الأمم المتحدة

A/HRC/39/29

الجمعية العامة

Distr.: General
3 August 2018
Arabic
Original: English

مجلس حقوق الإنسان

الدورة التاسعة والثلاثون

البندان ٢ و٣ من جدول الأعمال

التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان وتقريرا المفوضية السامية لحقوق الإنسان 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 مفوض الأمم المتحدة السامي لحقوق الإنسان

موجز

يقدَّم هذا التقرير عملاً بالقرار ٣٤/٧ الذي طلب فيه مجلس حقوق الإنسان إلى المفوض السامي لحقوق الإنسان أن يعدّ تقريراً بهدف تحديد وتوضيح المبادئ والمعايير وأفضل الممارسات فيما يتعلق بتعزيز وحماية الحق في الخصوصية في العصر الرقمي، بما في ذلك مسؤولية مؤسسات الأعمال في هذا الصدد، وأن يقدمه إلى مجلس حقوق الإنسان في دورته التاسعة والثلاثين.

GE.18-12799(A)

1812799

أولاً- مقدمة

١- باتت الحاجة إلى مواجهة التحديات التي يفرضها عالم التكنولوجيا الرقمية على الحق في الخصوصية أكثر إلحاحاً من أي وقت مضى. فالتكنولوجيا الرقمية، التي تستغل باستمرار البيانات المرتبطة بحياة الأشخاص، تتغلغل تدريجياً في النسيج الاجتماعي والثقافي والاقتصادي والسياسي للمجتمعات الحديثة، مدفوعةً في الغالب من القطاع الخاص. وثمة تهديد ناجم عن التكنولوجيات التي تستخدم البيانات استخداماً كثيفاً، وهي تحتل موقعاً متنامياً باستمرار من قبيل البيانات الضخمة والذكاء الاصطناعي، ألا وهو إقامة بيئة رقمية تدخّلية تتيح للدول ومؤسسات الأعمال ممارسة المراقبة، وتحليل سلوك الناس والتنبؤ به، بل والتلاعب به أيضاً إلى حد غير مسبوق. وإذا كان لا يسعنا إنكار إمكانية توظيف التكنولوجيات القائمة على البيانات في استخدامات مفيدة للغاية، فإن هذه التطورات التكنولوجية تنطوي على مخاطر كبيرة بالنسبة إلى الكرامة الإنسانية، والاستقلالية والخصوصية، وممارسة حقوق الإنسان بوجه عام، في حال عدم إدارتها بعناية شديدة.

٢- وباتت الجهات الفاعلة على الصعيدين الدولي والإقليمي تدرك أكثر فأكثر التحديات الماثلة، وقد بدأت تتحرك بناءً على ذلك. وأنشأ مجلس حقوق الإنسان ولاية المقرر الخاص المعني بالحق في الخصوصية في تموز/يوليه ٢٠١٥. وفي العديد من القرارات، أعرب مجلس حقوق الإنسان والجمعية العامة عن شواغلهما بشأن المخاطر التي تهدد الخصوصية نتيجةً للتدابير التي تتخذها الدول من أجل فرض المراقبة أو نتيجةً للممارسات الصادرة عن قطاع الأعمال[(١)]. وعلى الصعيد الإقليمي، أدى عدد من التدابير المعتمدة إلى تعزيز حماية خصوصية البيانات، ومنها نظام الاتحاد الأوروبي العام لحماية البيانات الذي بدأ نفاذه مؤخراً بآثارٍ مترتبة على الصعيد العالمي؛ وبروتوكول مجلس أوروبا لاستكمال وتحديث اتفاقية حماية الأفراد فيما يخص المعالجة الآلية للبيانات الشخصية؛ والمبادئ التوجيهية لمفوضية الاتحاد الأفريقي المتعلقة بحماية البيانات الشخصية في أفريقيا. وفي الوقت نفسه، اعتمدت حكومات عديدة قوانين أو تشريعات لمضاعفة صلاحياتها في مجال المراقبة، وتم ذلك في الكثير من الأحيان بسبل لا ترقى إلى المعايير الدولية السارية في مجال حقوق الإنسان[(٢)].

٣- ويقدِّم هذا التقرير توجيهات بشأن كيفية التصدي لبعض التحديات الملحة الماثلة أمام الحق في الخصوصية في العصر الرقمي. كما يقدّم لمحة عامة عن الإطار القانوني الدولي، ويتضمن مناقشة بشأن أهم الاتجاهات الراهنة. ثم يتناول التزامات الدول ومسؤولية مؤسسات الأعمال، بما في ذلك مناقشة بشأن الضمانات الكافية وأنشطة الرقابة. ويعرض الفصل الأخير من التقرير بعض الآراء بشأن سبل الانتصاف من الانتهاكات والتجاوزات المتعلقة بالخصوصية.

(١) انظر، على سبيل المثال، قرارات الجمعية العامة ١٦٧/٦٨ و١٦٦/٦٩ و١٩٩/٧١ وقراري مجلس حقوق الإنسان ١٦/٢٨ و٧/٣٤ والمقرر ١١٧/٢٥.

(٢) انظر، على سبيل المثال، Anja Seibert-Fohr, "Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy" (April 2018), متاح على: https://ssrn.com/abstract=3168711؛ انظر https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee و www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SR_right_privacy.pdf.

٤- ويستند التقرير إلى تقرير عام ٢٠١٤ المقدم من المفوض السامي عن الحق في الخصوصية في العصر الرقمي (A/HRC/27/37) وإلى عروض ومناقشات حلقة عمل الخبراء المعقودة في جنيف في شباط/فبراير ٢٠١٨[٣]. ويعتمد أيضاً على ٦٣ من التقارير الخطية الواردة من مجموعة واسعة من أصحاب المصلحة[٤].

ثانياً- ماذا يعني الحق في الخصوصية في العصر الرقمي

٥- يُعَدُّ الحق في الخصوصية أحد حقوق الإنسان الأساسية، على النحو المعترف به في المادة ١٢ من الإعلان العالمي لحقوق الإنسان وفي المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، وكذلك في العديد من الصكوك الدولية والإقليمية الأخرى لحقوق الإنسان[٥][٦]. ويمكن تعريف الخصوصية بأنها التسليم بحق الأفراد في التمتع بفسحة للتنمية الذاتية، تقوم على مبدأي التفاعل والحرية، أو حقهم في "مجال خاص" يسع لهم فيه التفاعل أو عدم التفاعل مع الآخرين، دون الخضوع إلى تدخل الدولة ولا إلى تدخل تطفّلي زائد يمارسه أفراد آخرون بلا دعوة (انظر، على سبيل المثال، A/HRC/13/37، الفقرة ١١، وA/HRC/23/40، الفقرتين ٢٢ و٤٢). وفي البيئة الرقمية، تكتسي خصوصية المعلومات أهمية بوجه خاص، وهذا يشمل، في آن معاً، المعلومات المتوافرة والمعلومات التي يمكن الحصول عليها عن شخص ما وعن حياته، والقرارات المتخذة استناداً إلى تلك المعلومات.

٦- وتشمل حماية الحق في الخصوصية نطاقاً واسعاً لا يقتصر على المعلومات الموضوعية المتوافرة في مجال الاتصالات، إنما أيضاً البيانات الوصفية التي، عند تحليلها وتجميعها، "قد توفر نظرة عن سلوك الفرد وعلاقاته الاجتماعية والأشياء المفضَّلة لديه وهويته. وهي بيانات تتجاوز حتى تلك التي تتيحها إمكانية الحصول على محتوى اتصال خاص" (انظر A/HRC/27/37، الفقرة ١٩). ولا تقتصر حماية الحق في الخصوصية على الأماكن الخاصة أو المنعزلة، من قبيل منزل شخص ما على سبيل المثال، بل تمتد إلى الأماكن العامة والمعلومات المتاحة للجمهور (انظر CCPR/C/COL/CO/7، الفقرة ٣٢). فعلى سبيل المثال، يتأثر الحق في الخصوصية عندما تقوم حكومة ما بمراقبة مكان عام، كسوق أو محطة قطارات، فتراقب الأفراد المتواجدين في ذلك المكان. وعندما يتم جمع وتحليل المعلومات المتاحة للجمهور بشأن فرد ما في وسائل التواصل الاجتماعي، فذلك يطال أيضاً الحق في الخصوصية،[٧] لأن نشر المعلومات للعموم لا يعني أن مضمونها غير مشمول بالحماية[٨].

---

(٣) انظر www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgePrivacyWorkhop.aspx؛ البث الشبكي متاح على: http://webtv.un.org/search/part-1.1-un-expert-workshop-on-the-right-to-privacy-in-the-digital-age/5734527899001/?term=2018-02-19&sort=date&page=2.

(٤) جميع التقارير متاحة على: www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

(٥) انظر، على سبيل المثال، المادة ١٦ من اتفاقية حقوق الطفل؛ والمادة ١٤ من الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم؛ والمادة ٢٢ من اتفاقية حقوق الأشخاص ذوي الإعاقة.

(٦) انظر، مثلاً، المادة ١٠ من الميثاق الأفريقي لحقوق الطفل ورفاهه؛ والمادة ١١ من الاتفاقية الأمريكية لحقوق الإنسان؛ والمادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان.

(٧) انظر المعلومات المقدمة من المنظمة الدولية لحماية الخصوصية لإدراجها في هذا التقرير.

(٨) Anja Seibert-Fohr, "Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy".

٧- ولا يتأثر الحق في الخصوصية فقط عن طريق فحص أو استخدام المعلومات المتعلقة بشخص ما من جانب شخص آخر أو بواسطة الخوارزميات[٩]. ذلك أن مجرد إنتاج وجمع البيانات المتعلقة بهوية شخص، وأسرته أو حياته، يؤثران بالفعل على الحق في الخصوصية لأن الفرد يفقد نتيجةً لذلك السيطرة إلى حد ما على تلك المعلومات، مما قد يعرض خصوصيته للخطر (انظر A/HRC/27/37، الفقرة ٢٠)[١٠]. وبالإضافة إلى ذلك، فإن مجرد تنفيذ مراقبة سرية يُعد تدخلاً في الحق في الخصوصية (المرجع نفسه)[١١].

٨- وينطبق الحق في الخصوصية بالتساوي على كل فرد. ويُعتبر وجود أي فرق في توفير الحماية لذلك الحق على أساس الجنسية، أو لأي أسباب أخرى، أمراً متعارضاً مع الحق في المساواة وفي عدم التمييز المنصوص عليه في المادة ٢٦ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

٩- وهذا يعني أنه يجب على الدولة الطرف أن تحترم وتكفل الحقوق المنصوص عليها في العهد لأي شخص يخضع لسلطتها أو لسيطرتها الفعلية حتى ولو لم يكن موجوداً داخل إقليمها[١٢]. وينطبق قانون حقوق الإنسان أيضاً عندما تمارس الدولة سلطتها أو سيطرتها الفعلية فيما يتعلق بالهياكل الأساسية للاتصالات الرقمية، أينما وجدت، مثلاً عند التنصت المباشر على الهياكل الأساسية للاتصالات الموجودة خارج إقليم تلك الدولة أو عن طريق اختراقها. وبالمثل، عندما تمارس الدولة ولاية تنظيمية على طرف ثالث يتحكم بالمعلومات المتعلقة بشخص ما (مقدم الخدمات السحابية مثلاً)، يتعين على تلك الدولة أيضاً توسيع نطاق حماية حقوق الإنسان لكي يشمل الأشخاص الذين ستتأثر خصوصيتهم إن تم اقتناء تلك المعلومات أو استخدامها (انظر A/HRC/27/37، الفقرة ٣٤).

١٠- ووفقاً للمادة ١٧ من العهد، لا يجوز أي تدخل إلا إذا لم يكن تعسفياً وغير قانوني. ودأبت آليات حقوق الإنسان على تفسير هذه العبارات باعتبارها تشير إلى مبادئ أساسية هي المشروعية والضرورة والتناسب (انظر A/HRC/27/37 ، الفقرات من ٢١ إلى ٢٧)[١٣]. وتمشياً مع تلك المبادئ، لا يجوز للدول أن تتدخل في الحق في الخصوصية إلا في الحدود المنصوص عليها في القانون، ويجب أن تحدد التشريعات ذات الصلة الظروفَ المفصلة التي يجوز فيها هذا التدخل[١٤]. ويُعتبر التدخل تعسفياً وغير قانوني ليس فقط عندما لا يكون منصوصاً عليه في القانون، إنما أيضاً عندما يكون القانون نفسه أو التدخل المعني متعارضاً مع أحكام العهد

---

(٩) انظر: Paul Bernal, "Data gathering, surveillance and human rights: recasting the debate", *Journal of Cyber Policy*, vol. 1, No. 2 (2016).

(١٠) انظر أيضاً: European Court of Human Rights, *Rotaru v. Romania*, application No. 28341/95, judgment of 4 May 2000 و*Kopp v. Switzerland*, application No. 23224/94, judgment of 25 March 1998.

(١١) انظر أيضاً: European Court of Human Rights, *Roman Zakharov v. Russia*, application No. 47143/06, judgment of 4 December 2015.

(١٢) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٣١ (٢٠٠٤) بشأن طبيعة الالتزام القانوني العام المفروض على الدول الأطراف في العهد، الفقرة ١٠.

(١٣) انظر أيضاً قرار مجلس حقوق الإنسان ٧/٣٤، الفقرة ٢.

(١٤) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ١٦(١٩٨٨) بشأن الحق في حرمة الحياة الخاصة، الفقرتين ٣ و٨.

ومقاصده وأهدافه[١٥]. ولا تكون القيود مشروعة وغير تعسفية إلا إذا كانت تخدم غرضاً مشروعاً (انظر A/HRC/29/32، الفقرة ٣٣). ويتعين أن تكون القيود ضرورية لبلوغ ذلك الهدف المشروع، ومتناسبة معه، ويجب أن تكون أقل الخيارات المتاحة تدخلاً. وعلاوة على ذلك، فإن أي تقييد للحق في الخصوصية يجب ألا يجرِّد جوهر ذلك الحق من معناه (انظر A/69/397، الفقرة ٥١).

١١- ويكتسي الحق في الخصوصية أهمية أساسية من أجل التمتع بحقوق الإنسان وممارستها على شبكة الإنترنت وخارجها. كما يشكل أحد الأسس التي يقوم عليها المجتمع الديمقراطي، ويؤدي دوراً رئيسياً في إعمال مجموعة واسعة من حقوق الإنسان التي تتراوح بين حرية التعبير (انظر A/HRC/23/40 وA/HRC/29/32، الفقرة ١٥) وحرية التجمع وتكوين الجمعيات (انظر A/HRC/31/66، الفقرات من ٧٣ إلى ٧٨ وA/72/135، الفقرات من ٤٧ إلى ٥٠) وحظر التمييز وغير ذلك[١٦]. ويمكن أن ينجم عن التدخل في الحق في الخصوصية أثر غير تناسبي على بعض الأفراد و/أو الجماعات، مما يؤدي إلى تفاقم ممارسات عدم المساواة والتمييز[١٧]. وقد تنجم أيضاً عن القواعد التنظيمية الفضفاضة بشأن الخصوصية قيود لا مبرر لها على سائر الحقوق، ولا سيما حرية التعبير، مثلاً عند حدوث تدخلٍ نتيجةً لقاعدة تنظيمية غير متناسبة مع التقارير الإخبارية المشروعة والتعبير الفني أو البحث العلمي. ونظراً لضيق الحيز المتاح ههنا، لن يبحث هذا التقرير الترابط القائم بين الحق في الخصوصية وجميع حقوق الإنسان الأخرى، والأثر التمييزي الناجم على أفراد وفئات محددة، والنُهج الهادفة إلى حماية تلك الحقوق.

ثالثاً- التدخلات في الخصوصية: الاتجاهات والشواغل

ألف- زيادة الاعتماد على البيانات الشخصية من جانب الحكومات ومؤسسات الأعمال

البصمات الرقمية المتزايدة

١٢- تعمل الدول ومؤسسات الأعمال على حد سواء على جمع واستخدام كميات لا تني تزداد من البيانات المتعلقة بالحياة الخاصة للأفراد. ويتم جمع تدفقات هائلة من البيانات المتعلقة ببلايين الأفراد عن طريق الحواسيب الشخصية، والهواتف الذكية، والساعات الذكية، وأدوات تتبع اللياقة البدنية، وغيرها من الملابس التكنولوجية. وثمة عدد متزايد بسرعة من الأدوات وأجهزة الاستشعار الأخرى المترابطة والقائمة فيما يسمى المنازل الذكية والمدن الذكية التي تأتي بدفق إضافي من البيانات. كما أن نطاق وعمق المعلومات التي تُجمع وتُستخدم هما من الضخامة بحيث أنهما يشملان أجهزة التعرف على هوية المستخدم، وعناوين البريد الإلكتروني، وأرقام الهاتف، والبيانات البيومترية والمالية والمتعلقة بالصحة، والأنماط السلوكية. وهذا يحدث في الغالب من دون علم الأشخاص المعنيين ومن دون موافقتهم الفعلية.

(١٥) المرجع نفسه، الفقرة ٤.

(١٦) انظر: Paul Bernal, "Data gathering, surveillance and human rights: recasting the debate".

(١٧) انظر قرار الجمعية العامة ١٩٩/٧١، الفقرة ٥ (ز)؛ وقرار مجلس حقوق الإنسان ٧/٣٤، الفقرة ٥ (ز)؛ والشبكة الدولية لمنظمات الحريات المدنية، المعلومات المقدمة لإدراجها في هذا التقرير.

تبادل البيانات ودمجها

١٣- تتبادل مؤسسات الأعمال والدول البيانات الشخصية الواردة من مختلف المصادر وقواعد البيانات وتعمل على دمجها باستمرار، ويتولى سماسرة البيانات دوراً رئيسياً لتحقيق هذه الغاية. وفي النتيجة، يجد الأفراد أنفسهم في موقع ضعف، إذ يبدو من شبه المستحيل تعقب من يملك أي نوع من المعلومات المتعلقة بهم، ناهيك عن التحكم بالسبل العديدة التي يمكن أن تُستخدم فيها تلك المعلومات.

البيانات البيومترية

١٤- تعمل الدول ومؤسسات الأعمال بصورة متزايدة على نشر نُظم الاعتماد على جمع واستخدام البيانات البيومترية، كالحمض النووي الريبي المنزوع الأكسيجين (الدنا)، وهندسة الوجه البشري، والصوت، وشبكية العين، وقزحية العين، وبصمات الأصابع. وقد أنشأ بعض البلدان قواعد بيانات مركزية ضخمة من أجل تخزين هذه المعلومات لمجموعة متنوعة من الأغراض، بدءاً من ضمان الأمن القومي وإجراء التحقيقات الجنائية، وصولاً إلى التعرف على هوية الأشخاص من أجل توفير خدمات أساسية كالخدمات الاجتماعية والمالية والتعليم. وتقوم الجهات الحكومية في جميع أنحاء العالم بنشر كاميرات نظام المراقبة بالفيديو في المدن ومحطات القطار والمطارات، وتتيح التعرف على قسمات الوجه لتحديد هوية الأشخاص تلقائياً وإصدار إنذار بشأنهم، عند الاقتضاء. وتُستخدم التكنولوجيات البيومترية بشكل متزايد لضبط حركات الهجرة، سواء على الحدود أو داخل البلدان. ويثير إنشاء قواعد البيانات الضخمة المتعلقة بالبيانات البيومترية شواغل كبيرة في مجال حقوق الإنسان. وتُعتبر هذه البيانات حساسة بوجه خاص، إذ ترتبط بطبيعتها ارتباطاً وثيقاً بشخص معين وبحياة ذلك الشخص، ويمكن إساءة استخدامها على نحو خطير. فعلى سبيل المثال، من الصعب للغاية الانتصاف من سرقة الهوية على أساس الاستدلال البيولوجي، وقد يؤثر هذا النوع من السرقة تأثيراً خطيراً على حقوق الفرد. وعلاوة على ذلك، يجوز استخدام البيانات البيومترية لأغراض تختلف عن الأغراض التي جُمعت من أجلها، بما في ذلك تعقب الأفراد بشكل غير قانوني ومراقبتهم. ونظراً إلى هذه المخاطر، ينبغي إيلاء اهتمام خاص لمسألتي الضرورة والتناسب في جمع البيانات البيومترية. وعليه، فإنه من المثير للقلق أن تشرع بعض الدول في مشاريع واسعة النطاق تقوم على البيانات البيومترية بدون أن تكون لديها ضمانات قانونية وإجرائية كافية.

تزايد القدرة التحليلية

١٥- يتواصل نمو القدرة التحليلية للتكنولوجيا القائمة على البيانات بسرعة متزايدة. وعلى نحو متزايد أيضاً، تتيح الدراسات التحليلية للبيانات الضخمة والذكاء الاصطناعي حصول الدول ومؤسسات الأعمال على معلومات بالغة الدقة عن حياة الناس، وإجراء استنتاجات بشأن خصائصهم البدنية والعقلية، وإنتاج مجموعات من الملامح المفصّلة عن شخصياتهم. كما أن العديد من النظم التي تستخدمها الحكومات ومؤسسات الأعمال قائمة لهذا الغرض تحديداً، أي الحصول على أكبر قدر ممكن من المعلومات عن الأفراد من أجل تحليلهم وتحديد ملامحهم وتقييمهم وتصنيفهم واتخاذ القرارات بشأنهم في النهاية، وتُتخذ هذه القرارات بالوسائل الآلية في الكثير من الأحيان.

١٦- وتنطوي البيئة الناجمة عن هذا الواقع على مخاطر بالنسبة إلى الأفراد والمجتمعات، وهي مخاطر لا يمكن المبالغة في تقدير أهميتها. فعلى سبيل المثال، شهدت السنوات الأخيرة انتهاكات للبيانات الشخصية على نطاق هائل، مما يعرض الأشخاص المعنيين لخطر سرقة الهوية والكشف عن معلومات حميمة. ويجري الربط بين جمع البيانات وتحليلها بشكل غير مشروع واستهداف فئات محددة من الناخبين. ويسع استخدام الملامح المتاحة وعمليات تصنيف الأفراد ضمن "درجات" أو "مرتبات" بغية تقييم أهلية الحصول على الرعاية الصحية، وتغطية التأمين الصحي، والخدمات المالية وغيرها. وقد تؤدي القرارات المستندة إلى بيانات غير شفافة في قضايا ذات مخاطرة عالية، مثلاً في إجراءات تحديد العقوبات وعمليات تقييم معاودة الإجرام، إلى المساس بالإجراءات القانونية الواجبة. كما أن المحاولات الرامية إلى تحديد الأفراد باعتبارهم يشكلون تهديدات أمنية محتملة في سياق عمل الشرطة التنبؤي تثير الشواغل، في ضوء المسائل المطروحة بشأن الشفافية، واتساع نطاق الإجراءات المتخذة، وواجب المساءلة، واحتمالات نشوء ممارسات تمييزية[١٨].

باء- المراقبة التي تفرضها الدولة واعتراض الاتصالات

المراقبة على نطاق واسع

١٧- يواصل العديد من الدول تنفيذ عمليات مراقبة سرية على نطاق واسع واعتراض الاتصالات، بما يشمل جمع وتخزين وتحليل بيانات جميع المستخدمين فيما يتعلق بمجموعة واسعة من وسائل الاتصال (مثلاً رسائل البريد الإلكتروني، والمكالمات الهاتفية والمكالمات بالفيديو، والرسائل النصية، والمواقع الشبكية التي تمت زيارتها). وبينما يزعم بعض الدول أن هذه المراقبة الجماعية العشوائية ضرورية لحماية الأمن القومي، فإن هذه الممارسة "لا يُسمح بها بموجب القانون الدولي لحقوق الإنسان، بما أنه لا يمكن إجراء تحليل فردي من حيث الضرورة والتناسب في سياق هذه التدابير" (انظر A/HRC/33/29، الفقرة ٥٨)[١٩]. وعلى نحو ما أشارت إليه المحكمة الأوروبية لحقوق الإنسان، "فقد يؤدي نظام المراقبة السرية المنشأ لحماية الأمن القومي إلى تقويض أو حتى تدمير الديمقراطية تحت ستار الدفاع عنها"[٢٠].

الحصول على بيانات مستخدمي مؤسسات الأعمال

١٨- كثيراً ما تعتمد الدول على مؤسسات الأعمال من أجل جمع واعتراض البيانات الشخصية. فعلى سبيل المثال، تفرض بعض الدول على شركات الاتصالات الهاتفية وشركات تقديم خدمات الإنترنت أن يتاح لها الوصول المباشر إلى تدفقات البيانات الجارية عن طريق شبكاتها. وتثير هذه النظم التي تمكّن من الحصول على البيانات بطريقة مباشرة قلقاً شديداً، لأنها عرضة بوجه خاص لإساءة الاستعمال، وتميل إلى الالتفاف على الضمانات الإجرائية

(١٨) انظر: Ajay Sandhu, "Data driven policing: highlighting some risks associated with predicting crime", Human Rights Centre, Essex University.

(١٩) انظر أيضاً: A/HRC/27/37، الفقرة ٢٥.

(٢٠) انظر: *Roman Zakharov v. Russia*, para. 232.

الرئيسية[٢١]. وتطلب بعض الدول أيضاً أن يتاح لها الحصول على كميات ضخمة من المعلومات المجمعة والمخزنة لدى شركات الاتصالات الهاتفية وشركات تقديم خدمات الإنترنت. ولا تزال الدول تفرض التزامات إجبارية على شركات الاتصالات ومقدمي خدمات الإنترنت من أجل الاحتفاظ ببيانات الاتصالات لفترات طويلة من الزمن[٢٢]. ويُلزم العديد من هذه القوانين الشركات بالقيام عشوائياً بجمع وتخزين كافة البيانات بشأن حركة الاتصالات لكلّ المشتركين والمستخدمين فيما يتعلق بجميع وسائل الاتصال الإلكتروني. ويؤدي ذلك إلى الحد من قدرة الناس على التواصل دون أن يُكشف عن هويتهم، وتعريضهم إلى إساءة استعمال تلك الاتصالات، بل وقد ييسّر الكشف عنها لأطراف ثالثة، بما يشمل المجرمين، والمعارضين السياسيين، والمنافسين في مجال الأعمال، وذلك عن طريق الاختراق الحاسوبي أو غيره من أساليب خرق البيانات. وهذه القوانين تتجاوز حدود ما يمكن اعتباره ضرورياً وتناسبياً[٢٣].

الاختراق الحاسوبي

١٩- يبدو أن الحكومات تعتمد بشكل متزايد على برامجيات الاختراق الهجومية من أجل التسلل إلى الأجهزة الرقمية للأفراد. وهذا النوع من الاختراق الحاسوبي يتيح القيام عشوائياً باعتراض وجمع كل أنواع الاتصالات والبيانات، سواء كانت مشفّرة أو غير مشفّرة، ويتيح أيضاً الاطّلاع عن بُعد وبشكل سري على محتوى الأجهزة الشخصية والبيانات المخزنة فيها، مما يمكّن من إجراء مراقبة آنية للبيانات المتوافرة على هذه الأجهزة والتلاعب بها[٢٤]. وهذا يمثل خطراً ليس على الحق في الخصوصية فحسب، إنما أيضاً على الحقوق المتعلقة بالنزاهة الإجرائية عندما يُسمح باستخدام هذه الأدلة في الإجراءات القانونية (انظر A/HRC/23/40، الفقرة ٦٢) .كما يثير الاختراق الحاسوبي شواغل كبيرة متعلقة بالحصانة من الاختصاص المحلي، إذ يمكن أن يؤثر على الأفراد في شتى الولايات القضائية[٢٥]. وعلاوة على ذلك، يعتمد الاختراق الحاسوبي على استغلال أوجه الضعف في نُظم تكنولوجيا المعلومات والاتصالات، ويُسهم بالتالي في تصاعد التهديدات الأمنية لملايين المستخدمين.

المحاولات الرامية إلى إضعاف التشفير والقدرة على إخفاء الهوية

٢٠- ينجم عن المحاولات المتكررة من جانب الدول لإضعاف تكنولوجيا التشفير والحد من القدرة على الاستعانة بأدوات إخفاء الهوية تهديدات لأمن وسرية الاتصالات والأنشطة الأخرى على الإنترنت. ويدعو بعض الدول إلى إصدار إذن رسمي بالدخول من الأبواب الخلفية للاطّلاع على الاتصالات المشفرة، أو إلى إلزام مقدمي خدمات الاتصالات المشفرة بتسليم

(٢١) انظر: *Roman Zakharov v. Russia*, para. 270.

(٢٢) انظر: CCPR/C/ZAF/CO/1، الفقرتين ٤٢ و٤٣، وCCPR/C/PAK/CO/1، الفقرتين ٣٥ و٣٦.

(٢٣) انظر، على سبيل المثال، European Court of Justice joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Swedish Post and Telecom Authority and Secretary of State for the Home Department v. Watson*, judgment of 21 December 2016, para. 107؛ والوثيقة CCPR/C/ZAF/CO/1، الفقرتين ٤٢ و٤٣؛ والوثيقة CCPR/C/CMR/CO/5، الفقرتين ٣٩ و٤٠.

(٢٤) انظر: Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "Encryption and anonymity follow-up report" (June 2018).

(٢٥) انظر التقرير المقدم من المنظمة الدولية لحماية الخصوصية.

مفـاتيح التشـفير (انظـر A/HRC/29/32، الفقـرات ٣٨ إلى ٤٥) أو حـتى إلى حظـر أو عرقلـة تطبيقـات مؤمَّنـة معينـة في مجـال الاتصـالات، بمـا في ذلـك الرسـائل المشـفرة والشـبكات الخاصـة الافتراضية وشبكات إخفاء الهوية. إذ يتيح التشفير وإخفاء الهوية للأفراد والجماعات حيزاً من الخصوصية على الإنترنت للإعراب عن آرائهم وممارسة حرية التعبير دون تدخل تعسفي وغير قـانوني أو هجمـات تستهدفهم (A/HRC/29/32)[٢٦]. وتُستخدم أدوات التشفير وإخفـاء الهوية على نطاق واسع في جميع أنحاء العالم، بما في ذلك من جانب المدافعين عن حقوق الإنسان، ومنظمـات المجتمـع المـدني، والصـحفيين، والمبلِّغين عـن المخالفـات، والمنشـقين السياسـيين الـذين يواجهـون الاضـطهاد والمضـايقة. ومـن شـأن إضـعافهم أن يهـدد خصوصـية جميـع المسـتخدمين ويعرضـهم للتـدخلات غـير المشـروعة لـيس مـن جانـب الـدول فحسـب، إنمـا أيضـاً مـن جانـب الجهـات من غـير الـدول، بمـا في ذلـك الشـبكات الإجراميـة[٢٧]. ويتعـارض هـذا الأثـر العشـوائي الواسع النطاق مع مبدأ التناسب (انظر A/HRC/29/32، الفقرة ٣٦).

تبادل المعلومات الاستخبارية

٢١- تقوم الحكومات في جميع أنحاء العالم على نحو روتيني بتبادل المعلومات الاستخبارية عن الأفراد خارج أي إطار قانوني ودون رقابة كافية[٢٨]. ويطرح تبادل المعلومات الاستخبارية خطراً جسيماً يتمثل في إمكانية لجوء الدولة إلى هذا النهج للالتفاف على القيود القانونية المحلية، عن طريق الاعتماد على الآخرين للحصول على المعلومات ومن ثم تبادلها. وهذه الممارسة لا تفي بشرط المشروعية وقد تقوّض الحق في الخصوصية في جوهره (انظر A/HRC/27/37، الفقرة ٣٠). ويصبح التهديد الماثل أمام حماية حقوق الإنسان شديداً بالأخص عند تقاسم المعلومات الاستخبارية مع دول معروفة بضعف حالتها في مجال سيادة القانون و/أو بسجل طويل من الانتهاكات المنهجية المرتكبة في مجال حقوق الإنسان. وثمة احتمال بأن يكون قد تم الحصول على المعلومات الاستخبارية الواردة إلى دولة من دولة أخرى في انتهاكٍ للقانون الدولي، بوسائل منها التعذيب وغيره من ضروب المعاملة القاسية أو اللاإنسانية أو المهينة. وما يزيد من المخاطر المتعلقة بحقوق الإنسان نتيجةً لتبادل المعلومات الاستخبارية هو انعدام الشفافية والمساءلة في ترتيبات تبادل المعلومات الاستخبارية حالياً، وعدم خضوع هذه العملية للرقابة (انظر A/69/397، الفقـرة ٤٤، وCCPR/C/GBR/CO/7، الفقـرة ٢٤، وCCPR/C/SWE/CO/7، الفقـرة ٣٦). وفيما عدا استثناءات قليلة جداً، لم تتعامل التشريعات حتى الآن مع مسألة تبادل المعلومات

(٢٦) انظر أيضاً: UCI Law International Justice Clinic, “Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression”؛ وAmnesty International, “Encryption. A matter of human rights” (March 2016)؛ و Wolfgang Schulz and Joris van Hoboken, “Human rights and encryption”, United Nations Educational, Scientific and Cultural Organization (2016).

(٢٧) انظر: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138.

(٢٨) انظر: Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards* (April 2018) و www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf.

الاستخبارية بناءً على أسس قانونية سليمة امتثالاً لمبدأ الشرعية في إطار القانون الدولي لحقوق الإنسان[٢٩].

الحصول على البيانات التي تحتفظ بها مؤسسات الأعمال عبر الحدود الوطنية

٢٢- في الآونة الأخيرة، بُذلت جهود لإنشاء آليات قانونية بغية تيسير حصول الدول على المعلومات الشخصية المخزنة على خواديم مؤسسات الأعمال في الخارج. ومما لا شك فيه أن الحصول على الأدلة في سياق تحقيق جنائي يمثل هدفاً هاماً ومشروعاً. بيد أن هذه الإمكانية يمكن أن تؤدي إلى إضعاف الضمانات الإجرائية أو إلى الالتفاف عليها، ويُذكر من بين تلك الضمانات شرط الحصول على إذن من هيئة مستقلة وإنشاء آليات الرقابة اللازمة لهذه الغاية. وقد تؤثر الطلبات الواردة عبر الحدود الوطنية تأثيراً سلبياً على تمكّن الأفراد من استئناف الأحكام القضائية والاستعانة بآليات الانتصاف. وما يثير القلق بوجه خاص هو الإمكانية المتاحة لدول معروفة بضعف حالتها في مجال سيادة القانون و/أو بسجلات تطرح إشكالاً في مجال حقوق الإنسان للحصول على معلومات حساسة بشأن الأفراد بدون أن تتوافر لهؤلاء الحماية الكافية من الانتهاكات المتعلقة بحقوق الإنسان.

رابعاً- مسؤوليات الدول

ألف- مسؤولية الدول عن احترام الحق في الخصوصية وواجب حمايته في العصر الرقمي

٢٣- تُلزم المادة ٢(١) من العهد الدولي الخاص بالحقوق المدنية والسياسية الدول باحترام وكفالة الحقوق المعترف بها في العهد لجميع الأفراد الموجودين داخل أراضيها و/أو الخاضعين لولايتها، دون أي تمييز. ويتعين على الدول الأطراف في العهد الامتناع عن انتهاك الحقوق المعترف بها في العهد، كما يجب أن تكون أي قيود يتم فرضها على أيٍّ من الحقوق المعترف بها جائزةً بموجب الأحكام ذات الصلة من العهد[٣٠]. غير أن التزامات الدول لا تقتصر على الالتزام باحترام الحقوق بل تشمل أيضاً تدابير "إيجابية" لحماية التمتع بالحقوق. وفي سياق الحق في الخصوصية، هذا يعني واجب اتخاذ تدابير تشريعية وغيرها من التدابير لإنفاذ حظر التدخل والتهجم على نحو غير قانوني أو تعسفي والحماية منهما، سواء كانا صادرين عن سلطات الدولة أم عن أشخاص طبيعيين أو اعتباريين[٣١].

٢٤- وينعكس واجب الحماية في الركيزة الأولى للمبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان، المعنونة "واجب الدولة في حماية حقوق الإنسان"، التي توضح النتائج المترتبة على واجب الدول في الحماية من الآثار الضارة بحقوق الإنسان الناجمة عن الشركات. وينص المبدأ ١ من المبادئ التوجيهية على اتخاذ الخطوات المناسبة لمنع انتهاكات حقوق الإنسان والتحقيق فيها والمعاقبة عليها والانتصاف منها، عن طريق سياسات وتشريعات وأنظمة وأحكام قضائية فعالة. وتُبين المبادئ اللاحقة مختلف المجالات القانونية ومجالات السياسة العامة التي

(٢٩) انظر التقرير المقدم من المنظمة الدولية لحماية الخصوصية.

(٣٠) انظر: اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٣١، الفقرة ٦.

(٣١) انظر: اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ١٦، الفقرتين ١ و٩؛ والتعليق العام رقم ٣١، الفقرة ٨.

ينبغي للدول أن تعتمد فيها "مزيجاً ذكياً من التدابير" الإلزامية والطوعية على الصعيدين الوطني والدولي، من أجل تعزيز احترام حقوق الإنسان من جانب مؤسسات الأعمال[٣٢]. وتشمل الأمثلة بشأن تطبيق النهج المنصوص عليه في المبادئ التوجيهية، فيما يتعلق بقطاع تكنولوجيا المعلومات والاتصالات، التوجيه القطاعي القائم على مستوى الاتحاد الأوروبي، الذي يركز على الكيفية التي ينبغي أن تتعامل بها مؤسسات تكنولوجيا المعلومات والاتصالات مع أي آثار ضارة تنجم عن أنشطتها.

٢٥- وينطوي واجب الدول في الحماية من انتهاك الحق في الخصوصية من جانب الشركات والأطراف الثالثة الأخرى المنشأة/التي يوجد مقرها ضمن الولاية القضائية للدولة المعنية على آثار تتجاوز حدود تلك الولاية. فعلى سبيل المثال، ينبغي أن يكون لدى الدول نظم لمراقبة الصادرات تسري على تكنولوجيات المراقبة، وتنص على تقييم الإطار القانوني الذي يحكم استخدام تلك التكنولوجيات في بلد المقصد، وسجل المستخدم النهائي المقترح في مجال حقوق الإنسان، وضمانات وإجراءات رقابية لاستخدام صلاحيات المراقبة. ويجب إدراج الضمانات المتعلقة بحقوق الإنسان في اتفاقات رخص التصدير. وعلاوة على ذلك، تقع على عاتق الدول حماية الأشخاص الخاضعين لولايتها القضائية من التدخل في حقهم في الخصوصية خارج الحدود الإقليمية، من قبيل وسائل اعتراض الاتصالات أو الاختراق الحاسوبي.

باء- مسؤولية الدول عن وضع الضمانات الكافية وإجراءات المراقبة الفعالة

٢٦- يعتمد التمتع بالحق في الخصوصية إلى حد كبير على وجود إطار قانوني وتنظيمي ومؤسسي ينص على وجود ضمانات كافية، بما في ذلك آليات المراقبة الفعالة. ففي عصر تتوافر فيه للدول ولمؤسسات الأعمال إمكانية الحصول على كم هائل من البيانات الشخصية، حيث لا يملك الأفراد سوى معرفة محدودة بالكيفية التي يتم بها استخدام المعلومات المتعلقة بهم وبحياتهم والتحكم بها، من الضروري التركيز على التدابير الكفيلة بالتخفيف من الأثر المترتب على حقوق الإنسان نتيجةً لعدم التماثل على صعيدي القوة والمعلومات.

١- الإطار الشامل للحماية من التدخل غير المبرر

٢٧- ينبغي أن يستند الإطار الذي تضعه الدولة بغية حماية الخصوصية أساساً إلى قوانين تتعلق بمعايير معالجة المعلومات الشخصية من قِبَل الدول والجهات الفاعلة في القطاع الخاص على حد سواء[٣٣]. وبينما تتمتع الدول بسلطة تقديرية لتحديد مزيج ذكي من التدابير التي تنظم استخدام المعلومات الشخصية من جانب الشركات، فإن المادة ١٧(٢) من العهد الدولي الخاص بالحقوق المدنية والسياسية تنص على ضرورة حماية الأفراد بمقتضى القانون. كما أن الترابط المتزايد بين معالجة البيانات العامة والبيانات الخاصة، والسجل المتاح بهذا الشأن حتى

(٣٢) انظر المبدأ ٢، الشرح.

(٣٣) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ١٦، الفقرة ٩، وA/HRC/13/37، الفقرة ٦١، وA/HRC/17/27، الفقرة ٥٦. وللاطلاع على لمحة عالمية شاملة بشأن التشريعات المتعلقة بخصوصية البيانات، انظر: Graham Greenleaf, University of New South Wales، المعلومات المقدمة لإدراجها في هذا التقرير. وفي هذا التقرير، يُقصد بمصطلح "معالجة" أي عملية تُجرى على البيانات الشخصية، بما في ذلك جمعها، والاحتفاظ بها، واستخدامها، وتعديلها، وحذفها، والكشف عنها، وإحالتها، ودمجها.

الآن الذي يشير إلى إساءة الاستعمال المتكررة على نطاق واسع للمعلومات الشخصية من جانب بعض مؤسسات الأعمال، كلها عوامل تؤكد ضرورة وضع تدابير تشريعية لبلوغ مستوى كافٍ من الحماية فيما يتعلق بالخصوصية[٣٤].

٢٨- ويتزايد توافق الآراء القائم على الصعيد العالمي بشأن المعايير الدنيا التي ينبغي أن تحكم معالجة البيانات الشخصية من جانب الدول ومؤسسات الأعمال والجهات الفاعلة الأخرى في القطاع الخاص. وتشمل الصكوك الدولية والمبادئ التوجيهية التي تعكس هذا التطور المبادئ التوجيهية لعام ١٩٩٠ لتنظيم استخدام ملفات البيانات الشخصية المجهزة إلكترونياً؛ واتفاقية مجلس أوروبا لعام ١٩٨١ بشأن حماية الأفراد فيما يخص المعالجة الآلية للبيانات الشخصية وصيغتها المحدثة، التي تحدد مستوى عالياً من الحماية على الصعيد الدولي[٣٥]؛ والمبادئ التوجيهية بشأن الخصوصية لعام ١٩٨٠ التي وضعتها منظمة التعاون والتنمية في الميدان الاقتصادي وجرى استكمالها في عام ٢٠١٣؛ واتفاقية الاتحاد الأفريقي المتعلقة بأمن الفضاء الإلكتروني وحماية البيانات الشخصية لعام ٢٠١٤ (اتفاقية مالابو)؛ وقرار مدريد الذي اعتمده المؤتمر الدولي للمفوضين المعنيين بالخصوصية وحماية البيانات؛ والإطار المتعلق بالخصوصية لعام ٢٠١٥ الصادر عن منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ، في جملة صكوك أخرى. وقد جرى الاسترشاد بهذه المعايير، ولا سيما الاتفاقية بشأن حماية الأفراد فيما يخص المعالجة الآلية للبيانات الشخصية، من أجل وضع الأطر المتعلقة بخصوصية البيانات للعديد من الدول، ويمكن الاسترشاد بها أيضاً بغية تصميم الأدوات المناسبة في مجال السياسة العامة[٣٦].

٢٩- وتنص الصكوك والمبادئ التوجيهية المذكورة أعلاه على مجموعة من المبادئ والحقوق والالتزامات الرئيسية التي تكفل الحد الأدنى من الحماية للبيانات الشخصية. فأولاً، ينبغي أن تكون معالجة البيانات الشخصية عادلة ومشروعة وشفافة. ويتعين إبلاغ الأفراد المعنيين بأن معالجة بياناتهم الشخصية جارية، وبالظروف المحيطة بهذه العملية، وبطابعها ونطاقها، بوسائل منها السياسات الشفافة المتعلقة بخصوصية البيانات. ومنعاً لاستخدام المعلومات الشخصية بشكل تعسفي، ينبغي أن تستند معالجة البيانات الشخصية إلى الموافقة الحرة، والمحددة، والمستنيرة، والقطعية للأفراد المعنيين، أو إلى أساس شرعي آخر منصوص عليه في القانون[٣٧]. ويتعين أن تكون معالجة البيانات الشخصية ضرورية وتناسبية مع غرض مشروع يحدّده الكيان الذي يقوم بمعالجة البيانات. وبناءً على ذلك، يجب أن تكون كمية البيانات وأنواعها وفترة الاحتفاظ بها محدودة، وأن تتسم البيانات بالدقة، وأن تُستخدم تقنيات إخفاء الهوية والأسماء المستعارة كلما أمكن ذلك. كما ينبغي تجنب التغيير في الغرض المنشود من البيانات بدون موافقة

(٣٤) انظر قراري مجلس حقوق الإنسان ٧/٣٤، الفقرة ٥(و)، و٧/٣٨، الفقرة ١٧.

(٣٥) بالإضافة إلى الدول الأعضاء في مجلس أوروبا البالغ عددها ٤٧ دولة، صدَّق على الاتفاقية كل من أوروغواي، وتونس، والسنغال، وموريشيوس. كما أن ثمة عدة دول أخرى بصدد الانضمام إلى الاتفاقية.

(٣٦) للاطلاع على التوجيهات بالتفصيل، انظر: https://privacyinternational.org/advocacy-briefing/2165/guide-policy-engagement-data-protection، و Access Now, "Creating a data protection framework: a do's and don'ts guide for lawmakers. Lessons from the EU general data protection regulation" (2018).

(٣٧) انظر المادة ٥(٢) من الصيغة المحدثة لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية؛ والمادة ١٣(١) من اتفاقية مالابو؛ والمبدأ ١٢ من قرار مدريد.

الشخص المعني، وعند القيام بذلك، لا بد من أن تقتصر التغييرات على أغراض تتوافق مع الغرض المحدد في البداية. ونظراً إلى تأثر البيانات الشخصية بعملية الكشف عنها بدون إذن، أو تعديلها أو حذفها، من الضروري اتخاذ التدابير الأمنية اللازمة في هذا الصدد. وعلاوة على ذلك، ينبغي أن تخضع الكيانات التي تقوم بمعالجة البيانات الشخصية للمساءلة عن مدى امتثالها للإطار القانوني والسياساتي الواجب التطبيق لمعالجة البيانات. وأخيراً، ينبغي أن تتمتع البيانات الحساسة بمستوى عال جداً من الحماية(٣٨).

٣٠- وفي جميع الصكوك والمبادئ التوجيهية المذكورة أعلاه، من المسلم به أن حقوقاً معينة يجب أن تُمنح للأشخاص الذين تجري معالجة بياناتهم. وكحد أدنى، يحق للأشخاص المتأثرين أن يكونوا على علم بأن ثمة بيانات شخصية تخصهم جرى الاحتفاظ بها ومعالجتها، وأن تتاح لهم إمكانية الاطّلاع على البيانات المخزنة، وتصحيح البيانات غير الدقيقة أو التي تجاوزتها الأحداث، وحذف أو تصحيح البيانات المخزنة بصورة غير قانونية أو غير ضرورية. كما تنص الصكوك الجديدة على حقوق إضافية هامة، منها على وجه الخصوص حق الاعتراض على معالجة البيانات الشخصية، أقلّه في الحالات التي لا يبيّن فيها الكيان الذي يقوم بتجهيزها أسباباً مشروعة وأساسية لذلك(٣٩). وينبغي أن تولي الدول اهتماماً خاصاً لتوفير حماية قوية من التدخل في الحق في الخصوصية عن طريق التحديد النمطي لمواصفات الأشخاص واتخاذ القرارات بشكل آلي. ويتعين أن تنطبق الحقوق المذكورة أعلاه أيضاً على المعلومات المستمدة والمستخلصة والمتنبّأ بها بوسائل آلية، ما دام يمكن اعتبار تلك المعلومات بياناتٍ شخصية. ومن المهم أن يكفل الإطار القانوني عدم إخضاع الحق في حرية التعبير للقيود التي تفرضها تلك الحقوق دون مبرر، بما في ذلك معالجة البيانات الشخصية لأغراض صحفية وفنية وأكاديمية.

٣١- ولا بد أيضاً من أن تنص الأطر المتعلقة بخصوصية البيانات على التزاماتٍ معينة للكيانات التي تقوم بمعالجة البيانات الشخصية. وهذا يشمل الجوانب التنظيمية، كإنشاء آلية مراقبة داخلية، فضلاً عن اتخاذ تدابير إلزامية، من قبيل الإخطار بخرق سرية البيانات، وإجراءات تقييم الأثر على الخصوصية. وفي بيئة تكنولوجية متزايدة التعقيد، تُسهم عمليات التقييم إسهاماً رئيسياً في منع وقوع أضرار متعلقة بالخصوصية والتخفيف من آثارها(٤٠). وعلاوة على ذلك، تمثِّل متطلبات تصميم المنتجات والخدمات، من قبيل كفالة الخصوصية بحكم التصميم(٤١) وكفالة الخصوصية بصفة تلقائية(٤٢)، أدواتٍ أساسية لحماية الحق في الخصوصية.

٣٢- وفي عالم تسوده العولمة، تُعتبر عمليات إحالة البيانات، بما في ذلك كميات كبيرة من البيانات الشخصية، أمراً شائعاً وضرورياً لتشغيل الكثير من الخدمات. ويجب على الدول أن تكفل ألا تؤدي هذه العمليات إلى تدخل غير مبرر في الحق في الخصوصية أو إلى تيسير ذلك

(٣٨) انظر المادة ٦ من الصيغة المحدثة لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية.

(٣٩) المرجع نفسه، المادة ٩(١)(د). انظر أيضاً المادة ٢١ من النظام العام لحماية البيانات والمادة ١٨(١) من اتفاقية مالابو.

(٤٠) للاطلاع على تحليل متعمق لنُهج تقييمات الأثر على الخصوصية، انظر: David Wright and Paul de Hert, eds., *Privacy Impact Assessment* (New York, Springer, 2012).

(٤١) بمعنى أنه يجب إدماج حماية الخصوصية منذ البداية عند تصميم نظام ما.

(٤٢) الالتزام بأن يكون النظام مهيّأ لاحترام الخصوصية بصفة تلقائية.

التدخل. وفي الوقت نفسه، يُستصوب تجنب وضع شروط صارمة بشأن تحديد موقع البيانات من أجل إلزام جميع الكيانات المعنية بالمعالجة بتخزين كافة البيانات الشخصية داخل البلد المعني (انظر، الفقرة ٦١) A/HRC/32/38. وعوضاً عن ذلك، ينبغي أن تركز الدول على سبل ضمان حماية البيانات الشخصية المنقولة إلى دول أخرى، أقله على المستوى المطلوب بموجب أحكام القانون الدولي لحقوق الإنسان.

٣٣- وينبغي للدول إنشاء هيئات رقابية مستقلة لمعالجة البيانات الشخصية. فهذه الهيئات ضرورية لحماية حقوق الإنسان للفرد من الممارسات التي تفرط في معالجة البيانات الشخصية. ويتعين أن تستند الهيئة الرقابية إلى قاعدة قانونية لتحديد ولايتها وصلاحياتها واستقلالها بوضوح. كما ينبغي تزويد الهيئة الرقابية بالموارد التقنية والمالية والبشرية اللازمة للقيام برصد فعال لأنشطة معالجة البيانات التي تقوم بها الدول ومؤسسات الأعمال، ولإنفاذ الشروط القانونية في هذا الصدد. وعلاوة على ذلك، يجب تزويد الهيئة الرقابية بالسلطة القانونية الكافية للاضطلاع بمهامها، بما في ذلك فرض جزاءات تتناسب مع الانتهاكات أو التجاوزات المرتكبة[٤٣].

٢- الضمانات الإجرائية والإشراف على عمليات المراقبة واعتراض الاتصالات

الضمانات

٣٤- مع أن جميع أنواع الأنشطة التي تضطلع بها الدول في مجال المراقبة يجب أن تقوم على أساس القانون (انظر A/HRC/27/37، الفقرة ٢٨)، فإن المقرر الخاص المعني بالحق في الخصوصية قد وجَّه الانتباه إلى عدم توافر التشريعات اللازمة بهذا الشأن على نطاق واسع. ومن الجدير بالذكر أنه في العديد من الولايات القضائية، يتم استبعاد وكالات الاستخبارات وإنفاذ القانون من أحكام التشريعات المتعلقة بخصوصية البيانات. وينبغي أن تكون هذه الاستثناءات محدودة، وأن تستند إلى مبدأي الضرورة والتناسب لكفالة مستوى كافٍ من خصوصية البيانات في جميع فروع الحكومة. ويتعين أن تسترشد التشريعات الخاصة بالمراقبة بالمعايير الدنيا الواردة أدناه.

٣٥- يكون الاطّلاع على أحكام القانون متاحاً لعامة الجمهور. أما القواعد السرية والتفسيرات السرية للقانون، فلا تتوافر لها الصفات الضرورية لكي تُعتبر "قانوناً" (المرجع نفسه، الفقرة ٢٩). وتكون القوانين دقيقة بما فيه الكفاية. ويجري تحديد السلطة التقديرية الممنوحة إلى السلطة التنفيذية أو إلى قاضٍ، وكيفية ممارستها، بدرجة معقولة من الوضوح (انظر A/69/397، الفقرة ٣٥)[٤٤]. وتحقيقاً لهذه الغاية، لا بد من وصف طبيعة الجرم المعني وفئة الأشخاص الذين قد يخضعون للمراقبة. ولا تُعتبر المبررات الغامضة والفضفاضة، كالإشارات غير الدقيقة إلى "الأمن القومي"، قوانين واضحة على نحو كاف. ويجب أن ترتكز المراقبة على أسباب كافية، وأن يكون أي قرار يأذن بالمراقبة محدد الهدف بشكل وافٍ.[٤٥] ويجب أن يُسنِد القانون صراحةً اختصاصات إجراء المراقبة والحصول على نتاج المراقبة إلى سلطات محددة.

(٤٣) انظر، على سبيل المثال، https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

(٤٤) انظر أيضاً: *Roman Zakharov v. Russia*, para. 230.

(٤٥) المرجع نفسه، الفقرتان ٢٤٨ و٢٦٠.

٣٦- وعلى صعيد نطاق المراقبة، ينبغي أن يشمل الإطار القانوني طلباتِ الدول الواردة إلى مؤسسات الأعمال. وينبغي أن يشمل أيضاً الحصول على المعلومات التي يُحتفظ بها خارج الحدود الإقليمية أو تبادل المعلومات مع الدول الأخرى. ويتعين أن ينص القانون بوضوح على هيكل يكفل المساءلة والشفافية داخل المؤسسات الحكومية التي تقوم بالمراقبة.

٣٧- ولا يمكن تبرير صلاحيات المراقبة السرية إلا إذا كانت ضرورية تماماً لتحقيق هدف مشروع، وتستوفي شرط التناسب (انظر A/HRC/23/40، الفقرة ٨٣(ب))[٤٦]. ويجب أن تقتصر تدابير المراقبة السرية على منع أخطر الجرائم أو التهديدات، أو التحقيق فيها. ويتعين أن تقتصر فترة المراقبة على الحد الأدنى اللازم لتحقيق الهدف المحدد. وينبغي أن تكون ثمة قواعد صارمة لاستخدام وتخزين البيانات التي تم الحصول عليها، وأن توضَّح تماماً الظروف التي تستلزم حذف البيانات التي جرى جمعها وتخزينها، بناءً على مبدأي الضرورة القصوى والتناسب[٤٧]. ويجب أن يخضع تبادل المعلومات الاستخبارية لنفس مبادئ المشروعية والضرورة القصوى والتناسب.

٣٨- وحيثما تنظر الحكومات في اتخاذ تدابير محددة الأهداف لتنفيذ اختراق حاسوبي، ينبغي أن تتبع نهجاً حذراً للغاية، وألا تلجأ إلى هذه التدابير إلا في ظروف استثنائية للتحقيق في أخطر الجرائم أو التهديدات أو منعها. ويجب أن يتم ذلك بمشاركة السلطة القضائية (انظر CCPR/C/ITA/CO/6، الفقرة ٣٧)[٤٨]. كما ينبغي تصميم عمليات الاختراق الحاسوبي بدقة، لكي ينحصر الحصول على المعلومات في أهداف معينة وأنواع محددة من المعلومات. وينبغي أيضاً أن تمتنع الدول عن إرغام الكيانات الخاصة على مساعدتها في عمليات الاختراق الحاسوبي، لما لذلك من آثار على أمن منتجاتها وخدماتها. ولا يجوز السماح بفرض فك الشفرة إلا على أساس كل حالة على حدة وفقاً لهدف محدد، ورهناً بأمر قضائي وضرورة حماية حقوق الأفراد في الإجراءات القانونية الواجبة (انظر A/HRC/29/32، الفقرة ٦٠).

منح الإذن وممارسة الرقابة بصفة مستقلة[٤٩]

٣٩- ينبغي أن تخضع تدابير المراقبة، بما في ذلك طلبات الحصول على بيانات الاتصالات من مؤسسات الأعمال وتبادل المعلومات الاستخبارية، لصدور إذن لهذه الغاية، على أن يتم استعراض تلك التدابير والإشراف عليها من جانب هيئات مستقلة في جميع المراحل، بما في ذلك عند طلبها لأول مرة، وأثناء تنفيذها وبعد إنهائها (انظر CCPR/C/FRA/CO/5، الفقرة ٥)[٥٠]. ولا بد للهيئة المستقلة التي تأذن بتدابير المراقبة الخاصة، والتي يفضَّل أن تكون سلطة قضائية، من التحقق من وجود أدلة واضحة وتهديدات مبررة لإجرائها، ومن أن المراقبة المقترحة هي مراقبة محددة الأهداف وضرورية للغاية وتناسبية وتجيز مسبقاً تدابير المراقبة (أو لا تجيزها).

---

(٤٦) انظر أيضاً: *Szabo and Vissy v. Hungary*, para. 73.

(٤٧) انظر: *Roman Zakharov v. Russia*, para. 231.

(٤٨) انظر أيضاً: Access Now, "A human rights response to government hacking" (September 2016) و"Privacy International, "Government hacking and surveillance: 10 necessary safeguards".

(٤٩) انظر: A/HRC/34/60 و European Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update*, (Luxembourg, Publications Office of the European Union, 2017).

(٥٠) انظر أيضاً: *Roman Zakharov v. Russia*, para. 233.

٤٠- ويمكن أن تتضمن أطر الرقابة مزيجاً من الرقابة الإدارية و/أو القضائية و/أو البرلمانية[٥١]. وينبغي أن تكون هيئات الرقابة مستقلة عن السلطات التي تقوم بالمراقبة، ومجهزةً بالخبرات والكفاءات والموارد المناسبة والكافية. كما ينبغي إقامة فصل بين صدور الإذن والاضطلاع بأنشطة الرقابة من الناحية المؤسسية. ويتعين أن تقوم هيئات الرقابة المستقلة بالتحقيق بشكل استباقي في أنشطة الذين ينفذون المراقبة، وأن تقوم برصدها أيضاً، وأن تتاح لها إمكانية الاطّلاع على نتاج المراقبة. وينبغي لها إجراء استعراضات دورية لقدرات عملية المراقبة والتطورات التكنولوجية المستجدة. وينبغي أن تكون الوكالات التي تقوم بالمراقبة ملزَمة بتوفير جميع المعلومات اللازمة للخضوع لرقابة فعالة عند الطلب، وبتقديم تقارير منتظمة إلى هيئات الرقابة، وينبغي أن تكون ملزَمة بالاحتفاظ بسجلات جميع تدابير المراقبة[٥٢]. ويجب أن تكون عمليات الرقابة شفافة وتخضع للتدقيق العام الملائم. كما تخضع القرارات الصادرة عن هيئات الرقابة لإمكانية الطعن أو المراجعة المستقلة. وإن عرض وجهات نظر متباينة على هيئات الرقابة، مثلاً من خلال مشاورات الخبراء وأصحاب المصلحة المتعددين (انظر، على سبيل المثال، A/HRC/34/60، الفقرة ٣٦)، يكتسي أهمية بوجه خاص في غياب عملية مقاضاة حضورية، إذ من الضروري أن يتم إرساء "نقاط احتكاك"، وأن تكون ثمة تحديات مستمرة للنُهج والتفاهمات القائمة[٥٣].

مبدأ الشفافية

٤١- لا بد لسلطات الدولة والهيئات الرقابية من المشاركة أيضاً في أنشطة إعلامية بشأن القوانين والسياسات والممارسات القائمة في مجال المراقبة واعتراض الاتصالات وغيرها من أشكال معالجة البيانات الشخصية، باعتبار أن المناقشة المفتوحة والتدقيق أمران ضروريان لفهم مزايا تقنيات المراقبة وقيودها (انظر A/HRC/13/37، الفقرة ٥٥). وينبغي إخطار الأشخاص المعنيين بأنهم كانوا موضع مراقبة، والقيام، بمقتضى الأمر الواقع، بتوضيح التدخل الذي جرى في حقهم في الخصوصية. وينبغي أن يحق لهم تغيير و/أو حذف المعلومات الشخصية غير ذات الصلة بالهدف المحدد لعملية المراقبة، بشرط ألا تكون هناك حاجة إلى تلك المعلومات بعد ذلك لإجراء أي تحقيق حالي أو معلق (انظر A/HRC/34/60، الفقرة ٣٨).

خامساً- مسؤوليات مؤسسات الأعمال

٤٢- توفر الركيزة الثانية من المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان مخططاً معتمداً لجميع المؤسسات، بصرف النظر عن حجمها وقطاع عملها وسياقها التشغيلي وملكيتها وهيكلها، من أجل منع ومعالجة جميع الآثار الضارة بحقوق الإنسان، بما في ذلك الحق في الخصوصية[٥٤]. ويبين المخطط مسؤولية مؤسسات الأعمال عن احترام جميع حقوق الإنسان

(٥١) انظر قرار الجمعية العامة ١٩٩/٧١، الفقرة ٥(د).

(٥٢) انظر: European Court of Human Rights, *Kennedy v. United Kingdom*, application No. 26839/05, judgment of 18 May 2010, para. 165، و*Roman Zakharov v. Russia*, para. 272.

(٥٣) انظر المعلومات المقدمة من Human Rights, Big Data and Technology Project, Human Rights Centre, University of Essex لإدراجها في هذا التقرير.

(٥٤) أقرَّ مجلس حقوق الإنسان المبادئ التوجيهية بالإجماع في قراره ٤/١٧.

المعترف بها دولياً، مما يعني أنه ينبغي لها أن تتجنب انتهاك حقوق الإنسان للآخرين ومعالجة الآثار الضارة بحقوق الإنسان التي تشارك في التسبب بها[٥٥]. وتسري المسؤولية عن احترام تلك الحقوق على جميع أنشطة الشركات وعلاقاتها التجارية. ومن المهم بوجه خاص، في الفضاء الرقمي، أن تنطبق المسؤولية عن احترام الحقوق بصرف النظر عن مكان تواجد الأشخاص المتضررين. وتسري المسؤولية عن احترام الحقوق بشكل مستقل عما إذا كانت الدولة تفي بالتزاماتها الخاصة بحقوق الإنسان أم لا.

٤٣- ويتطلب الوفاء بالمسؤولية عن احترام حقوق الإنسان أن تقوم مؤسسات الأعمال بما يلي: (أ) تفادي التسبب في آثار ضارة عن طريق الأنشطة التي تضطلع بها؛ (ب) تجنب الإسهام في إحداث الآثار الضارة عن طريق الأنشطة التي تضطلع بها، سواء بصورة مباشرة أو عن طريق بعض الكيانات الخارجية (الحكومات أو الأعمال التجارية أو غيرها)؛ (ج) السعي إلى منع الآثار الضارة بحقوق الإنسان التي ترتبط ارتباطاً مباشراً بعملياتها أو منتجاتها أو خدماتها في إطار علاقاتها التجارية، أو التخفيف منها، حتى ولو لم تكن قد أسهمت في إحداثها[٥٦]. فعلى سبيل المثال، تسهم الشركة التي تقدّم بياناتٍ بشأن المستخدمين إلى حكومة تقوم بعد ذلك باستعمال البيانات لتعقب المعارضين السياسيين وملاحقتهم قضائياً، في ارتكاب انتهاكاتٍ لحقوق الإنسان، بما في ذلك الحق في الخصوصية. كما أن الشركات التي تصنّع وتبيع التكنولوجيات المستخدمة في التدخلات غير القانونية أو التعسفية تسهم هي الأخرى في حدوث الآثار الضارة بحقوق الإنسان.

٤٤- وإذا كانت المطالب متضاربة فيما بين واجب احترام القانون الدولي لحقوق الإنسان والالتزامات القائمة بمقتضى القانون الوطني، ينبغي للشركات أن تسعى إلى احترام القانون الدولي لحقوق الإنسان إلى أقصى حد ممكن والتخفيف قدر الإمكان من أي أثر ضار، مثلاً عن طريق تفسير المطالب الحكومية بأكبر قدر ممكن من الدقة[٥٧].

٤٥- ويتطلب الوفاء بالمسؤولية عن احترام حقوق الإنسان أن تضع مؤسسات الأعمال سياساتٍ وإجراءات تتلاءم مع حجمها وظروف عملها، بما في ذلك ما يلي:

(أ) الإعلان عن الالتزام بالسياسة العامة على أعلى مستوى، وإدراج المسؤولية عن احترام حقوق الإنسان في جميع السياسات والإجراءات التشغيلية[٥٨]؛

(ب) تنفيذ عمليات بذل العناية الواجبة في مراعاة حقوق الإنسان، التي تستتبع ما يلي:

'١' إجراء عمليات تقييم الأثر على حقوق الإنسان من أجل تحديد وتقييم أي آثار ضارة بحقوق الإنسان، سواء كانت فعلية أو محتملة؛

'٢' إدماج نتائج التقييم في العمليات واتخاذ الإجراءات المناسبة لمنع أو تخفيف الآثار الضارة بحقوق الإنسان التي تم تحديدها؛

(٥٥) المبدأ التوجيهي ١١.

(٥٦) المبدأ التوجيهي ١٣. انظر أيضاً: OHCHR, "The corporate responsibility to respect human rights: an interpretive guide" (2012).

(٥٧) المبدأ التوجيهي ٢٣.

(٥٨) المبدأ التوجيهي ١٦.

'٣' تتبع فعالية الجهود المبذولة؛

'٤' الإبلاغ رسمياً عن الكيفية التي تمت بها معالجة الآثار الناجمة نتيجةً لأنشطتها على حقوق الإنسان[٥٩]؛

(ج) توفير سبل معالجة الانتهاكات أو التعاون مع الجهات الأخرى من أجل معالجة الانتهاكات حيثما تحدد الشركة آثاراً ضارة تسببت فيها أو أسهمت في حدوثها[٦٠].

٤٦- ووفقاً للمبادئ التوجيهية، تقع على عاتق جميع الشركات مسؤولية بذل العناية الواجبة في مراعاة حقوق الإنسان لتحديد ومعالجة أي آثار تمس حقوق الإنسان نتيجةً لأنشطتها. ومن الأمثلة الملموسة على ذلك أنه ينبغي للشركات التي تبيع تكنولوجيات المراقبة القيام، في إطار بذل العناية الواجبة، بتقييم شامل للأثر الناجم على حقوق الإنسان قبل أي معاملة تجارية محتملة. وينبغي أن تشمل تدابير تخفيف المخاطر ضماناتٍ واضحة بشأن الاستعمال النهائي، على أن يكون منصوصاً عليها في اتفاقات تعاقدية تشمل ضمانات قوية لحقوق الإنسان، وتمنع الاستخدام التعسفي أو غير القانوني للتكنولوجيا، وتكفل إجراء الاستعراضات الدورية لاستخدام التكنولوجيا من جانب الدول[٦١]. ويتعين على الشركات التي تجمع بيانات المستخدمين وتحتفظ بها أن تقيِّم المخاطر المتعلقة بالخصوصية نتيجةً للطلبات التي قد تتلقاها من الدول للحصول على هذه البيانات، بما في ذلك السياق القانوني والمؤسسي للدول المعنية. ويجب أن توفر الشركات إجراءات وضمانات كافية لمنع وتخفيف الأضرار المحتملة المتعلقة بالخصوصية وبحقوق الإنسان الأخرى. كما يجب إجراء عمليات تقييم الأثر على حقوق الإنسان في إطار شروط الخدمة وخيارات التصميم والهندسة التي لها انعكاسات على الأمن والخصوصية، وكذلك في إطار اتخاذ القرارات لتوفير الخدمات أو إنهائها في سياق معين (انظر A/HRC/32/38، الفقرة ١١).

٤٧- وفي سياق عملية بذل العناية الواجبة في مراعاة حقوق الإنسان، تنص المبادئ التوجيهية على واجب مؤسسات الأعمال بأن تأخذ في الاعتبار الكيفية التي تعالج بها آثار أنشطتها على حقوق الإنسان، وبأن تكون مستعدة لإيصال تلك الرسالة إلى خارج المؤسسة، ولا سيما عند إثارة شواغل في هذا الصدد من جانب أصحاب المصلحة المتضررين أو باسمهم[٦٢]. وفي البيئة الرقمية، هذا يستتبع الإفصاح عن أي بيانات شخصية يتم جمعها، وطول الفترة التي يجري تخزينها، ولأي غرض، وكيفية استخدامها، ومع أي جهات، وفي أي ظروف يتم تبادلها. وهذا يشمل أيضاً الطلبات التي تتلقاها الدول للحصول على بيانات المستخدمين. وفي الحالات التي تعوق فيها القوانين والأنظمة الوطنية عملية الإبلاغ، تشجَّع الشركات على أن تستغل إلى أقصى حد ممكن أي نفوذ لديها وأن تبذل كل الجهود الممكنة من أجل إصدار هذه المعلومات.

(٥٩) المبادئ التوجيهية من ١٧ إلى ٢١.

(٦٠) المبدأ التوجيهي ٢٢ والفرع سادساً من هذا التقرير.

(٦١) انظر: المنظمة الدولية لحماية الخصوصية (Privacy International)، المعلومات المقدمة إلى المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير (كانون الثاني/يناير ٢٠١٦)، متاحة على الرابط التالي: www.ohchr.org/Documents/Issues/Expression/PrivateSector/PrivacyInternational.pdf.

(٦٢) المبدأ التوجيهي ٢١.

٤٨- وفي إطار تفعيل التزامات السياسة العامة بموجب المبادئ التوجيهية، وضع قطاع تكنولوجيا المعلومات والاتصالات توجيهات بشأن كيفية تنفيذ السياسات المتعلقة بحقوق الإنسان. وتشمل هذه المبادرات مبادئ مبادرة الشبكة العالمية بشأن حرية التعبير والخصوصية[٦٣] والمبادئ التوجيهية المتعلقة بحوار قطاع الاتصالات السلكية واللاسلكية[٦٤]. فعلى سبيل المثال، تنص مبادئ مبادرة الشبكة العالمية تحديداً على أن الشركات المشارِكة "ستستخدم وسائل الحماية فيما يتعلق بالمعلومات الشخصية" و"ستحترم حقوق الخصوصية للمستخدمين وتعمل على حمايتها عند مواجهة مطالب أو قوانين أو أنظمة حكومية تؤثر على الخصوصية بطريقة لا تتوافق مع القوانين والمعايير المعترف بها دولياً".

٤٩- ويُجري مؤشر مساءلة الشركات لترتيب الحقوق الرقمية تقييماً لعدد من شركات الإنترنت والهاتف الجوال والاتصالات، على وجه التحديد، بشأن التزاماتها وسياساتها المعلنة التي تؤثر على حرية التعبير والخصوصية[٦٥]. ويمكن أن يتيح ذلك أداة مفيدة لمساءلة الشركات عن تأثيرها على حقوق المستخدمين.

سادساً- سبل الانتصاف

٥٠- يجب أن تتاح لضحايا الانتهاكات أو التجاوزات المتعلقة بالخصوصية التي ترتكبها الدول و/أو مؤسسات الأعمال سبل انتصاف فعالة. ولا يقع على عاتق الدول الوفاء بالالتزامات بكفالة المساءلة والانتصاف في أعقاب انتهاكاتِ حقوق الإنسان التي ترتكبها الجهات الحكومية فحسب، بل يجب عليها أيضاً أن تتخذ الخطوات المناسبة لكفالة حصول ضحايا انتهاكات حقوق الإنسان المرتبطة بالأعمال التجارية على سبل انتصاف فعالة (انظر الركيزة الثالثة من المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان). وتبعاً لطبيعة قضية أو حالة معينة، ينبغي أن يكون الضحايا قادرين على تحقيق الانتصاف من خلال آليات التظلم الفعَّالة القضائية أو غير القضائية القائمة على مستوى الدولة (A/HRC/32/19 وCorr.1 وAdd.1 وA/HRC/38/20 وAdd.1). وتشمل الآليات غير القضائية ذات الصلة على مستوى الدولة، في سياق تكنولوجيا المعلومات والاتصالات، الهيئاتِ المستقلة التي لديها صلاحيات لمراقبة ممارسات الدولة والقطاع الخاص فيما يتعلق بخصوصية البيانات، من قبيل هيئات حماية الخصوصية والبيانات.

٥١- وفي إطار المبادئ التوجيهية أيضاً، ينبغي لمؤسسات الأعمال متى رأت أنها تسببت في آثار ضارة بحقوق الإنسان أو أسهمت في ذلك، أن توفر الانتصاف من أي آثار ضارة بحقوق الإنسان قد تكون تسببت فيها أو أسهمت في ذلك، أو أن تتعاون مع الجهات الأخرى من أجل توفير الانتصاف عن طريق عمليات مشروعة[٦٦]. ولكي يمكن اعتبار أي آلية غير قضائية

(٦٣) متاحة على: https://globalnetworkinitiative.org/gni-principles/. انظر أيضاً المعلومات المقدمة من مبادرة الشبكة العالمية (Global Network Initiative) لإدراجها في هذا التقرير.

(٦٤) متاحة على: www.telecomindustrydialogue.org/about/guiding-principles/.

(٦٥) انظر: https://rankingdigitalrights.org/index2018/.

(٦٦) المبدأ التوجيهي ٢٢.

من الآليات الفعالة، ينبغي أن تكون مشروعة، ومتيسِّرة، وذات طرائق عمل متوقعة، ومنصفة، ومتوافقة مع الحقوق، وشفافة، ومصدراً للتعلم المستمر، وقائمة على أساس الحوار والمشاركة متى تعلق الأمر بآليات التظلم على المستوى التنفيذي[٦٧].

٥٢- وفي الحالات التي لا تسبب المؤسسة أثراً ضاراً ولا تسهم في حدوثه، إنما يكون الأثر مرتبطاً على نحو مباشر بعملياتها أو منتجاتها أو خدماتها عن طريق علاقة عمل، فإن الإجراء الملائم الذي ينبغي اتخاذه يرد بالتفصيل في المبدأ التوجيهي ١٩. وقد يشمل استغلال أي نفوذ يسع للمؤسسة أن تمارسه إزاء شريك أعمالها أو عميلها من أجل التأثير عليه وتوفير الانتصاف[٦٨].

٥٣- وتسلط المبادئ التوجيهية الضوء أيضاً على الدور الذي يمكن أن تؤديه آليات التظلم على المستوى التنفيذي في معالجة المظالم مباشرةً. ويمكن أن تتخذ هذه الآليات مجموعة من الأشكال، وهذا يعتمد على نوع الشركة المعنية، واحتياجات أصحاب المصلحة فيها، وصورة الشركة فيما يتعلق بالمخاطر التي تسببها في مجال حقوق الإنسان. ومن أجل تحديد سبل تصميم تلك الآليات والأخذ بها في قطاع تكنولوجيا المعلومات والاتصالات من الناحية العملية، لا بد من إجراء المزيد من المناقشات داخل القطاع ومع أصحاب المصلحة.

٥٤- لكن في الممارسة العملية، توجد ثغرات وعقبات كبيرة أمام إتاحة سبل الانتصاف من انتهاكات الخصوصية. إذ يطرح الطابع عبر الوطني لعمليات المراقبة واعتراض الاتصالات، والآثار المترتبة عليها، والأشكال العديدة لمعالجة البيانات الشخصية، تحدياتٍ قانونية وعملية (انظر A/HRC/34/60، الفقرة ٣٤). وبالإضافة إلى ذلك، يشكل عدم معرفة الضحايا بحدوث تدخلات غير مبررة إزاءهم وافتقارهم إلى دليل بهذا الشأن، عقبة متكررة أمام الوصول إلى سبل الانتصاف (انظر A/HRC/27/37، الفقرة ٤٠). فعلى سبيل المثال، كثيراً ما تكون طلبات الدول للحصول على البيانات التي تحتفظ بها الشركات مصحوبة "بأوامر تقييدية" تمنع الشركات من إخطار الأفراد المعنيين. وكثيراً ما تمتنع الدول أيضاً عن إخطار المتأثرين بتدابير المراقبة الأخرى، ولا سيما في حالات المراقبة على نطاق واسع. ومع التسليم بأن الإخطار المسبق أو المتزامن مع العملية قد يعرض فعالية تدابير المراقبة المشروعة للخطر، ينبغي مع ذلك إخطار الأفراد المعنيين بمجرد الانتهاء من العملية المنفذة بشأنهم (انظر A/HRC/23/40، الفقرة ٨٢). وإذا لم يكن ذلك ممكناً، ينبغي أن يمنح القانون الأهلية بسهولة للأشخاص المتأثرين نظرياً بتلك التدابير (انظر A/HRC/13/37، الفقرة ٣٨). وبالمثل، ينبغي لمؤسسات الأعمال أن تُخطر عملاءها بمجرد علمها بوقوع انتهاكات للبيانات الشخصية قد تؤثر على حقوقهم.

٥٥- وتواجه الضحايا أيضاً تحديات جديدة ومتزايدة في سياق اتخاذ القرارات بناءً على الحسابات الخوارزمية، حيث قد لا يتمكن الأفراد من الحصول على البيانات المدخلة، أو من الطعن في النتائج التي توصلت إليها الحسابات الخوارزمية، أو من معرفة الكيفية التي تم بها

(٦٧) المبدأ التوجيهي ٣١.

(٦٨) المبدأ التوجيهي ١٩ وشرحه. انظر أيضاً: OHCHR, “The corporate responsibility to respect human rights: an interpretive guide”, pp. 48–52.

استخدام هذه النتائج من أجل اتخاذ القرارات[٦٩]. وينبغي أن تنظر الدول ومؤسسات الأعمال، بالتعاون مع أصحاب المصلحة الآخرين، في الآليات الممكنة لمعالجة هذه المسألة، من قبيل إنشاء هيئات تدقيق الخبراء المزودة بالموارد الكافية.

٥٦- وتشكل طبيعة الضرر الناجم عن انتهاكات الخصوصية مصدر تحديات أخرى. إذ من الصعب إعادة الأمور إلى نصابها على إثر وقوع انتهاكات متعلقة بالخصوصية، وقد يؤدي ذلك إلى بروز عواقب مستمرة وإلى آثار أخرى على صعيد حقوق الإنسان ككل. ذلك أن سهولة الاحتفاظ بالبيانات وموجز المعلومات، وتبادلها، وإعادة توظيفها لأغراض أخرى، ودمجها، كلها عوامل تؤثر على ديمومة البيانات الرقمية، وتعني أن الفرد قد يواجه مخاطر جديدة ومستمرة على حقوقه في المستقبل[٧٠].

٥٧- وتؤثر الأضرار التي تلحق بالخصوصية إلى حد كبير على حياة الشخص، حتى عندما لا يكون الأثرُ الاقتصادي أو أي أثر آخر قابلاً للقياس الكمي؛ لكن ينبغي ألا تمنع طبيعة الضرر الناجم الضحايا من التماس الانتصاف. وعلى سبيل المثال، يسع تمكين منظمات حماية المستهلك من المطالبة بالتعويض باسم ضحايا الانتهاكات التي ترتكبها الشركات في مجال الخصوصية.

سابعاً- استنتاجات وتوصيات

٥٨- يوفر الإطار الدولي لحقوق الإنسان أساساً متيناً من أجل وضع الاستجابات للتحديات المتعددة الناشئة في العصر الرقمي. وثمة حاجة ملحة لأن تفي الدول تماماً بالتزاماتها باحترام الحق في الخصوصية، وكذلك بواجبها في حماية الحق في الخصوصية، بما في ذلك إزاء الانتهاكات التي ترتكبها الشركات. وتحقيقاً لهذه الغاية، يتعين على الدول وضع الإطار القانوني والسياساتي المناسب، بما يشمل التشريعات والأنظمة الملائمة لحماية الخصوصية، بما في ذلك مبادئ المشروعية والتناسب والضرورة، فضلاً عن إقامة الضمانات والرقابة وإتاحة سبل الانتصاف.

٥٩- ويتطلب العديد من المسائل التي لم يمكن تناولها في هذا التقرير المزيد من البحث المتعمق، بما في ذلك العلاقة بين الحق في الخصوصية وحقوق الإنسان الأخرى، وبما يشمل الحقوق الاقتصادية والاجتماعية والثقافية؛ والآثار غير التناسبية أو التمييزية الناجمة عن التدخل في الخصوصية إزاء الأفراد و/أو الفئات المعرضة للخطر؛ والآثار الناجمة عن البيانات الضخمة والتعلم الآلي، بما في ذلك لغرض التنبؤ والوقاية، على التمتع بالحق في الخصوصية وحقوق الإنسان الأخرى؛ وتنظيم أسواق تكنولوجيات المراقبة.

٦٠- وتشكل طبيعة وأشكال سبل الانتصاف التي تستجيب على نحو فعال لحالات انتهاك الحق في الخصوصية مجالاً آخر يتطلب المزيد من الاهتمام. وكخطوة أولى، ينبغي إجراء تحديد منهجي لأنواع التدابير التصحيحية التي ستكون ملائمة في حالات مختلفة.

(٦٩) انظر المعلومات المقدمة من University of Essex Human Rights, Big Data and Technology Project، الفقرة ٣٣.

(٧٠) المرجع نفسه، الفقرة ٧.

ويمكن استخدام ذلك في وضع المزيد من التوجيهات. وعند إجراء التحليل، ينبغي إيلاء الاعتبار الواجب للتوجيهات والتوصيات التي وُضعت عن طريق مشروع المساءلة والانتصاف التابع لمفوضية الأمم المتحدة لحقوق الإنسان. وبوجه أعم، ينبغي بذل جهود لوضع أدوات توجيهية محددةِ القطاع بشأن مسؤوليات مؤسسات الأعمال عن احترام الحق في الخصوصية.

٦١- ويوصي المفوض السامي بأن تقوم الدول بما يلي:

(أ) الاعتراف بالتبعات الكاملة الناجمة عن التكنولوجيات الجديدة، ولا سيما التكنولوجيات المستنِدة إلى البيانات، إزاء الحق في الخصوصية وجميع حقوق الإنسان الأخرى؛

(ب) اعتماد تشريعات قوية الأثر ومُحكمة وشاملة في مجال الخصوصية، بما في ذلك بشأن خصوصية البيانات، وبما يمتثل للقانون الدولي لحقوق الإنسان من حيث الضمانات والرقابة وسبل الانتصاف من أجل حماية الحق في الخصوصية على نحو فعال؛

(ج) كفالة عدم نشر النُظم القائمة على الاستخدام الكثيف للبيانات، بما في ذلك النُظم التي تشمل جمع البيانات البيومترية والاحتفاظ بها، إلا عندما يمكن للدول أن تُبيِّن أنها ضرورية وتناسبية لتحقيق هدف مشروع؛

(د) إنشاء هيئات مستقلة وتزويدها بالصلاحيات اللازمة لمراقبة ممارسات الدولة والقطاع الخاص فيما يتعلق بخصوصية البيانات، والتحقيق في الانتهاكات، وتلقي الشكاوى من الأفراد والمنظمات، وإصدار غرامات وعقوبات فعالة أخرى على معالجة البيانات الشخصية بشكل غير قانوني من جانب الهيئات العامة والخاصة؛

(هـ) سنّ التشريعات المناسبة واللجوء إلى الوسائل الأخرى المتاحة لكفالة امتثال أي تدخل في الحق في الخصوصية، بما في ذلك عن طريق مراقبة الاتصالات وتبادل المعلومات الاستخبارية، لأحكام القانون الدولي لحقوق الإنسان، بما يشمل مبادئ المشروعية والضرورة والتناسب، وتحقيق هدف مشروع، وبصرف النظر عن جنسية الأفراد المتضررين أو مكان وجودهم، والتوضيح بأن منح الإذن باتخاذ تدابير المراقبة يتطلب وجود سبب كافٍ يدعو إلى الافتراض أن فرداً معيناً قد ارتكب أو أنه يرتكب جرماً، أو أنه يشارك في أعمال يمكن اعتبارها تهديداً محدداً للأمن القومي؛

(و) تعزيز الآليات المستقلة لإصدار الإذن بممارسة أنشطة المراقبة من جانب الدولة وتطبيق رقابة على تلك الأنشطة، وكفالة أن تكون تلك الآليات مختصة ومجهزة بموارد كافية لرصد وإنفاذ مشروعية تدابير المراقبة وضرورتها وتناسبها؛

(ز) استعراض القوانين لكفالة أنها لا تفرض شرط الاحتفاظ الشامل والعشوائي ببيانات الاتصالات على شركات الاتصالات وغيرها من الشركات؛

(ح) اتخاذ خطوات من أجل تعزيز الشفافية والمساءلة في اقتناء الدول لتكنولوجيات المراقبة؛

(ط) تنفيذ الواجبات الواقعة على عاتق الدول بالكامل للحماية من انتهاكات الحق في الخصوصية من جانب مؤسسات الأعمال في جميع القطاعات ذات الصلة، بما في

ذلك قطاع تكنولوجيا المعلومات والاتصالات، عن طريق اتخاذ الخطوات المناسبة لمنع هذه الانتهاكات والتحقيق فيها والمعاقبة عليها والانتصاف منها باعتماد السياسات والتشريعات والأنظمة والأحكام القضائية الفعالة؛

(ي) كفالة حصول جميع ضحايا الانتهاكات والتجاوزات للحق في الخصوصية على سبل انتصاف فعالة، بما في ذلك في القضايا العابرة للحدود.

٦٢- ويوصي المفوض السامي بأن تقوم مؤسسات الأعمال بما يلي:

(أ) بذل كل الجهود الممكنة للوفاء بمسؤوليتها عن احترام الحق في الخصوصية وجميع حقوق الإنسان الأخرى. وكحد أدنى، ينبغي أن تعمل مؤسسات الأعمال على تنفيذ المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان تنفيذاً كاملاً، مما ينطوي على بذل العناية الواجبة في مراعاة حقوق الإنسان على نحو فعال في جميع عملياتها وفيما يتعلق بجميع حقوق الإنسان، بما في ذلك الحق في الخصوصية، واتخاذ الإجراءات المناسبة لمنع الآثار ذات الصلة سواء كانت فعلية أو محتملة، والتخفيف منها ومعالجتها؛

(ب) السعي إلى كفالة مستوى عالٍ من الأمان والسرية لأي اتصالات تقوم مؤسسات الأعمال بإحالتها ولأي بيانات شخصية تقوم بجمعها أو تخزينها أو معالجتها بطريقة أخرى. وإجراء تقييمات بشأن أفضل السبل المتاحة لتصميم وتحديث أمن المنتجات والخدمات على أساس مستمر؛

(ج) الامتثال لمبادئ الخصوصية الرئيسية المشار إليها في الفقرات من ٢٩ إلى ٣١ من هذا التقرير وكفالة أكبر قدر ممكن من الشفافية في سياساتها وممارساتها الداخلية التي تؤثر على الحق في خصوصية مستخدميها وعملائها؛

(د) إتاحة الانتصاف عن طريق عمليات مشروعة، أو التعاون مع الجهات الأخرى من أجل إتاحة الانتصاف، عندما تتسبب مؤسسات الأعمال في آثار ضارة أو تسهم في حدوثها، بما في ذلك من خلال آليات فعالة للتظلم على المستوى التنفيذي؛

(هـ) الإسهام في عمل مشروع المساءلة والانتصاف التابع لمفوضية الأمم المتحدة السامية لحقوق الإنسان، الهادف إلى وضع توجيهات وتوصيات لتعزيز فعالية آليات التظلم غير التابعة للدولة فيما يتعلق بانتهاكات الحق في الخصوصية في الفضاء الرقمي.