم الصادر في ٢٩ تموز/يوليه ١٩٨٨، الفقرة ١٧٢؛ والمحكمة الأوروبية لحقوق الإنسان، *أوزيل وآخرون ضد تركيا*، الحكم الصادر في ١٧ تشرين الثاني/نوفمبر ٢٠١٥، الفقرة ١٧٠.

انتصاف فعال عندما تقع انتهاكات من جانب جهات فاعلة خاصة (انظر الفقرة ٧ من التعليق العام رقم ٣١؛ والوثيقة A/HRC/17/31، المرفق، المبدأين ٣ و٢٥).

٧- وكثيراً ما تكون الإجراءات الحكومية المبينة أدناه غير مستوفية لمعايير قانون حقوق الإنسان. وعلاوة على ذلك، يؤدي غياب الشفافية إلى انتشار تدخلات الحكومة في صناعة الوصول الرقمي. ويشمل انعدام الشفافية وجود قوانين غامضة تمنح سلطات تقديرية مفرطة، وفرض قيود قانونية تمنع قيام طرف ثالث بكشف المعلومات المتعلقة بوصول الحكومة إلى بيانات المستخدمين ووضع قواعد تقييدية. ويؤدي انعدام الشفافية إلى تقويض سيادة القانون، فضلاً عن عدم تمكين عامة الجمهور من فهم هذا القطاع[٥].

ألف- إيقاف شبكة الإنترنت والاتصالات السلكية واللاسلكية

٨- إيقاف شبكة الإنترنت والاتصالات السلكية واللاسلكية يشمل اتخاذ تدابير لمنع أو إعاقة الوصول إلى المعلومات على الإنترنت أو نشرها، ما يشكل انتهاكاً لقانون حقوق الإنسان (انظر الفقرة ١٠ من الوثيقة A/HRC/32/13)[٦]. ولتنفيذ إيقاف شبكة الإنترنت أو الاتصالات، عادة ما تستعين الحكومات بالجهات الفاعلة الخاصة التي تشغّل الشبكات أو تيسّر تدفق المعلومات على الشبكة. والهجمات الواسعة النطاق على الهياكل الأساسية التي ترتكبها أطراف خاصة، مثل حجب الخدمة الموزّع قد يكون لها تأثير يتمثل في توقف الخدمة. وغالباً ما يرتبط إيقاف خدمات الإنترنت بتوقف الشبكة تماماً، لكن ذلك قد يحدث أيضاً عند قطع اتصالات الهاتف الجوال أو المواقع الشبكية أو وسائل التواصل الاجتماعي وتطبيقات الرسائل أو تضييق نطاقها أو جعلها "غير صالحة للاستخدام بشكل فعال"[٧]. وقد يؤثر إيقاف الخدمات على مدن أو مناطق داخل بلد ما، أو على بلد بأكمله أو عدة بلدان، وقد يستمر لفترات تتراوح بين ساعات وأشهر.

٩- وعمليات إيقاف الخدمة التي تصدر بها أوامر صريحة أو دون أساس قانوني واضح تشكل خرقاً لمقتضيات المادة ١٩(٣) من العهد التي تنص على أن تكون القيود "محددة بنص القانون". وفي تشاد، لم تتمكن السلطات من تقديم تفسيرات معقولة تبرر سلسلة عمليات إيقاف شبكة الإنترنت ووسائط التواصل الاجتماعي بين شباط/فبراير وتشرين الأول/أكتوبر ٢٠١٦، ما أدى إلى افتراض أنها كانت غير قانونية[٨]. وفي غابون، يُزعم حدوث انقطاع عام لشبكة الإنترنت كل مساء لمدة أسبوعين تقريباً خلال فترة انتخابات عام ٢٠١٦، خلافاً لتأكيدات الحكومة بشأن عدم تعطيل هذه الخدمات[٩].

١٠- ولم يستوف أيضاً شرط المشروعية فيما يتعلق بعمليات إيقاف خدمات الإنترنت التي أُمر بتطبيقها بموجب قوانين ولوائح صيغت بصورة غامضة. وفي طاجيكستان، يجيز القانون المعدّل بشأن فرض حالة الطوارئ للحكومة إيقاف خدمات الهاتف المحمول وشبكة الإنترنت دون الحاجة إلى أمر

(٥) تحالف الحرية على شبكة الإنترنت، تقرير الفريق العامل ٣: الخصوصية والشفافية على شبكة الإنترنت، تشرين الثاني/نوفمبر ٢٠١٥.

(٦) سجلت منظمة "الوصول الآن" إيقاف الخدمات ١٥ مرة في عام ٢٠١٥ و٥٦ مرة في عام ٢٠١٦. وسجلت أول عملية لإيقاف الخدمات في نيبال في شباط/فبراير ٢٠٠٥.

(٧) Access Now submission, part I, p. 1.

(٨) Internet Sans Frontières submission, p. 2, TCD 3/2016.

(٩) المرجع نفسه، GAB 1/2016.

من المحكمة عقب إعلان حالة الطوارئ[١٠]. ولم يحدد القانون توقيت أو أغراض إعلان حالة الطوارئ. وهذا الغموض يمنح السلطات سلطة تقديرية مطلقة لتنفيذ عمليات إيقاف الخدمات. وفي بعض البلدان، تعتمد السلطات على قوانين عفا عليها الزمن لتبرير عمليات إيقاف الخدمات[١١]. كما أن القوانين واللوائح المعتمدة والمنفذة بصورة سرية تنتهك شرط المشروعية. وفي الولايات المتحدة الأمريكية، أدخل مركز التنسيق الوطني للاتصالات السلكية واللاسلكية تعديلات كبيرة على المنشورات العامة المتعلقة بإجراءات التشغيل الموحدة ٣٠٣، وهي لائحة تنفيذية تحدد "الإجراءات المفصلة" بشأن "تعطيل خدمة الهاتف المحمول"[١٢] ولم يُحتج علناً على هذه الإجراءات، غير أن احتمال تهرب السلطات من التدقيق القانوني والمساءلة العامة يتعارض مع المادة ١٩ من العهد.

١١- والقيود المفروضة على التعبير يجب أن تكون لازمة لتحقيق الأهداف المحددة في المادة ١٩(٣) من العهد، ولا ينبغي التذرع بها لتبرير قمع مناصرة الحقوق الديمقراطية (انظر الفقرة ٢٣ من التعليق العام رقم ٣٤ للجنة المعنية بحقوق الإنسان؛ والوثيقة A/71/373، الفقرة ٢٦). بيد أن الحكومات كثيراً ما تعمد إلى إيقاف الخدمات خلال المظاهرات والانتخابات وغيرها من الأحداث الاستثنائية المتعلقة بالمصلحة العامة، وذلك مع تقديم توضيحات غير كافية أو دون أي توضيحات[١٣]. وفي البحرين، يُزعم أن إيقاف خدمات الهاتف المحمول والإنترنت في دوراز قد تزامن مع اعتصامات جرت خارج منزل زعيم ديني بارز أقدمت الحكومة على تجريده من حق المواطنة[١٤]. وأُفيد أن مستخدمي الإنترنت في جمهورية فنزويلا البوليفارية حُرموا الوصول إلى الإنترنت أثناء الاحتجاجات الواسعة النطاق ضد الحكومة في عام ٢٠١٤[١٥]. وقد سجلت حالات إيقاف لخدمة الإنترنت خلال أو قبل الانتخابات أو الاحتجاجات التي شهدتها كل من الكاميرون[١٦] وغامبيا[١٧] والهند[١٨] وميانمار[١٩] وجمهورية إيران الإسلامية[٢٠] وأوغندا[٢١] والجبل الأسود[٢٢].

---

(١٠) المفوضية السامية لحقوق الإنسان، "الملاحظات الأولية لمقرر الأمم المتحدة الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، دافيد كاي، في ختام زيارته إلى طاجيكستان، نشرة صحفية (٩ آذار/مارس ٢٠١٦).

(١١) India, Code of Criminal Procedure, sect. 144; also Apar Gupta and Raman Jit Singh Chima, "The cost of internet shutdowns", *The Indian Express* (26 October 2016).

(١٢) الولايات المتحدة الأمريكية، مركز التنسيق الوطني لإجراءات التشغيل الموحدة ٣٠٣.

(١٣) Access Now submission, part I, pp. 5-7.

(١٤) مركز البحرين لحقوق الإنسان، *عرقلة الحقوق الرقمية في البحرين* (٢٠١٦)، الصفحتان ١٣-١٤.

(١٥) Danny O'Brien, "Venezuela's Internet crackdown escalates into regional blackout", Electronic Frontier Foundation (20 February 2014).

(١٦) مفوضية حقوق الإنسان، "الخبير التابع للأمم المتحدة يحث الكاميرون على إعادة تشغيل خدمات الإنترنت التي قطعت بصورة تنتهك الحقوق"، نشرة صحفية (١٠ شباط/فبراير ٢٠١٧).

(١٧) Deji Olukotun, "Gambia shuts down Internet on eve of elections", Access Now (30 November 2016).

(١٨) Software Freedom Law Center, "Internet shutdowns in India, 2013-2016".

(١٩) Freedom House, "Freedom on the Net: Myanmar" (2011).

(٢٠) Center for Democracy and Technology, "Iran's Internet throttling: unacceptable now, unacceptable then" (3 July 2013).

(٢١) Article 19, "Uganda: Blanket ban on social media on election day is disproportionate" press release (18 February 2016).

(٢٢) Global Voices, "WhatsApp and Viber blocked on election day in Montenegro" (17 October 2016).

١٢- إن عدم توضيح أسباب عمليات إيقاف الخدمات أو الاعتراف بها يولد الشعور بأن الغرض منها هو قمع الإبلاغ أو النقد أو المعارضة. وثمة ادعاءات ترد في تقارير بشأن القمع والعنف الذي تجيزه الدولة عقب قطع خدمات الشبكة مفادها أن بعض الدول تستغل إيقاف خدمات الإنترنت لارتكاب انتهاكات والتستر عليها. وفي السودان، على سبيل المثال، قُطعت خدمة الإنترنت لعدة ساعات خلال التصدي بصورة فتاكة للمتظاهرين الذين خرجوا احتجاجاً على زيادة أسعار الوقود في أيلول/سبتمبر ٢٠١٣[٢٣].

١٣- ولاحظ المراقبون أيضاً اللجوء على نحو متزايد إلى قطع خدمات الإنترنت لمنع الطلاب من الغش أثناء الامتحانات الوطنية. وقد تكون أوزبكستان الدولة الأولى التي تذرعت بهذا المبرر أثناء امتحانات القبول للجامعات عام ٢٠١٤[٢٤]. وفي عام ٢٠١٦، يُدعى أن السلطات أمرت بقطع خدمات الإنترنت خلال الامتحانات في كل من الهند والجزائر وإثيوبيا والعراق[٢٥].

١٤- ومما لا شك فيه أن عمليات إيقاف خدمات الإنترنت لم تستوف معيار الضرورة. وتقتضي الضرورة أن تحقق عمليات إيقاف الخدمات هدفها المعلن، الذي عادة ما تؤدي إلى تقويضه في واقع الأمر. وتحتج بعض الحكومات بأن من المهم منع انتشار الأنباء عن وقوع هجمات إرهابية، حتى إذا كان الأخبار دقيقة، بغية منع وقوع ذعر وتصرفات مستنسخة[٢٦]. ومع ذلك، فقد تبين أن إبقاء الربط الشبكي يمكن أن يخفف من الشواغل المتعلقة بالسلامة العامة ويساعد على استعادة النظام العام. فخلال الاضطرابات العامة التي شهدتها مدينة لندن عام ٢٠١١ على سبيل المثال، استخدمت السلطات شبكات التواصل الاجتماعي من أجل تحديد الجناة، ونشر المعلومات الدقيقة وإجراء عمليات التنظيف. وفي كشمير، أفادت الشرطة بالدور الإيجابي للهواتف المحمولة في تحديد أماكن أشخاص كانوا محاصرين أثناء الهجمات الإرهابية[٢٧].

١٥- وقد تكون عمليات إيقاف خدمات الإنترنت متباينة ومتفاوتة من حيث مدتها ونطاقها الجغرافي، لكنها تكون غير متناسبة بشكل عام، إذ يصبح مستخدمو الإنترنت معزولين عن خدمات الطوارئ والمعلومات الصحية، والخدمات المصرفية الجوالة والتجارة الإلكترونية، ووسائل النقل، والمدارس، ورصد عمليات التصويت والانتخابات، والتقارير المتعلقة بالأزمات والأحداث الرئيسية، والتحقيقات الخاصة بحقوق الإنسان[٢٨]. ونظراً لعدد الأنشطة والخدمات الأساسية المتأثرة، تؤدي عمليات إيقاف الخدمات إلى تقييد التعبير وتتعارض مع الحقوق الأساسية الأخرى.

---

(٢٣) هيومن رايتس ووتش، "السودان: عشرات القتلى خلال الاحتجاجات" (٢٧ سبتمبر ٢٠١٣).

(٢٤) Access Now submission, part I; also Freedom House, "Freedom on the Net: Uzbekistan" (2016).

(٢٥) هيومن رايتس ووتش، "السودان: عشرات القتلى خلال الاحتجاجات" (٢٧ سبتمبر ٢٠١٣).

(٢٦) انظر على سبيل المثال، مفوضية حقوق الإنسان، "الاستنتاجات والملاحظات الأولية للمقرر الخاص المعني بالحق في حرية الرأي والتعبير عن زيارته إلى تركيا، ١٤-١٨ تشرين الثاني/نوفمبر ٢٠١٦"، نشرة صحفية (١٨ تشرين الثاني/نوفمبر ٢٠١٦).

(٢٧) Institute for Human Rights and Business (IHRB), "Security v. Access: The impact of mobile network shutdowns", case study: Telenor Pakistan (September 2015), pp. 31-32.

(٢٨) Access Now submission, part I, pp. 11-14; also Global Network Initiative submission.

١٦- ويؤثر إيقاف خدمات الإنترنت كذلك على مجالات تتجاوز تلك المتعلقة بشواغل محددة[٢٩]. ففي باكستان، وتمهيداً لتنظيم موكب الاحتفال باليوم الوطني، يُزعم أن شبكات الهاتف المحمول قُطعت في مكان الاحتفال وكذلك في مناطق محيطة لم يكن من المتوقع أن تشهد أي تهديدات أمنية[٣٠]. وخلال زيارة البابا إلى الفلبين عام ٢٠١٥، جرى قطع شبكات الهاتف المحمول لأسباب تتعلق بالسلامة على نحو تجاوز مسار تحركه[٣١]. وعندما تُعطّل خدمات أو برامج محددة، عادة ما تستهدف الحكومات أكثرها كفاءة وأمناً أو تلك المستخدمة على نطاق واسع[٣٢].

باء- وصول الحكومة إلى بيانات المستخدمين

١٧- تعتمد المراقبة الحكومية في الوقت الراهن على الوصول إلى اتصالات وبيانات مستخدمي الشبكات المملوكة للقطاع الخاص. وكثيراً ما يتطلب هذا الوصول الحصول على المساعدة من جهات فاعلة خاصة، لكنه قد يحدث دون علمها أو مشاركتها. ومثلما هو الحال بالنسبة لسائر أشكال المراقبة، فإن وصول الحكومة إلى هذه البيانات قد يشكل تدخلاً في خصوصية الأفراد على نحو يمكن أن يؤدي بصورة مباشرة أو غير مباشرة إلى تقييد حرية تطوير الأفكار وتبادلها (انظر A/HRC/23/40، الفقرة ٢٤). إن الوصول دون مسوغ إلى البيانات الشخصية ينطوي على تحذير للمستخدمين ويدفعهم إلى التفكير ملياً فيما يقولون وربما تجنب الإدلاء بآراء مخالفة، ويردع تبادل المعلومات وغير ذلك من العمليات المتعلقة بممارسة حرية التعبير التي قد تخضع لرقابة الحكومة (انظر A/HRC/27/37، الفقرة ٢٠).

طلبات الحصول على بيانات المستخدمين

١٨- تُشكل القوانين والقواعد الغامضة انتهاكاً لشرط المشروعية (انظر A/HRC/23/40، الفقرة ٥٠). فقانون الاتصالات والوسائط المتعددة في ماليزيا، على سبيل المثال، يسمح للسلطات بأن تأمر بكشف "أي اتصال أو فئة اتصالات" لدى "وقوع أي حالة طوارئ عامة أو حفاظاً على السلامة العامة". ولا يحدد هذا القانون الظروف التي تؤدي إلى إعلان حالة الطوارئ العامة، وتُعتبر مصادقة الملك عليها "دليلاً قاطعاً على ضرورتها"[٣٣]. وفي قطر، تتمتع الجهات المعنية بإنفاذ القانون بالحق على نطاق واسع في طلب الوصول إلى اتصالات عملاء مقدمي الخدمات في الحالات المتعلقة بالأمن القومي أو الطوارئ[٣٤]. وهذه الأحكام تمكن السلطات من طلب بيانات المستخدمين بالاستناد فقط إلى دواعي الأمن الوطني. ولذا، لا يمكن للمستخدمين التنبؤ بقدر معقول من اليقين بالظروف التي تؤدي إلى تمكين السلطات من كشف اتصالاتهم وما يتعلق بها من بيانات.

(٢٩) IHRB, "Security v. Access: The impact of mobile network shutdowns", case study: Telenor Pakistan (September 2015), p. 20.

(٣٠) المرجع السابق، الصفحتان ٢٧-٢٨.

(٣١) Deniz Duru Aydin, "Five excuses governments (ab)use to justify Internet shutdowns" Access Now (6 October 2016)

(٣٢) Article 19 submission, p. 2.

(٣٣) ماليزيا، قانون الاتصالات والوسائط المتعددة، (١٩٩٨) الباب ٢٦٦.

(٣٤) قطر، المرسوم بقانون رقم ٣٤ لعام ٢٠٠٦.

١٩- ولا ينبغي إرغام مقدمي الخدمات على كشف بيانات المستخدمين إلا بأمر من السلطات القضائية يثبت الضرورة والتناسب بغية تحقيق هدف مشروع. ويستوجب القانون الجنائي الكندي أن تقدم الجهات المعنية بإنفاذ القانون طلبات الكشف عن التسجيلات الهاتفية المتعلقة بتحقيقات جنائية إلى القضاء للموافقة عليها[٣٥]. وفي البرتغال، يجب أن تحصل السلطات على أمر قضائي لإجبار الجهات المعنية على الكشف عن بيانات الاتصالات[٣٦]. بيد أن القوانين الوطنية غالباً ما لا تستوجب صدور إذن قضائي من أجل الحصول على بيانات المستخدمين. وفي بنغلاديش، تحتاج السلطات إلى موافقة السلطات التنفيذية فقط من أجل الوصول إلى بيانات الاتصالات الخاصة بالمشتركين في شبكات الاتصالات السلكية واللاسلكية على أساس دواعي الأمن القومي وصون النظام العام[٣٧].

٢٠- والقوانين التي تلزم الجهات الخاصة بإنشاء قواعد بيانات كبيرة تشمل بيانات المستخدمين وتكون في متناول الحكومة تثير شواغل تتعلق بالضرورة والتناسب. ففي كازاخستان، يُلزم مقدمو الخدمات بالاحتفاظ بأرقام الهواتف وعناوين البريد الإلكتروني وعناوين بروتوكول الإنترنت ومعلومات الفواتير لمدة سنتين[٣٨]. ويطلب الاتحاد الروسي من الجهات الفاعلة الخاصة تخزين محتوى جميع محادثات العملاء ورسائلهم النصية لمدة ستة أشهر، وتخزين ما يتصل بها من بيانات فوقية لمدة ثلاث سنوات[٣٩]. كما يطلب البلدان تخزين هذه البيانات محلياً[٤٠]. وفي البلدان التي تكون فيها وسيلة الاتصال المهيمنة هي الهواتف المحمولة، هناك قوانين تلزم بتسجيل شريحة الاشتراك في الهواتف المحمولة وتقتضي من غالبية السكان الإفصاح عن معلومات تحدد الهوية الشخصية (انظر A/HRC/29/32، الفقرة ٥١). إن إلزام مقدمي الخدمات بالاحتفاظ بكميات ضخمة من بيانات المستخدمين يتناقض مع معايير الإجراءات القانونية الواجبة، مثل ضرورة وجود اشتباه شخصي في ارتكاب عمل مخالف للقانون.

إنهاء التشفير

٢١- منذ صدور تقرير المقرر الخاص عن التشفير وإخفاء الهوية (A/HRC/29/32)، تزايدت على الصعيد العالمي التدابير غير الضرورية وغير المتناسبة فيما يتعلق بإنهاء التشفير وهي تهدد بتقويض حرية التعبير والأمن الرقمي للمستخدمين. وفي المملكة المتحدة لبريطانيا العظمى وآيرلندا الشمالية، على سبيل المثال، يجيز قانون تنظيم سلطات التحقيق لعام ٢٠١٦ أن يصدر وزير الدولة "إشعارات بشأن القدرة التقنية" يطلب فيها من موفري الخدمات رفع "الحماية الإلكترونية" عن الاتصالات – تدبير يمكن أن يوجد ثغرة أمنية أو يقيد التشفير أو يضعفه[٤١].

(٣٥) انظر التقرير المقدم من كندا، صفحة ٦.

(٣٦) البرتغال، قانون الإجراءات الجنائية، المواد ١٨٧-١٩٠.

(٣٧) بنغلاديش، قانون تنظيم الاتصالات السلكية واللاسلكية (٢٠٠١) الباب ٩٧.

(٣٨) كازاخستان، القرار الحكومي رقم ١٥٩٣ (٢٣ كانون الأول/ديسمبر ٢٠١١).

(٣٩) المفوضية السامية لحقوق الإنسان، رسالة إلى حكومة الاتحاد الروسي، ٢٨ تموز/يوليه ٢٠١٦ (OL RUS 7/2016).

(٤٠) Article 19 submission, p. 5.

(٤١) المملكة المتحدة لبريطانيا العظمى وآيرلندا الشمالية، قانون تنظيم سلطات التحقيق، المادة ٢٥٣(٢٠١٦)؛ والمفوضية السامية لحقوق الإنسان، رسالة إلى حكومة المملكة المتحدة، ٢٢ كانون الأول/ديسمبر ٢٠١٥ (AL GBR 4/2015).

ولم تقدم الدول أدلة كافية تبيّن أن إضعاف الحماية الأمنية على هذا النحو هو أقل الوسائل تدخلاً من أجل حماية الأمن القومي والنظام العام، لا سيما بالنظر إلى نطاق وعمق أدوات التحقيق الأخرى المتاحة لها (المرجع نفسه، الفقرة ٣٩).

الوصول المباشر

٢٢- إن الوصول المباشر إلى الإنترنت وشبكات الاتصالات السلكية واللاسلكية يمكن السلطات من اعتراض الاتصالات ورصدها دون خشية من الرقابة القانونية أو المساءلة. وقد عزز التقدم التكنولوجي قدرة الجهات المعنية بإنفاذ القانون ووكالات الاستخبارات على الوصول المباشر إلى الشبكات دون مشاركة أو علم مشغلي الشبكات[٤٢]. وخلال الانتخابات العامة التي جرت عام ٢٠١٤ في جمهورية مقدونيا اليوغوسلافية سابقاً، يُزعم أن سلطات الاستخبارات تمكنت من الوصول المباشر إلى الشبكات الرئيسية للاتصالات السلكية واللاسلكية في البلد لاعتراض اتصالات أكثر من ٢٠ ٠٠٠ شخص، بينهم سياسيون ومسؤولون حكوميون وصحفيون. وتلقى العديد من المستهدفين نسخاً من اتصالاتهم الهاتفية[٤٣]. وفي الهند، يبدو أن السلطات تعكف على تطوير نظام رصد مركزي يتيح "حصول الوكالات الحكومية على الأرقام المستهدفة بصورة إلكترونية من خلال شبكة آمنة دون أي تدخل من مقدمي خدمات الاتصالات السلكية واللاسلكية"[٤٤]. ولا يبدو أن هذه الأنشطة تُنفّذ بموجب نص قانوني، وهي غير خاضعة للحصول على إذن قضائي أو رقابة خارجية. وعلاوة على ذلك، فهي تشكل مخاطر على أمن وسلامة الهياكل الأساسية للشبكات تثير شواغل تتعلق بالتناسب.

جيم- حياد شبكة الإنترنت

٢٣- حياد شبكة الإنترنت - هو المبدأ المتمثل في ضرورة التعامل مع جميع بيانات الإنترنت بصورة متساوية ودون تدخل لا موجب له - يعزز الوصول إلى المعلومات على أوسع نطاق ممكن[٤٥]. وفي هذا العصر الرقمي، لا تكون حرية الاختيار بين مصادر المعلومات هادفة إلا عندما يتم بث محتوى وتطبيقات الإنترنت دون تمييز لا موجب له أو تدخل من جانب جهات فاعلة من غير الدول، بما في ذلك الجهات التي توفر خدمات الإنترنت. إن واجب الدولة الإيجابي المتمثل في تعزيز حرية التعبير يدعو بقوة إلى حياد الشبكة من أجل تعزيز الوصول إلى المعلومات بصورة غير تمييزية وعلى أوسع نطاق ممكن.

تحديد الأولويات المدفوع الأجر

٢٤- وفقاً لبرامج تحديد الأولويات المدفوع الأجر، يتعامل مقدمو خدمات الإنترنت معاملة تفضيلية مع أنواع معينة من المعلومات مقارنة بغيرها، وذلك نظير مقابل مالي أو مزايا تجارية أخرى. وهذه البرامج تؤدي بالفعل إلى إنشاء مسارات شبكية سريعة لمقدمي المحتوى الذين

(٤٢) Privacy International submission; and Telecommunications Industry Dialogue submission, p. 3.

(٤٣) Privacy International, "Macedonia: Society On Tap" (23 March 2016).

(٤٤) Access Now submission, part II, p. 4.

(٤٥) Luca Belli submission; and Article 19 submission, pp. 7-8.

يمكنهم دفع مبالغ إضافية، ومسارات بطيئة لسائر الجهات الأخرى[٤٦]. وتؤدي هذه التراتبية في تدفق البيانات إلى التأثير على خيارات المستخدمين. ويعاني المستخدمون من ارتفاع التكاليف أو تدني جودة الخدمة عندما يحاولون الوصول إلى محتوى وتطبيقات الإنترنت في مسارات بطيئة. وفي الوقت نفسه، قد يضطرون دون علمهم أو طلبهم إلى التعامل مع محتوى يحظى بالأولوية.

٢٥- وهناك العديد من الدول التي تحظر الأولويات المدفوعة الأجر. فعلى سبيل المثال، فإن هولندا، وهي من أوائل الدول التي تبنت حياد شبكة الإنترنت، تمنع موفري الخدمات من تحديد "أسعار الوصول إلى الإنترنت حسب الخدمات والتطبيقات التي تُقدم أو تستخدم عن طريق برامج تحديد الأولويات"[٤٧] كما أن الأمر المتعلق بشبكة الإنترنت المفتوحة الصادر عام ٢٠١٥ عن لجنة الاتصالات الاتحادية في الولايات المتحدة يحظر "قيام جهة مالكة لشبكة ذات نطاق عريض بمنح الأفضلية بطريقة مباشرة أو غير مباشرة لتدفق بعض البيانات على حساب غيرها نظير مقابل (مالي أو غيره) من طرف ثالث، أو لفائدة كيان منتسب للشبكة"[٤٨].

توفير الخدمة دون مقابل

٢٦- توفير الخدمة دون مقابل يتمثل في عدم فرض رسوم على استخدام بيانات الإنترنت المرتبطة بتطبيق أو خدمات بعينها؛ أو على خدمات أو تطبيقات أخرى تكون خاضعة في الوقت نفسه لحساب التكاليف حسب فترة الاستخدام. وترتيبات توفير الخدمة دون مقابل تتراوح بين برامج توفير البيانات التي تعفي بعض خدمات الإنترنت من حساب استخدام المشترك إلى توفير الوصول غير المحسوب إلى خدمات معينة دون الحاجة إلى شراء برنامج للحصول على الخدمة[٤٩]. وعلى الرغم من التفاوتات، فإن ترتيبات الخدمة دون مقابل توفر ميزة الوصول إلى المحتويات وقد تزيد تكلفة الحصول على البيانات الخاضعة للحساب. وبالنسبة للمستخدمين الذين يعانون من تكبد تكاليف الحصول على البيانات المحسوبة التكلفة، فقد ينتهي بهم الأمر إلى الاعتماد حصراً على الخدمات المقدمة دون مقابل، ما يؤدي إلى محدودية الوصول إلى المعلومات بالنسبة لمجتمعات قد تكون مهمشة أصلاً فيما يخص الوصول إلى المعلومات والمشاركة في الحياة العامة.

٢٧- وترتيبات الخدمة دون مقابل قد توفر الوصول بشكل محدود إلى خدمة الإنترنت في مناطق قد تفتقر لهذه الخدمة تماماً لولا ذلك[٥٠]. بيد أن الوصول إلى الإنترنت على نطاق أوسع

---

(٤٦) Dawn C. Nunziato and Arturo J. Carrillo, "The price of paid prioritization: The international and domestic consequences of the failure to protect Net neutrality in the United States", Georgetown Journal of International Affairs: International Engagement on Cyber V: Securing Critical Infrastructure (2 October 2015), p. 103.

(٤٧) هولندا، قانون الاتصالات السلكية واللاسلكية، المادة ٧-٤ ألف (٣).
Telecommunications Act. ders on ber Vlo, ernet Intermediaries, or Assessing Benefits and Harms e 19. lecom service providers on.

(٤٨) United States of America, Federal Communications Commission, Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 18. This Order, possibly under threat at the time of writing the present report, remains a useful template for net neutrality regulation.

(٤٩) Erik Stallman and R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms", Center for Democracy and Technology (January 2016).

(٥٠) المرجع نفسه، الصفحتان ٤ و١١.

قد يظل بعيد المنال عن المستخدمين، ما يجعلهم محبوسين دوماً في مجال شبكي محصور[٥١]. وثمة حاجة إلى إجراء دراسة أوسع نطاقاً بشأن افتراض أن محدودية الوصول ستتحول في نهاية المطاف إلى ربط شبكي كامل. وقد يعتمد ذلك على عوامل من قبيل سلوك المستخدمين، وظروف السوق، والمشهد العام لحقوق الإنسان والبيئة التنظيمية[٥٢].

٢٨- وقد أدت هذه الاعتبارات المتضاربة إلى تباينات في النهج التنظيمية. ففي الهند، انتهت الشواغل العامة بشأن تطبيقات فيسبوك الأساسية المجانية إلى حظر أي ترتيب "يؤدي إلى فرض تعريفات تمييزية على خدمات البيانات التي تقدم إلى المستخدمين مجاناً أو بمقابل على أساس المحتوى"[٥٣]. وهناك قيود على الخدمة دون مقابل تفرضها كل من شيلي والنرويج وهولندا وفنلندا وآيسلندا وإستونيا ولاتفيا وليتوانيا ومالطة واليابان[٥٤]. وفي المقابل، اعتمدت الولايات المتحدة، ثم لاحقاً الهيئة الأوروبية لمنظمي الاتصالات الإلكترونية، مبادئ توجيهية تتعلق بتناول كل حالة على حدة[٥٥]. والدول التي تعتمد مبدأ دراسة كل حالة على حدة ينبغي لها أن تدقق بعناية وأن ترفض، عند الاقتضاء، الترتيبات التي من شأنها، في جملة أمور، أن توفر مجانية الوصول إلى محتوى خاص بجهات منتسبة، أو تشترط توفير مجانية الخدمة مقابل مبالغ مالية أو تعطي أفضلية الوصول إلى تطبيقات بعينها ضمن فئة من التطبيقات المماثلة (على سبيل المثال، توفير مجانية الوصول إلى خدمات بث موسيقى محددة دون سواها). وبالإضافة إلى ذلك، ينبغي للدول أن تشترط على الشركات الكشف بصورة مجدية عن ممارسات إدارة تدفق المعلومات. فعلى سبيل المثال، تطلب شيلي من مقدمي خدمات الإنترنت الكشف عن سرعة الوصول إلى الإنترنت، وفروقات التكلفة والسرعة بين الروابط الوطنية والدولية، وضمانات الخدمات ذات الصلة[٥٦].

ثالثاً- مقدمو الخدمات الرقمية وحرية التعبير

٢٩- يقع على عاتق الدول واجب راسخ فيما يتعلق باحترام وحماية حرية التعبير، بيد أن الجهات الفاعلة الخاصة التي تنشئ خدمات الوصول الرقمي وتشغلها وتصينها تضطلع بدور حاسم أيضاً في هذا المجال.

(٥١) Barbara van Schewick, "Network neutrality and zero-rating", submission to the United States Federal Communications Commission (19 February 2014), p. 7.

(٥٢) Erik Stallman and R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms" (January 2016), p. 15.

(٥٣) India, Telecom Regulatory Authority, "TRAI releases the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016", press release (8 February 2016).

(٥٤) Emily Hong, "A zero sum game? What you should know about zero-rating", *New America Weekly*, Edition 109 (4 February 2016).

(٥٥) United States, Federal Communications Commission, Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 21; and BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (August 2016) (BoR (16) 127).

(٥٦) Chile, Ley No. 20.453, art. 24 H (D).

ألف- الاتصالات السلكية واللاسلكية ومقدمو خدمات الإنترنت

٣٠- شركات الاتصالات السلكية واللاسلكية، ومقدمو خدمات الإنترنت (يُشار إليهم جميعاً في هذا التقرير بعبارة "مقدمو الخدمات") يقدمون طائفة متنوعة من الخدمات. وفي حين أن هذه الجهات تعمل أساساً في مجال تشغيل وبيع خدمة الوصول إلى سلسلة من الشبكات تشمل شبكة الإنترنت، فهي تمكن المستخدمين أيضاً من التواصل وتقاسم المعلومات من خلال الخدمات الجوالة والخطوط الهاتفية الأرضية التقليدية (انظر A/HRC/32/38، الفقرة ١٦). ولا تزال الجهات المقدمة للخدمات مملوكة للدولة في العديد من المناطق، غير أن هناك عدداً متزايداً من الجهات التي أنشأها القطاع الخاص ويتولى إدارتها. وما فتئت هذه الصناعة تتخذ طابعاً متعدد الجنسيات: بعضٌ من أكبر مقدمي الخدمات على الصعيد العالمي يقوم بشغيل شبكات في عدة بلدان ومناطق، وغالباً ما يكون ذلك عن طريق شراكات مع شركات محلية أو فروع خاصة بالشركات الأم.

٣١- ويواجه مقدمو الخدمات، بوصفهم مسؤولين عن شبكات معلومات كبيرة، ضغوطاً كبيرة من جانب الحكومات لإجبارهم على الامتثال لأنشطة الرقابة والمراقبة. ولتشغيل شبكة في بلد ما، يجب على مقدمي الخدمات الاستثمار بصورة كبيرة في الهياكل الأساسية المادية والتجارية، بما يشمل معدات الشبكات والموظفين. وعادة ما يخضعون لقوانين محلية وغيرها من شروط إصدار التراخيص الواردة في اتفاقات مع الدول. وبالإضافة إلى الضغوط القانونية، يواجه مقدمو الخدمات ممارسات تخويف خارج نطاق القانون، مثل تهديد سلامة موظفيها وهياكلها الأساسية في حالة عدم الإذعان[٥٧].

٣٢- ويحاول العديد من مقدمي الخدمات مقاومة طلبات الرقابة والمراقبة، بيد أن العديدين منهم يساعدون الحكومات في جهودها في هذا المجال دون الاعتراض عليها بصورة مجدية. وفي الولايات المتحدة، يُدعى أن أحد أكبر مقدمي الخدمات في البلد قد استحدث "محرك بحث عالي الكفاءة" لتيسير وصول الجهات المكلفة بإنفاذ القانون إلى الاتصالات الهاتفية للعملاء، مع أنه غير ملزم قانوناً بأن يفعل ذلك[٥٨]. وفي المملكة المتحدة، قُدمت شكوى إلى منظمة التعاون والتنمية في الميدان الاقتصادي يُدعى فيها أن مقدمي خدمات رئيسيين منحوا وكالة الاستخبارات في البلد إمكانية الوصول إلى شبكاتهم وبيانات المشتركين بصورة تتجاوز ما هو مطلوب بموجب القانون آنذاك[٥٩].

٣٣- وهناك عدد متزايد من مقدمي الخدمات الذين يعكفون على وضع ترتيبات مع وسائل الإعلام وغيرها من الشركات المنتجة للمحتوى على نحو يهدد حياد الشبكة، ويمارسون ضغوطاً مكثفة من أجل الحصول على تنازلات فيما يتعلق بمعايير حياد شبكة الإنترنت. فعلى سبيل المثال، وفي حين يعكف المنظمون الأوروبيون على وضع مبادئ توجيهية بشأن حياد الإنترنت، فقد أصدر ١٧ من مقدمي الخدمات الرئيسيين في المنطقة "البيان المتعلق بتكنولوجيا شبكات

(٥٧) Telecommunications Industry Dialogue submission, p. 10.

(٥٨) Dave Maass and Aaron Mackey, "Law enforcement's secret 'super search engine' amasses trillions of phone records for decades", Electronic Frontier Foundation (29 November 2016).

(٥٩) المنظمة الدولية لحماية الخصوصية، "الشكوى المقدمة من منظمة التعاون والتنمية في الميدان الاقتصادي ضد بريتيش تيليكوم، مؤسسة فيريزون فودافون كيبل، وشركة فيتيل، وإنتروورت".

الجيل الخامس (G5)" الذي يحذرون فيه من أن وضع مبادئ توجيهية "مفرطة التقييد" من شأنه أن يؤخر الاستثمار في هذه التكنولوجيا التي تشكل الجيل القادم من شبكات الهاتف الجوال عبر الإنترنت[٦٠].

باء- نقاط تبادل الإنترنت

٣٤- تتيح نقاط تبادل الإنترنت (نقاط التبادل) تبادل حركة المعلومات عبر الإنترنت داخل وفيما بين الشبكات التي تديرها مجموعة مختلفة من مقدمي الخدمات داخل بلد أو إقليم[٦١]. وهذا الشكل من الترابط يحول دون مرور حركة الإنترنت، على المستوى المحلي أو الإقليمي، عبر مسارات دولية طويلة وملتوية، مما يحسّن من سرعة وكفاءة الاتصال بشبكة الإنترنت. ومن الممكن أن تتولى شركات الهياكل الأساسية للإنترنت إنشاء نقاط تبادل، كجزء من مجموعة واسعة من الخدمات التي تُباع إلى مقدمي الخدمات أو تُدار كمنظمات غير ربحية أو طوعية[٦٢].

٣٥- وتتداول نقاط التبادل حجماً هائلاً من حركة الإنترنت، ويمكن ترشيحها أو اعتراضها بناءً على طلب الحكومة. ويشير العدد المتزايد لعمليات الرقابة والمراقبة باستخدام نقاط التبادل إلى أن هذه النقاط هي نقاط اختناق رئيسية، حتى وإن كان دورها غير واضح على نحو دقيق. ففي عام ٢٠١٣، مثلاً، بينت الطريقة التي جرى بها منع الاتصال بموقع يوتيوب في باكستان أن هذه المنصة جرى ترشيحها عن طريق نقاط التبادل، لا عن طريق مقدمي خدمة الإنترنت، وذلك بطريقة تُعرف باسم "اعتراض حزم البيانات"[٦٣]. وتشير مذكرة داخلية مسرّبة أعدتها جهة متعددة الجنسيات تعمل في مجال تقديم خدمة الإنترنت في إكوادور إلى أن المستخدمين لم يتمكنوا من الاتصال بموقعي غوغل ويوتيوب في آذار/مارس ٢٠١٤ لأن جمعية مقدمي خدمات الإنترنت في إكوادور، وهي هيئة خاصة تدير اثنتين من نقاط التبادل الرئيسية في البلد، "منعت الاتصال بمواقع معينة على الإنترنت بناءً على طلب الحكومة الوطنية"[٦٤]. وقد أثار الكشف عن عمليات مراقبة واسعة تقوم بها وكالة الأمن الوطني بالولايات المتحدة قلقاً لدى التكنولوجيين من أن تعترض الوكالة جزءاً كبيراً من حركة الإنترنت المحلية والخارجية باستهداف نقاط التبادل في الولايات المتحدة[٦٥]. وفي أيلول/سبتمبر ٢٠١٦، رفضت أكبر نقطة تبادل للإنترنت في العالم، موجودة في ألمانيا، الأوامر القانونية التي أصدرتها وكالة الاستخبارات في البلد بمراقبة الاتصالات الدولية التي تمر عبر محورها[٦٦].

---

(٦٠) Article 19 submission, p. 9.

(٦١) انظر www.bgp4.as/internet-exchanges/.

(٦٢) Jason Gerson and Patrick Ryan, "A primer on Internet exchange points for policymakers and non-engineers" *Social Science Research Network* (12 August 2012), p. 10.

(٦٣) Zubair Nabi, "The anatomy of web censorship in Pakistan" (2013), p. 4.

(٦٤) Katitza Rodriguez, "Leaked documents confirm Ecuador's Internet censorship machine", Electronic Frontier Foundation (14 April 2016).

(٦٥) Andrew Clement and Jonathan Obar, "Canadian Internet 'boomerang' traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges", *in Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Michael Geist, ed. (University of Ottawa Press, 2015).

(٦٦) De Cix, "Information on the lawsuit against the Federal Republic of Germany" (16 September 2016).

جيم- شبكات إيصال المحتوى

٣٦- تُعرَّف شبكات إيصال المحتوى بأنها شبكة من أجهزة الخادوم موزعة توزيعاً استراتيجياً حول العالم بهدف الإيصال الفعال للصفحات الشبكية وغير ذلك من محتوى الإنترنت. ويعتمد منتجو المحتوى الضخم على هذه الشبكات من أجل الوصول إلى أكبر عدد من المستخدمين في أسرع وقت ممكن[٦٧]. وتخزن شبكة إيصال المحتوى نسخاً من المحتوى الذي تستضيفه على هذه المنصات، وتعيد توجيه أي طلب من المستخدمين للوصول إلى هذا المحتوى من أجهزة خادوم المنصة إلى أجهزة الخادوم في شبكتها الموجودة في أقرب مكان إلى المستخدم[٦٨]. وتؤدي هذه العملية إلى تحسين سرعة إيصال المحتوى، لا سيما إلى المستخدمين البعيدين عن أجهزة خادوم المنصة. وتُعتبر شركات إيصال المحتوى وسيلة فعالة للحماية من حجب المواقع الشبكية؛ ولا تؤثر إجراءات الرقابة على أجهزة الخادوم التي تستضيف موقعاً شبكياً معيناً أو منصة معينة على قدرة شبكة إيصال المحتوى على إيصال نسخ من المحتوى نفسه إلى المستخدمين[٦٩]. كما أصبحت شبكات إيصال المحتوى حاجزاً مهماً ضد أعطال الشبكة. وقد حفّز الطلب على الوصول السريع منتجي المحتوى الضخم على استثمار موارد كبيرة في الهياكل الأساسية والخدمات التي يمكنها أن تتصدى لهجمات منع الخدمة الموزَّع وغيرها من الهجمات الخبيثة[٧٠].

٣٧- ومرونة تصدي شبكات إيصال المحتوى للرقابة قد جعلتها أهدافاً تتعرض لقيود غير متناسبة على حرية التعبير. ففي مصر، أدى حجب موقع *العربي الجديد* في آب/أغسطس ٢٠١٦ إلى منع الوصول إلى محتوى المواقع الأخرى التي تتشارك في نفس شبكة إيصال المحتوى، رغم عدم انتماء هذه المواقع إلى موقع العربي الجديد، مما حدا بالباحثين إلى الاعتقاد بأن السلطات استهدفت تلك الشبكة بعينها[٧١]. وفي الصين، تشير التقارير إلى حجب شبكة إيصال المحتوى المسماة EdgeCast عن طريق مرشح وطني، وتعرض هذه الشبكة محتوى عدد من المواقع الشبكية الكبرى في البلد[٧٢].

٣٨- ونظراً إلى أن شبكات إيصال المحتوى تعالج أعداداً كبيرة من الطلبات المقدمة من المستخدمين للوصول إلى محتوى الإنترنت في مواقع شبكية ومنصات متعددة، تخضع هذه الشبكات أيضاً لمراقبة الحكومة. ففي عام ٢٠١٦، مثلاً، أفادت شبكة خدمات أمازون ويب Amazon Web Services، التي تضم واحدة من أكبر شبكات إيصال المحتوى في العالم[٧٣]، بأن عدد الطلبات الحكومية للوصول إلى البيانات تضاعف بأكثر من ضعفين بالمقارنة مع العام السابق[٧٤]. ويعتقد الباحثون أيضاً أن أنشطة المراقبة الجماعية تستهدف على نحو استراتيجي

(٦٧) Geoff Huston, "The death of transit?", Asia Pacific Network Information Centre (27 October 2016).

(٦٨) Vangie Beal, "CDN - Content Delivery Network", *Webopedia*.

(٦٩) John Holowczak and Amir Houmansadr, "CacheBrowser: bypassing Chinese censorship without proxies using cached content" (2015).

(٧٠) Geoff Huston, "The death of transit?", Asia Pacific Network Information Centre (27 October 2016).

(٧١) Leonid Evdokimov and Vasilis Ververis, "Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections?", Open Observatory of Network Interference (27 October 2016).

(٧٢) Joss Wright, "A quick investigation of EdgeCast CDN blocking in China", blog, Oxford Internet Institute (18 November 2014).

(٧٣) في وقت كتابة هذا التقرير، كانت شبكة Amazon Cloudfront تخدم أكبر عدد من المجالات الشبكية في العالم.

(٧٤) Amazon Information Request Report (June 2016).

شبكات إيصال المحتوى من أجل زيادة جمع المعلومات إلى أقصى حد ممكن، أما كيفية إجراء ذلك ونطاق مشاركة شبكات إيصال المحتوى، إن وُجدت، فغير واضحين[٧٥].

دال- بائعو معدات الشبكات

٣٩- يوفر البائعون المعدات والبرمجيات التي تشكل الأساس لشبكات الإنترنت والاتصالات السلكية واللاسلكية. وتشمل معدات الشبكات كلاً من الموجهات والمفاتيح ونقاط الوصول، مما يمكِّن من الربط بين أجهزة وشبكات متعددة (انظر A/HRC/32/38، الفقرة ١٨). كما نوَّع البائعون أنشطتهم لكي يوفروا معدات نقل الصوت باستخدام بروتوكول الإنترنت، وهي المعدات التي تمكِّن من إجراء مكالمات لا سلكية، وتكنولوجيا إنترنت الأشياء التي تتيح الربط الشبكي فيما بين الأجهزة الذكية[٧٦]. ونادراً ما يتعامل البائعون مباشرةً مع المشترين: فعملاؤهم الرئيسيون هم مشغلو الإنترنت، كالحكومات أو مقدمي خدمة الإنترنت أو شبكات إيصال المحتوى. ونتيجةً لذلك، ينبغي للبائعين تهيئة الشبكات بما يطابق المعايير التقنية المحددة من هؤلاء المشغلين، بما في ذلك المعايير التي يفرضها القانون المحلي (مثل متطلبات إنفاذ القانون والأمن الوطني). غير أن البائعين يمكنهم أيضاً تصميم أو تعديل المعدات والتكنولوجيا بما يضمن مطابقتها للمواصفات الخاصة أو الحكومية.

٤٠- وبالنظر إلى النموذج التجاري للبائعين، يجب عليهم تقصي تحديات حقوق الإنسان التي يواجهها أو يهيئها عملاؤهم. ففي مجال المراقبة، كثيراً ما يلتزم البائعون بإجراءات "الاعتراض القانوني"، التي تتطلب تهيئة الشبكات على نحو يمكّن الحكومة من الوصول إلى بيانات المستخدمين[٧٧]. وبالإضافة إلى ذلك، قد يُتعاقد مع البائعين على إنشاء "نظم للإدارة والوساطة" تيسّر تبادل البيانات المعترضة بين مشغلي الإنترنت والسلطة الحكومية، فضلاً عن النظم الحكومية التي تعالج البيانات المعترضة[٧٨]. وفي إطار الترتيبات التي يدير بموجبها البائعون الشبكات التي يقيمونها، قد يتحملون أيضاً مسؤولية تلبية الطلبات المقدمة من الحكومة للحصول على بيانات المستخدمين نيابة عن المشغِّل[٧٩].

٤١- ويثير تصميم معدات وتكنولوجيا الشبكات المتعددة الاستخدامات شواغل تتعلق بحرية التعبير والخصوصية. فأجهزة تفقُّد الرزمة العميق، مثلاً، تُستخدم لأغراض تقنية غير ضارة، مثل إدارة اكتظاظ الشبكات، ولكنها استُخدمت أيضاً لترشيح محتوى الإنترنت، واعتراض الاتصالات، وتقليص سرعة تدفق البيانات. وتُهيئ شبكات الهواتف المحمولة بحيث يمكنها رصد مواقع الهواتف الخلوية لضمان استخدام خدمات الهواتف المحمولة من أي مكان، غير أن هذا الرصد قد يُستخدم أيضاً لاستهداف المستخدمين[٨٠].

---

(٧٥) انظر، مثلاً، Harrison Weber, "How the NSA & FBI made Facebook the perfect mass surveillance tool", *Venture Beat* (15 May 2014).

(٧٦) Michael E. Raynor and Phil Wilson, "Beyond the dumb pipe: The IoT and the new role for network service providers", Deloitte University Press (2 September 2015).

(٧٧) انظر، مثلاً، Council of the European Union resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal C 329; and Privacy International submission, pp. 2-3.

(٧٨) IHRB, "Human rights challenges of telecommunications vendors: addressing the possible misuse of telecommunications systems: case study: Ericsson" (November 2014), p. 16.

(٧٩) المرجع نفسه، الصفحة ١٧.

(٨٠) المرجع نفسه، صفحة ١٣.

٤٢- وتشير بعض الأدلة إلى أن البائعين قد يدعمون إجراءات الرقابة والمراقبة التي تتخذها الحكومات. ففي قضية منظورة أمام محاكم الولايات المتحدة، اتُّهمت شركة سيسكو CISCO بتصميم وتنفيذ وصيانة شبكة صينية للمراقبة والأمن الداخلي، تُعرف باسم Golden Shield[٨١]. (تنفي شركة سيسكو تلك الادعاءات)[٨٢]. وفي إثيوبيا، توصلت مجموعات حقوق الإنسان إلى أن شركة ZTE صممت وركّبت قاعدة بيانات لإدارة العملاء لشركة Ethio Telecom، أتاحت إمكانية المراقبة التدخلية[٨٣].

هاء- أطراف فاعلة خاصة أخرى

٤٣- تنطبق النتائج والتوصيات الواردة في هذا التقرير على أي كيان يشترك في تقديم خدمة الوصول الرقمي على النحو المبين أعلاه. ويتزايد عدد شركات الإنترنت التي تضيف إلى مهامها خدمات مهمة تتعلق بالوصول الرقمي والهياكل الأساسية الرقمية. فمثلاً، تقدم الآن أيضاً شركتا Alibaba وTencent، وهما من أكبر شركات الإنترنت الصينية، خدمات شبكات إيصال المحتوى[٨٤]. وتجرِّب شركة غوغل أساليب لتقديم خدمات الوصول اللاسلكي بطريقة تتجاوز مقدمي الخدمات التقليديين؛ وفي عام ٢٠١٠، أطلقت غوغل خدمة الاتصال بالإنترنت العالي السرعة للمنازل والشركات في مدن مختارة في الولايات المتحدة[٨٥]. وتتعاون غوغل أيضاً مع فيسبوك ومايكروسوفت على مد شبكات كابلات في عمق البحر للربط بين المستخدمين دون الاعتماد على معدات أو نظم تابعة لطرف ثالث[٨٦].

٤٤- وتضع منظمات وضع المعايير، رغم أنها ليست "أطرافاً فاعلة في هذه الصناعة" بالمعنى الدقيق، بروتوكولات ومعايير تقنية تتيح إمكانية التشغيل البيني في الاتصالات السلكية واللاسلكية والهياكل الأساسية للإنترنت. وقد يؤثر وضع المعايير، التي تتجاهل اعتبارات حقوق الإنسان، سلبياً على حرية التعبير. فمثلاً، أدى عدم إدراج طبقة لتأمين نقل البيانات كعنصر في بروتوكول لغة نقل النصوص (HTTP) إلى تعريض حركة الشبكة للرقابة والمراقبة. ولذلك فإن جهود المجتمع التقني الرامية إلى إدراج العناية الواجبة بحقوق الإنسان في عملية وضع المعايير هي خطوة في الاتجاه الصحيح[٨٧].

---

(٨١) United States District Court for the Northern District of California, San Jose Division, *Doe et al. v. Cisco Systems, Inc. et al.*, Case No. 5:11-cv-02449-EJD-PSGx (18 September 2013).

(٨٢) John Earnhardt, "Cisco Q&A on China and censorship" Cisco blogs (2 March 2006).

(٨٣) Human Rights Watch, "They know everything we do: telecom and Internet surveillance in Ethiopia" (25 March 2014).

(٨٤) Tencent Cloud CDN and Alibaba Cloud CDN.

(٨٥) Klint Finley, "Google eyes blazing-fast wireless as a way into your home", *Wired* (12 August 2016).

(٨٦) Joon Ian Wong, "Google and Facebook are doubling down on Internet infrastructure with a new Pacific cable", *Quartz* (17 October 2016).

(٨٧) Internet Research Task Force, "Research into human rights protocol considerations" (25 February 2017). Available at https://datatracker.ietf.org/doc/draft-irtf-hrpc-research/?include_text=1. The supplementary annex analyzes the roles and responsibilities of standards developing organizations in more detail.

رابعاً- مسؤوليات مقدمي خدمة الوصول الرقمي تجاه حقوق الإنسان

٤٥- تعترف المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان بمسؤولية الشركات التجارية عن احترام حقوق الإنسان، بغض النظر عن التزامات الدولة أو تنفيذ الدولة لتلك الالتزامات (انظر A/HRC/17/31، المرفق؛ وA/HRC/32/38، الفقرتان ٩ و١٠). وتمثل هذه المبادئ التوجيهية خطاً أساسياً أدنى لمساءلة الشركات عن حقوق الإنسان، حيث تحث الشركات على إصدار بيانات عامة بشأن الالتزام باحترام حقوق الإنسان، بدعم من الإدارة العليا أو الإدارة التنفيذية؛ وعلى تنفيذ عمليات العناية الواجبة التي "تحدد وتمنع وتخفِّف وتفسِّر"، على نحو مجدٍ، الآثار الفعلية والمحتملة لجميع عمليات الشركة على حقوق الإنسان، وتتيح علاج الآثار السلبية على حقوق الإنسان أو التعاون على علاجها (انظر A/HRC/17/31، المرفق، المبادئ من ١٦ إلى ٢٤).

ألف- اعتبارات السياق

٤٦- تشدد المبادئ التوجيهية على ضرورة مراعاة الشركات لخصائص سياق العمل عند تنفيذ مسؤولياتها المتعلقة بحقوق الإنسان (المرجع نفسه). ويجب مراعاة مختلف السياقات في صناعة الوصول الرقمي.

مقدمو خدمات الوصول يقدمون منفعة عامة

٤٧- تنتمي صناعة الوصول الرقمي إلى مجال التعبير الرقمي؛ وتعتمد صلاحيتها التجارية على المستخدمين الذين يلتمسون ويتلقون ويذيعون المعلومات والأفكار المتعلقة بالشبكات التي تقيمها هذه الصناعة وتشغِّلها. وبالنظر إلى أن الشبكات المملوكة للقطاع الخاص ضرورية للممارسة المعاصرة لحرية التعبير، يضطلع مشغلو هذه الشبكات أيضاً بمهام اجتماعية وعامة بالغة الأهمية. ومن شأن القرارات الصادرة عن تلك الصناعة، سواء أكانت استجابة لطلبات الحكومة أم نابعة من المصالح التجارية، أن تؤثر بشكل مباشر على حرية التعبير وعلى حقوق الإنسان ذات الصلة، بطرق مفيدة وضارة على السواء.

القيود المفروضة على الاتصال بالإنترنت تؤثر على حرية التعبير في العالم

٤٨- عادةً ما تتسم آثار هذه الصناعة على حقوق الإنسان بطابع عالمي، وتؤثر على المستخدمين ولو في الأسواق الأخرى غير الأسواق التي تخدمها الشركة المعنية. فمثلاً، من الممكن أن تؤدي مراقبة نقطة تبادل واحدة في الولايات المتحدة إلى رصد تدفقات ضخمة من الاتصالات فيما بين الأمريكيين والأجانب، بل والاتصالات الدائرة فقط فيما بين الأجانب. وبالمثل، تؤثر أوجه الضعف الأمنية الكامنة في تصميم الشبكات على جميع المستخدمين الذين يعتمدون على الشبكة الضعيفة في الاتصال الرقمي، بمن فيهم المستخدمون البعيدون عن الشبكة. وبناءً على ذلك، ينبغي للشركات أن تحدد وتعالج الآثار الواسعة لأنشطتها على حرية التعبير بشكل عام، بالإضافة إلى آثارها على العملاء أو أصحاب الحقوق في الأسواق التي تعمل بها. وللتأكد من ذلك، قد تختلف الطريقة التي تفسِّر بها هذه الشركات آثار أنشطتها بحسب حجمها ومواردها وملكيتها وهيكلها وسياق تشغيلها (المرجع نفسه، المبدأ ١٤). فمثلاً، ينبغي لجميع مقدمي الخدمات فحص طلبات الحصول على بيانات المستخدمين للتأكد من مطابقتها للمجموعة الدنيا من الإجراءات الرسمية، بغض النظر عن مصدر الطلب أو المستخدم المتأثر. ولكن في الوقت الذي قد تتوافر فيه لدى مقدم

الخدمة المتعدد الجنسيات أفرقة لفحص الطلبات، قد يكلِّف مقدم الخدمة الصغير الحجم أو المتوسط الحجم أفرقته المعنية بالسياسة القانونية أو العامة بأداء الوظيفة نفسها.

الصناعة معرضة لضغط الدولة على حرية التعبير

٤٩- تهدف المبادئ التوجيهية إلى علاج الفجوة في مساءلة الشركات، التي لا تُنفذ لعدم وجود تشريع وطني أو لعدم تنفيذه(٨٨). ورغم ذلك، يفرض الإنفاذ المتحمس للقانون المحلي تحديات لحقوق الإنسان في صناعة الوصول الرقمي. فمثلاً، قد تحمِّل الدولة مقدمي الخدمة المسؤولية عن محتوى الإنترنت الذي ينشره المستخدمون على شبكاتهم، أو قد تضغط عليهم الدولة لتقييد هذا المحتوى، وذلك بموجب قوانين متنوعة بقدر تنوع مسائل خطاب الكراهية والتشهير والجريمة الإلكترونية والمساس بالذات الملكية. غير أن هذه المسؤولية الوسيطة تهيئ حافزاً قوياً للرقيب: فقد يجد مقدمو الخدمات أن الأسلم هو عدم رفض هذا التنظيم وإنما الإفراط في تنظيم المحتوى بحيث يؤدي ذلك في نهاية الأمر إلى تقييد التعبير المشروع أو القانوني. ويتصاعد أيضاً الضغط الذي يهدف إلى المساعدة في الرقابة والمراقبة من جانب الدولة عندما تعمد السلطات إلى مضايقة أو تهديد أو اعتقال الموظفين أو محاولة التلاعب بشبكات الشركة أو معداتها(٨٩).

... وإنما أيضاً يحتل موقعاً فريداً يكفل احترام حقوق المستخدمين

٥٠- يؤدي الدور المزدوج لهذه الصناعة، بوصفها عاملاً يمكِّن من الوصول الرقمي ونقطة طبيعية للقيود المفروضة من الدولة، إلى زيادة أهمية الصناعة كحاجز أمام التدخل المفرط من جانب الحكومات أو الجهات الخاصة. فمثلاً، عادةً ما يكون مقدمو الخدمة في أفضل وضع لوقف أي طلب بالإغلاق أو بالحصول على بيانات المستخدم. وتحتل شبكات إيصال المحتوى موقعاً استراتيجياً على الهياكل الأساسية للإنترنت لمواجهة الهجمات الخبيثة التي تعوق الوصول. ويتمتع البائعون بمؤهلات فريدة تمكِّنهم من تقييم ما إذا كانت منتجاتهم ستُستخدم، أو يجري استخدامها، لتيسير انتهاكات حقوق الإنسان، ولا سيما عندما يبذلون العناية الواجبة في سياق المبيعات أو يقدمون خدمات مستمرة.

باء- المسؤولية عن احترام حرية المستخدمين في التعبير

٥١- لكي تفعِّل صناعة الوصول الرقمي التزاماتها بحقوق الإنسان، ينبغي أن تخصص موارد مناسبة، على الأقل للممارسات المبينة فيما يلي. ورغم أن هذه المبادئ تُقيَّم في سياق الوصول الرقمي، فإن لها أيضاً صلة بقطاعات أخرى في الاقتصاد الرقمي، مثل وسائط التواصل الاجتماعي، والتجارة، والمراقبة، والبحث.

(٨٨) Yael Ronen, "Big Brother's little helpers: the right to privacy and the responsibility of Internet service providers", *Utrecht Journal of International and European Law*, vol. 31, No. 80 (February 2015), p. 76.

(٨٩) في عام ٢٠١٤، اقترن طلب إغلاق شبكات، تلقته شركة أورانج المتعددة الجنسيات المقدمة لخدمات الاتصالات السلكية واللاسلكية من سلطات جمهورية جنوب أفريقيا، وفقاً للتقارير، "بالتهديد بفرض عقوبات شخصية في حالة عدم الامتثال". انظر Telecommunications Industry Dialogue submission, p. 11.

١- بذل العناية الواجبة

٥٢- تمكِّن العناية الواجبة مقدم خدمة الوصول الرقمي من تحديد ومنع وتخفيف آثار أنشطته على حقوق الإنسان (انظر A/HRC/17/31، المرفق، المبدأ ١٩). وبينما لا يمكن تطبيق نُهُج العناية الواجبة التي تناسب جميع الحالات، أو لا يُنصح باتباعها، تشكِّل عمليات تقييم الأثر على حقوق الإنسان وسيلة لتقييم ومواجهة المخاطر المحدقة بحرية التعبير والخصوصية[٩٠]. وتشمل العناية الواجبة، على الأقل، ما يلي.

السياسات التي تنظم بذل العناية الواجبة

٥٣- ينبغي للشركات أن تضع معايير واضحة ومحددة لتحديد الأنشطة التي تشمل مقتضيات حرية التعبير وأن تطلق عمليات العناية الواجبة[٩١]. وتمثل الآثار الماضية والراهنة لأنشطة الشركة على حقوق الإنسان، وكذلك ممارسة الصناعة، مؤشرات مفيدة. وفي صناعة الوصول الرقمي، قد تشمل هذه الأنشطة عمليات اندماج وتملُّك؛ ودخول السوق أو الخروج منه؛ وطلبات حكومية أو غير حكومية لتقييد المحتوى أو الاطلاع على بيانات المستخدم؛ وفرض قيود على المحتوى وسياسات الخصوصية أو تغييرها؛ وتغيير المنتجات فيما يتعلق بمراقبة المحتوى أو الاتصالات المشفرة؛ والترتيبات التي تيسر أولوية الوصول إلى محتوى وتطبيقات الإنترنت؛ وتصميم وبيع وشراء معدات وتكنولوجيات اعتراض وترشيح الشبكات، والتدريب المرتبط بذلك؛ وخدمات المشورة[٩٢]. وهذه القائمة، غير الشاملة، "تتطلب العناية والتحديث المستمرين"، مع مراعاة المجالات الجديدة للأعمال التجارية، والتطورات في مجال التكنولوجيا، والتغيرات الأخرى في السياق التشغيلي[٩٣].

مسائل للدراسة

٥٤- ينبغي لعمليات بذل العناية الواجبة أن تدرس بصورة نقدية، على الأقل، القوانين والمعايير المحلية والدولية الواجبة التطبيق، بما في ذلك أوجه التعارض المحتملة بين القوانين المحلية وحقوق الإنسان؛ والمخاطر المحدقة بحرية التعبير والخصوصية، المتضمنة في منتجات الشركة وخدماتها؛ واستراتيجيات تخفيف ومنع هذه المخاطر؛ والحدود المفروضة على فعالية هذه الاستراتيجيات بالنظر إلى البيئة القانونية أو التنظيمية أو التشغيلية للشركة؛ وإمكانية تعزيز حقوق الإنسان في جميع عمليات الشركة[٩٤].

---

(٩٠) من أمثلة الشركات الكبرى المقدمة لخدمات الاتصالات السلكية واللاسلكية، التي أجرت عمليات تقييم لآثار أنشطتها على حقوق الإنسان، شركة Telia Company وشركة Telefonica. المرجع نفسه، الصفحتان ٧ و٨.

(٩١) أدمجت شركة نوكيا سمة آلية في أداة مبيعاتها تحصر مخاطر مبيعاتها المحتملة على حقوق الإنسان. المرجع نفسه، الصفحة ٧.

(٩٢) European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pp. 32-36.

(٩٣) Michael A. Samway, "Business, human rights and the Internet: a framework for implementation", in *Human Dignity and the Future of Global Institutions*, Mark P. Lagon and Anthony Clark Arend, eds. (Washington, D.C., Georgetown University Press, 2014), p. 308.

(٩٤) المرجع نفسه، الصفحات ٣١٠ إلى ٣١٢، للاطلاع على استعراض أكثر شمولاً للمجالات المواضيعية ذات الصلة التي ينبغي أن تشملها عمليات بذل العناية الواجبة.

العملية الداخلية والتدريب

٥٥- رغم أهمية الموظفين المهنيين المعنيين بالعمل التجاري وحقوق الإنسان في أية شركة، لا ينبغي أن يكون بذل العناية الواجبة مسؤوليتهم وحدهم، وإنما يجب أن تشترك فيها أفرقة أخرى فعالة داخل العمل التجاري. ويتطلب ذلك حواراً وتعاوناً فيما بين مختلف وحدات العمل التجاري (مثل الخصوصية، وإنفاذ القانون، والعلاقات الحكومية، والامتثال، وإدارة المخاطر، وتطوير المنتجات، والعمليات) والمهنيين (كالمهندسين، والباحثين في مجال خبرات المستخدمين، وأفرقة المبيعات، والتنفيذيين في العمل التجاري)[٩٥]. وفي سياق الخصوصية، توصّل الباحثون إلى أن بعض التدابير، مثل "إشراك كبار التنفيذيين في وحدات العمل التجاري وإسناد المسؤولية إليهم" عن إدارة الخصوصية و"إشراك الموظفين ذوي الخبرة في مجال حماية الخصوصية والمسؤولية الشخصية عن الخصوصية ... في وحدات العمل التجاري"، تهيئ بيئة مؤاتية لحماية الخصوصية[٩٦]. ومن الممكن أيضاً أن تكفل ممارسات إدارية مماثلة احترام العمل التجاري لحرية التعبير. وبالنسبة إلى الشركات الصغيرة والمتوسطة الحجم، قد تتطلب هذه الاعتبارات القيام بالعملية برمتها من أجل المشاركة في أنشطة العناية الواجبة[٩٧].

الخبرة الخارجية

٥٦- بالنظر إلى المعارف الواسعة المطلوبة، يجب أن تعتمد عمليات العناية الواجبة على خبرة خارجية غير حكومية، منها المجتمع المدني المحلي، والمنظمات الدولية لحقوق الإنسان، وآليات حقوق الإنسان التابعة للمنظمات الدولية والإقليمية، والدوائر الأكاديمية، والمجتمع التقني. وتتيح أيضاً المنتديات التي تشارك فيها عدة جهات صاحبة مصلحة فرصاً للتعلم المشترك والمساءلة المتبادلة. فمثلاً، توصل الباحثون إلى أن العضوية في مبادرات حقوق الإنسان في قطاع معين أو صناعة معينة، مثل مبادرة الشبكة العالمية والحوار في قطاع الاتصالات السلكية واللاسلكية، تتوافق مع أداء الشركات في مجال حقوق الإنسان[٩٨].

التشاور مع المستخدمين ومع أصحاب الحقوق المتأثرين

٥٧- يراعي جميع مقدمي خدمات الوصول الرقمي حرية المستخدم النهائي في التعبير، بطريقة أو بأخرى. وبناءً على ذلك، ينبغي للشركات، بما فيها الشركات التي لا تتعامل مباشرة مع المستهلكين، أن تتشاور مع المستخدمين النهائيين في إطار عملية تقييم المخاطر التي تجريها. ويختلف هذا التشاور عن الجهود المشار إليها أعلاه والمتعلقة بإشراك عدة جهات صاحبة مصلحة، ويهدف هذا التشاور إلى إجراء "حوار ثنائي الاتجاه" من أجل "جمع آراء محددة أو مشورة محددة من الجهات صاحبة المصلحة المتأثرة (أو من ممثليها) تُراعى بعد ذلك في عمليات الشركة المتعلقة باتخاذ القرارات الداخلية والتنفيذ"[٩٩]. فمثلاً، يمكن التشاور مع الأفراد والجماعات الضعفاء

(٩٥) European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 36.

(٩٦) Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Massachusetts, MIT Press, 2015), p. 177.

(٩٧) European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 37.

(٩٨) Ranking Digital Rights submission, p. 5.

(٩٩) European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pp. 37-38.

والمهمشين في الوقت الذي تتواصل فيها مفاوضات الترخيص في بيئات التشغيل العالية الخطر أو أثناء عمليات تصميم واختبار وتنفيذ سياسات تقديم الخدمة دون مقابل. وينبغي أيضاً أن يشمل التشاور الجدي التواصل المنتظم مع منظمات المجتمع المدني، التي قد تكون وسيطاً مفيداً لتلبية احتياجات ومصالح المستخدمين النهائيين في مجتمعات معينة، والتي قد تكون هي نفسها معرّضة على نحو أشد لخطر الضغط بسبب أنشطتها في مجال الدعوة.

التقييمات الدينامية الجارية

٥٨- ينبغي أن تسارع الشركات إلى مواءمة عمليات بذل العناية الواجبة بما يتفق مع التغيرات في الظروف أو في السياق التشغيلي. فمثلاً، يجب أن يستمر تقييم المخاطر بعد مرحلة التصميم وعلى فترات منتظمة طوال دورة حياة المنتج أو الخدمة، مع مراعاة بعض العوامل، كالتغيرات في التكنولوجيا وفي الهياكل الأساسية وما يرتبط بذلك من أوجه ضعف أمنية، والتغيرات في سلوك المستهلك، والتعديلات في البيئة القانونية والسياسية والاجتماعية التي تعمل فيها الشركات[١٠٠].

٢- إدراج ضمانات حقوق الإنسان عن طريق التصميم

٥٩- على غرار أي تطوير تكنولوجي رئيسي، تعكس خيارات التصميم والهندسة اعتبارات السياسة العامة وينبغي أن تسترشد بمبدأ احترام حقوق الإنسان. فمثلاً، من شأن تجزئة الشبكة network slicing، وهي أساسية لتكنولوجيا الجيل الخامس "5G"، أن تمكِّن مقدمي خدمات الهواتف المحمولة من إدارة حركة الإنترنت بكفاءة أفضل وتلبية مجموعة احتياجات المستهلكين الآخذة في التزايد في عصر إنترنت الأشياء. وفي الوقت نفسه، يمكن أيضاً "تجزئة" الشبكات إلى ممرات سريعة وبطيئة تمنح أولوية الوصول إلى بعض تطبيقات الإنترنت قبل تطبيقات أخرى، مما قد يتدخل في حيادية الشبكة. وبناءً على ذلك، يجب على الشركات أن تضمن أن ينسجم تصميم وانتشار الابتكارات في معدات تكنولوجيا الشبكات - لا سيما ذات الاستخدامات المتعددة - مع حرية التعبير ومع معايير الخصوصية[١٠١].

٦٠- وينبغي للشركات أن تضطلع بدور فعال وتشاركي في وضع تدابير تعزز حرية التعبير والخصوصية. فمثلاً، يجب أن تُطبَّق تدابير الأمن الرقمي التي تكتشف وتمنع هجمات الحرمان من الخدمة والاختراق بحيث تستهدف الحركة الخبيثة دون التأثير على التفاعلات المشروعة فيما بين الأفراد والمنظمات والمجتمعات. ومن شأن تهيئة معدات الشبكة بحيث تقلل إلى أدنى مستوى من عمليات جمع المعلومات غير الضرورية عن المستخدمين - بالنظر إلى المتطلبات القانونية المحلية ومتطلبات التوجيه - أن تمنع بصورة فعالة الطلبات الفضفاضة للحصول على بيانات عن المستخدمين، حيث لا يمكن للشركات أن تسلِّم معلومات ليست في حوزتها[١٠٢]. وحتى إذا سُجِّلت معلومات المستخدم، فمن شأن الحدود الموضوعية المتعلقة بما إذا كانت هذه المعلومات يُحتفظ بها أم لا ولأية مدة أن يحد أيضاً من نطاق البيانات الشخصية والحساسة المتاحة لطرف ثالث.

(١٠٠) Business and Social Responsibility, "Applying the Guiding Principles on Business and Human Rights to the ICT industry", Version 2.0: Ten lessons learned, A briefing paper (September 2012), p. 9.

(١٠١) ARTICLE 19, "Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?" (15 September 2016).

(١٠٢) Electronic Frontier Foundation, "User privacy for ISPs and accidental ISPs".

٣- مشاركة الجهات صاحبة المصلحة

٦١- من الممكن أن يؤدي تواصل هيئات حقوق الإنسان مع الحكومات والشركات الشريكة وغيرها من الجهات صاحبة المصلحة إلى منع أو تخفيف انتهاكات حقوق الإنسان مستقبلاً. وينبغي للشركات المتعاملة مباشرةً مع الحكومات أن تضغط من أجل إدراج ضمانات حقوق الإنسان في رخص التشغيل وعقود المبيعات، ويشمل ذلك إدراج تأكيدات بعدم استعمال معدات الشركة أو تعديلها دون معرفة الشركة (وهو ما يمكن أن يكون لغرض تيسير انتهاكات حقوق الإنسان). ومن الممكن أيضاً أن يؤدي التدخل في الوقت المناسب أثناء التقاضي (مثل إعداد المذكرات الصديقة للمحكمة في القضايا التي تقيمها جماعات المجتمع المدني أو الشركات النظيرة ضد قوانين الرقابة أو المراقبة)، والضغط الموجه لفائدة حقوق الإنسان في العمليات التشريعية وعمليات وضع السياسات، إلى تعزيز الحماية القانونية لحرية التعبير والخصوصية.

٦٢- وينبغي أن تؤدي الترتيبات المتخذة مع الشركات الشريكة إلى تمكين جميع الأطراف من الاضطلاع بمسؤولياتها تجاه حقوق الإنسان. وينبغي أن تُصمم هذه الترتيبات، بوجهٍ خاص، بحيث تضمن التزام الفروع والشركاء في الشركات المشتركة والموردين والموزعين بأية سياسات تنفذها الشركة بشأن حرية التعبير والخصوصية. فمثلاً، عندما تتلقى العمليات المحلية طلبات غير تقليدية بفرض الرقابة والمراقبة، يجب أن تضمن سياسة الشركة تصعيد هذه الطلبات إلى الإدارة العالمية لغرض مراجعتها[١٠٣]. وينبغي إتاحة آليات الإبلاغ عن المخالفات لكلٍ من الموظفين والمتعاقدين. فإن كانت الشركات مرتبطة بعلاقات تجارية تطرح شواغل بشأن حقوق الإنسان، ينبغي للشركات أن تسعى بمرور الوقت إلى تحقيق منع أو تخفيف الضرر[١٠٤].

٦٣- وقد تحسِّن الشركات أيضاً احترام حقوق الإنسان عن طريق الإجراءات التعاونية. ويشمل هذا التعاون أنشطة التوعية والدعوة المشتركة مع الشركات النظيرة؛ والتعاون مع الهيئات الإقليمية أو الدولية، بما في ذلك آليات حقوق الإنسان والمؤسسات الاقتصادية؛ والعضوية في الجمعيات الصناعية والمبادرات التي تطلقها جهات عديدة صاحبة مصلحة[١٠٥]. ومن الممكن أيضاً أن تؤدي المشاورات المنتظمة مع المستخدمين، والمجتمع المدني، وأصحاب الحقوق المتأثرين، إلى حشد الدعم العام لجهود الشركات لمقاومة التدخل المفرط من جانب الحكومات. ويعزز التعاون فيما بين القطاعات القوة المعيارية لأفضل الممارسات والمعايير المتفق عليها في مجال حقوق الإنسان، مما يكثف الضغط على كلٍ من الحكومات والشركات النظيرة لكي تمتثل.

٤- استراتيجيات التخفيف[١٠٦]

٦٤- إذا تلقت الشركات طلبات تتعلق بتنظيم المحتوى والحصول على بيانات المستخدمين، يمكن اعتماد سياسات وممارسات معينة ملائمة للتخفيف من أضرار القيود التي قد تفرضها الحكومات.

---

(١٠٣) Telecommunications Industry Dialogue submission, pp. 13 and 16.

(١٠٤) SHIFT, "Using leverage in business relationships to reduce human rights risks" (New York, November 2013).

(١٠٥) Telecommunications Industry Dialogue submission, p. 12; and Global Network Initiative submission, p. 7.

(١٠٦) استفاد التوجيه الوارد في هذا الجزء استفادة كبيرة من تقرير الحوار المتعلق بقطاع الاتصالات السلكية واللاسلكية ومبادرة الشبكة العالمية، المعنون "تنفيذ المبادئ التوجيهية المتعلقة بأُسس حرية التعبير والخصوصية".

ضمان أن تكون الطلبات لفرض قيود على المحتوى والحصول على بيانات العملاء ممتثلة تماماً للقانون

٦٥- ينبغي أن تكفل الشركات أن تكون جميع الطلبات المتعلقة بفرض قيود على المحتوى والحصول على بيانات المستهلكين ممتثلة للمتطلبات الإجرائية والقانونية المنصوص عليها في القانون المحلي، وممتثلة أيضاً لمعايير الإجراءات الواجبة المقررة دولياً[١٠٧]. وفيما يخص التدخل المتعلق بحقوق الإنسان، يجب أن تأذن بتنفيذ هذه الطلبات محاكم أو هيئات قضائية مستقلة ونزيهة. وعلاوة على ذلك، ينبغي أن تطلب الشركات أن تُقدم هذه الطلبات خطياً وأن يُقدم تفسير واضح للأساس القانوني، واسم ووظيفة وتوقيع المسؤول المختص. وينبغي أيضاً للشركات أن تسعى إلى التحقق من أن المسؤول المعني أو الكيان الحكومي المعني مخول سلطة إصدار هذا الطلب[١٠٨]. ويجب أن تُطلب هذه الإجراءات الرسمية حتى ولو لم يشترطها القانون. وبالإضافة إلى ذلك، يجب أن تحتفظ الشركات، عند تنفيذ الطلب، بسجل لجميع المراسلات الخطية بينها وبين مقدم كل طلب وقوائم طلبات الحصول على بيانات المستخدمين، ما لم يمثل ذلك السجل مخاطر لا مبرر لها على الخصوصية[١٠٩].

تفسير نطاق الطلبات الحكومية والقوانين

٦٦- من شأن الطلبات الحكومية والأُطر القانونية الغامضة والمفتوحة أن تجعل من الصعب على الشركات أن تقرر ما إذا كانت هذه الطلبات والأُطر ممتثلة للقانون المحلي أم لا. غير أن الشركات يمكنها أن تخفف من هذا الغموض باعتماد سياسات على نطاق الشركة توجِّه جميع وحدات العمل التجاري، بما في ذلك الفروع المحلية، لحل أي غموض قانوني لصالح احترام حرية التعبير والخصوصية وحقوق الإنسان الأخرى. ولا تستند هذه السياسات حصراً إلى مسؤوليات مقدم الخدمة فيما يتعلق بحقوق الإنسان، وإنما أيضاً إلى التزام الدولة بالامتثال لقوانين حقوق الإنسان الواجبة التطبيق ولإجراءات الحماية ذات الصلة المنصوص عليها في القوانين المحلية (كالقانون الدستوري، وقانون الإجراءات الجنائية، وقانون حماية البيانات).

٦٧- ومن المنظور العملي، ينبغي للشركات أن تفسِّر الطلبات، قدر الإمكان، على نحوٍ يكفل أقل قدر من تقييد المحتوى وأقل قدر من الوصول إلى بيانات العميل. فمثلاً، عندما تبدو الطلبات فضفاضة، توصي مبادرة الشبكة العالمية بأن تلتمس الشركات توضيحاً بشأن نطاق الطلبات وأن تتلقى التعديلات المناسبة لهذه الطلبات[١١٠].

الاعتراض على الطلبات وعلى القوانين الأساسية

٦٨- ترغب الشركات في العمل في بيئة قانونية تمتثل لحقوق الإنسان ولمعايير الإجراءات القانونية الواجبة وسيادة القانون. وينبغي للشركات أن تستطلع جميع الخيارات القانونية للاعتراض على الطلبات التي تنطوي على تدخل مفرط -كطلبات إغلاق خدمات أو منصات بكاملها،

(١٠٧) انظر، مثلاً، the Manila Principles on Intermediary Liability and the International Principles on the Application of Human Rights to Communications Surveillance, co-authored by a number of non-governmental organizations.

(١٠٨) Global Network Initiative, "Implementation guidelines", pp. 5-6; also Telecommunications Industry Dialogue submission, pp. 8-10.

(١٠٩) Telecommunications Industry Dialogue submission, pp. 8-9.

(١١٠) المرجع نفسه.

أو عمليات إزالة موقع مُستهدف بوضوح بسبب الانتقاد أو الاختلاف، أو طلبات الحصول على بيانات عملاء تشمل مجموعة واسعة وغير محددة من المستخدمين(١١١).

٦٩- وكما هي الحال عند اتخاذ أي قرار بشأن إجراءات قانونية، تراعي الشركات مجموعة من الاعتبارات، مثل "التأثير المفيد المحتمل [على حقوق الإنسان]، واحتمال النجاح، وجسامة الحالة، والتكلفة، ومدى تمثيل الحالة، وما إذا كانت الحالة جزءاً من اتجاه أكبر(١١٢). غير أن الشركات ينبغي أن تولي اهتماماً كبيراً لاعتبارات حقوق الإنسان في عمليات اتخاذ القرار وأن تجري تقييماً دقيقاً للمنافع والمخاطر المحتملة للقرار على حقوق الإنسان. فمثلاً، يجب أن تميل الشركات إلى الاعتراض على الطلبات الفضفاضة إذا وُجد احتمال معقول للنجاح، حتى وإن استلزمت هذه الاعتراضات موارد كثيرة؛ ومن الناحية الأخرى، قد تتوخى الشركات خيارات بديلة إن كان الاعتراض سيمثل على الأرجح سابقة سلبية أو ردة فعل سلبية، وسيمسّ حرية التعبير والخصوصية.

٥- الشفافية

٧٠- الشفافية سمة رئيسية من سمات المسؤولية الجديرة بالاحترام من جانب صناعة الوصول الرقمي. وينبغي الكشف عن المعلومات المتعلقة بأنشطة الحكومات التي تتطلب مساعدة أو مشاركة من الشركات، وذلك إلى أبعد حد يسمح به القانون. وينبغي أن تدرك الشركات أن هذه المعلومات تُستخدم في المقام الأول من جانب المجتمع المدني بهدف الاعتراض أمام المحاكم على تجاوزات حقوق الإنسان، أو تسجيل المظالم أمام الآليات المحلية والدولية نيابةً عن المستخدمين، أو التماس سُبُل مساءلة بديلة. وبناءً على ذلك، يجب أن تكون عمليات الكشف عن المعلومات منتظمة ومستمرة، وبصيغة يسهل الوصول إليها وتوفر السياق المناسب.

٧١- وحتى إن كانت القوانين المحلية تحد من الشفافية الكاملة، ينبغي للشركات أن تكشف عن جميع المعلومات ذات الصلة والمعلومات التي يمكن المعاقبة عليها. فمثلاً، إن كان يُحظر على الشركات الكشف عن أصل أو أساس طلب يتعلق بالإغلاق، ينبغي للشركات أن تقدم تحديثات منتظمة عن الخدمات المتأثرة أو المستعادة، والخطوات التي تتخذها لمعالجة المسألة، وتفسيرات لهذا الوضع. وتؤدي أيضاً تدابير الشفافية المبتكرة، مثل نشر بيانات مجمَّعة وحجب معلومات مختارة(١١٣)، إلى تخفيف الآثار المترتبة على أوامر التقييد والقوانين الأخرى المتعلقة بعدم الكشف عن المعلومات. وينبغي أن تكشف الشركات عن جميع القوانين المحلية التي تمتثل لها، وأن تعترض، عند الإمكان، على أي قوانين أو لوائح تمنع أو تعوق الشركات من التحلي بالشفافية مع المستخدمين وعامة الجمهور(١١٤).

٧٢- وينبغي للشركات أن تكشف عن سياساتها وإجراءاتها ذات الصلة بحرية التعبير. وتشمل المعلومات ذات الصلة التي يُكشف عنها سياسات الاحتفاظ بالبيانات واستخدامها، وممارسات إدارة الشبكات، وبيع وشراء تكنولوجيات ترشيح واعتراض الشبكات(١١٥). وينبغي للشركات أيضاً

(١١١) Yael Ronen, "Big Brother's little helpers" (February 2015), p. 81.

(١١٢) Global Network Initiative, "Implementation guidelines".

(١١٣) مثلاً، عندما "طُلب إلى شركة Telia تعليق بعض الخدمات، لم تذكر الشركة أن ذلك هو نتيجة لمشاكل تقنية" Telecommunications Industry Dialogue submission, p. 14.

(١١٤) Telecommunications Industry Dialogue, "Information on country legal frameworks pertaining to freedom of expression and privacy in telecommunications" (2016).

(١١٥) Ranking Digital Rights submission.

أن تكشف عن المعلومات بشأن تواتر ونطاق وموضوع عمليات العناية الواجبة، وأن تقدم ملخصاً للنتائج الرفيعة المستوى. وعموماً، ينبغي للشركات الرجوع إلى العدد المتزايد من المصادر التي تتناول المؤشرات القيّمة في مجال الشفافية وأفضل الممارسات الأخرى المتعلقة بها. وينبغي أيضاً التشاور مع المستخدمين، والمجتمع المدني، والشركات النظيرة بشأن تصميم وتنفيذ تدابير الشفافية.

٦- سُبُل العلاج الفعالة

٧٣- رغم التقدم الذي شهدته السنوات الأخيرة في جوانب معينة لمسؤولية الشركات، تبدو الخطوات العلاجية غائبة في كثير من الأحيان من جدول أعمال القطاع الخاص. ورغم ذلك فإن سبل العلاج ركن أساسي في مسؤولية الشركات ويجب تقديمها كلما "تسبّبت الشركات أو أسهمت في إلحاق آثار سلبية" (انظر A/HRC/17/31، المرفق، المبدأ ٢٢). وتتحمّل الدول الواجب الأساسي في علاج تجاوزات حقوق الإنسان ذات الصلة بالعمل التجاري، ولا سيما التجاوزات التي توعز بها الدول، مثل التقييد الفضفاض للمحتوى، والطلبات غير القانونية للحصول على بيانات المستخدمين، والمراقبة غير المتناسبة. غير أن الشركات التي تفشل في تنفيذ تدابير العناية الواجبة المناسبة، وغير ذلك من الضمانات، قد تتسبّب أو تسهم أيضاً في هذه التجاوزات. وفي تلك الأوضاع، ينبغي للشركات أن "تكفل سبل العلاج أو أن تتعاون على توفيرها عن طريق العمليات المشروعة" (المرجع نفسه).

٧٤- وقد تشمل سبل العلاج وسائل مالية وغير مالية على السواء (المرجع نفسه، المبدأ ٢٧). وعندما يُنتقص من حرية التعبير، قد تشمل سبل العلاج الوصول إلى آليات المظالم، والحصول على معلومات عن الانتهاك، وضمانات عدم التكرار[١١٦]. وقد يحتاج المستخدمون الذين عُلقت حساباتهم إلى الترضية بسماع رأيهم وتقديم تفسيرات وتأكيدات لهم بعدم التكرار[١١٧].

٧٥- ومن الممكن أيضاً إصلاح أو تعزيز السياسات والآليات القائمة من أجل التصدي لانتهاكات حرية التعبير. فمثلاً، قد يجري مقدم الخدمة تحسينات لسياساته المتعلقة بتقييد المحتوى وللتدريب المقدم لأفرقة مراقبة المحتوى لتقليل احتمال الإزالة غير العادلة للمواقع أو فرض قيود فضفاضة على المحتوى، كالترشيح. ويمكن أيضاً تحديث آليات شكاوى العملاء لكي تسمح للمستخدمين بحصر ممارسات إدارة حركة الإنترنت، وتصنيفات الترشيح التجاري، وغير ذلك من القيود على المحتوى التي تعتبر مفرطة التقييد أو غير عادلة.

خامساً- الاستنتاجات والتوصيات

٧٦- يعتمد الأفراد على الوصول الرقمي لممارسة الحقوق الأساسية، مثل حرية الرأي والتعبير، والحق في الحياة وفي مجموعة من الحقوق الاقتصادية والاجتماعية والثقافية. وعادةً ما يواجه الأفراد أيضاً عقبات أمام الوصول: تتفاوت من الإغلاق إلى المراقبة. ويتناول هذا التقرير أساساً العقبات التي تمنع أو تعوق أو تستبعد التعبير عن طريق الاعتماد الصريح على الرقابة الرقمية. ولم يتناول هذا التقرير عقبات أخرى جسيمة – مثل عدم وجود هياكل أساسية كافية للاتصال، والتكاليف العالية للوصول التي تفرضها الحكومات،

(١١٦) Telecommunications Industry Dialogue submission, p. 17.

(١١٧) Peter Micek and Jeff Landale, “Forgotten pillar: the Telco remedy plan”, Access Now (May 2013), p. 6.

وعدم المساواة بين الجنسين، والعوائق اللغوية – التي قد تشكل أيضاً أشكالاً للرقابة[١١٨]. ولذلك يركز جزء كبير من التقرير على أدوار الدول وواجباتها. غير أن الدول تمارس على نحو متزايد الرقابة عن طريق القطاع الخاص. ولم يهدف التقرير إلى تناول القيود التي يفرضها قانون حقوق الإنسان على إجراءات الدول، فحسب، وإنما أيضاً المبادئ التي يجب على الجهات الفاعلة الخاصة أن تراعيها في سياق احترام حقوق الإنسان. وفيما يلي التوصيات الأساسية، التي سُلط الضوء عليها في التحليل الوارد أعلاه.

الدول ومجلس حقوق الإنسان

٧٧- أدان مجلس حقوق الإنسان بصورة قاطعة، في قراره ١٣/٣٢، التدابير الرامية إلى منع أو تعطيل الوصول إلى المعلومات أو نشرها على الإنترنت، في انتهاك للقانون الدولي لحقوق الإنسان، ودعا جميع الدول إلى الامتناع عن هذه التدابير ووقفها. ويجب أن تُكمَّل وتُفصّل هذه الإدانة، التي هي أساسية لكي يعزز المجلس حقوق الإنسان على شبكة الإنترنت. ويعتبر من قبيل تعمّد منع أو تعطيل الوصول اتخاذ أي إجراء لغلق شبكات الاتصالات السلكية واللاسلكية، وخدمات الهواتف المحمولة، ومواقع التواصل الاجتماعي، وما إلى ذلك. وينبغي للمجلس القيام بعمل في المستقبل لتوضيح القواعد التي تنطبق على الوصول الرقمي، على النحو المبين في هذا التقرير، بهدف تعزيز الحق في حرية الرأي والتعبير على الإنترنت.

٧٨- ومن المهم جداً للمجلس وللدول توضيح الصلة بين التدخّل في الخصوصية وحرية التعبير. ولتأكيد ذلك، يجب تقييم عملية التدخّل في الخصوصية بناءً على أسسها الموضوعية بموجب المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية والمعايير الأخرى لقانون حقوق الإنسان. غير أن بعض التدخلات – مثل الطلبات الفضفاضة للحصول على بيانات المستخدمين واحتفاظ طرف ثالث بهذه البيانات – قد يؤدي إلى آثار رادعة قصيرة الأمد وطويلة الأمد على حرية التعبير، ويجب تجنبها بحكم القانون والسياسات. وينبغي للدول، على أقل تقدير، أن تضمن أن تكون المراقبة مأذوناً بها من جانب سلطة قضائية مستقلة ونزيهة ومختصة تقر بأن الطلب ضروري ومتناسب لحماية هدف مشروع.

٧٩- ويشعر المقرر الخاص بقلق خاص بشأن التقارير التي تتحدث عن تعرض الشركات وموظفيها ومعداتها وهياكلها الأساسية للتهديد والتخويف. كما أن تركيز المجلس على الدور المهم للقطاع الخاص – وضرورة حمايته – مسألة جديرة بالاهتمام. وينبغي للدول أن تراجع جميع الأنشطة ذات الصلة بالوصول إلى الشبكات، لضمان قانونيتها وضرورتها وتناسبها، مع إيلاء اهتمام خاص لمسألة ما إذا كانت هذه الأنشطة هي الوسائل الأقل تدخلاً لحماية هدف مشروع أم لا.

(١١٨) Global Commission on Internet Governance submission; Arco Iris Libre de Cuba, Centro de Información Hablemos Press, Centro de Información Legal CubaLex, Mesa de Diálogo de la Juventud Cubana Plataforma Femenina Nuevo País, "Situación del derecho a la libertad de opinion y expression en Cuba" (Situation of the right to freedom of opinion and expression in Cuba) (July 2016), p. 20.

٨٠- ولا يمكن أن يتجاوز الدور الوقائي الذي قد تمارسه الدول على القطاع الخاص حداً معيناً. ولا ينبغي للدول أن تعزز المكسب الاقتصادي للكيانات الخاصة على حساب حقوق المستخدمين في حرية الرأي والتعبير. ومن ثمّ، يجب أن تحظر الدول محاولات إيلاء أولوية لأنواع معينة من محتوى أو تطبيقات الإنترنت على حساب غيرها نظير مقابل مادي أو منافع تجارية أخرى.

٨١- ولا يزال التقاطع بين سلوك الدول وأدوار الشركات في العصر الرقمي أمراً جديداً بالنسبة إلى العديد من الدول. وينطوي أحد السبل المفيدة للمضي قدماً، على الصعيدين الدولي والمحلي، على وضع خطط عمل وطنية بشأن العمل التجاري وحقوق الإنسان، من أجل إرساء طرق مجدية تتيح لجميع فئات صناعة الوصول الرقمي تحديد وعلاج آثار أنشطتها على حقوق الإنسان.

الأطراف الفاعلة الخاصة

٨٢- يدرك الأفراد والشركات في قطاع الوصول الرقمي، منذ سنوات، أنهم يؤدون دوراً أساسياً في التوسع الكبير في نطاق الوصول إلى خدمات المعلومات والاتصالات. فهم يعملون في مجال ينبغي أن يشمل نموذج النجاح فيه توسيع نطاق الوصول، وتعزيز الكفاءات، والتنوع، والشفافية. وينبغي للأفراد والشركات الاستفادة من المبادئ المحددة في هذا التقرير بوصفها أدوات لتعزيز أدوارهم في النهوض بحقوق المستخدمين في حرية التعبير. ومن هذا المنطلق، وبالإضافة إلى الالتزامات بحقوق الإنسان على مستوى السياسات الرفيعة المستوى، ينبغي أن تخصص هذه الصناعة موارد مناسبة للوفاء بهذه الالتزامات، بما في ذلك بذل العناية الواجبة، وخيارات التصميم والهندسة الموجهة نحو الحقوق، ومشاركة الجهات صاحبة المصلحة، واستراتيجيات منع أو تخفيف المخاطر على حقوق الإنسان، والشفافية، وسبل العلاج الفعالة. وفي هذا السياق، ينبغي أن يعتمد تصميم وتنفيذ مسؤولية الشركات تجاه حقوق الإنسان على الخبرات الداخلية والخارجية على السواء، مع ضمان الحصول على مدخلات مفيدة من العملاء وأصحاب الحقوق الآخرين المتأثرين، والمجتمع المدني، ومجتمع حقوق الإنسان.

٨٣- ولا يعني ذلك أن الشركات الخاصة لا تتعرض لضغوط. فهي تتعرض لذلك بالفعل. ولكن عندما تطلب الدول مشاركة الشركات في الرقابة أو المراقبة، ينبغي للشركات أن تسعى إلى منع أو تخفيف الآثار السلبية لمشاركتها على حقوق الإنسان إلى أقصى حد يسمح به القانون. وعلى أية حال، ينبغي أن تتخذ الشركات جميع التدابير الضرورية والقانونية لضمان ألا تتسبّب أو تسهم أو تتواطأ في حدوث تجاوزات لحقوق الإنسان. وينبغي تنظيم الترتيبات مع الشركات الشريكة لضمان التزام جميع الأطراف بمسؤولياتها تجاه حقوق الإنسان. وينبغي للشركات أن تسعى أيضاً إلى تحسين العلاقات التجارية القائمة، لمنع أو تخفيف الآثار السلبية على حقوق الإنسان.