الأمم المتحدة

A/HRC/23/40

الجمعية العامة

Distr.: General
17 April 2013
Arabic
Original: English

مجلس حقوق الإنسان

الدورة الثالثة والعشرون

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، فرانك لا رو*

موجز

يتناول هذا التقرير، المقدم وفقاً لقرار مجلس حقوق الإنسان ١٦/٤، بالتحليل تداعيات مراقبة الدول للاتصالات على ممارسة حقوق الإنسان في الخصوصية وفي حرية الرأي والتعبير. ويشدد التقرير، في معرض بحث أثر التطورات التكنولوجية الهامة التي حدثت في مجال الاتصالات، على الحاجة الملحة إلى تناول الطرائق الجديدة المتبعة في المراقبة بمزيد من الدراسة، وإلى تنقيح القوانين الوطنية التي تنظم هذه الممارسات بما يتماشى مع معايير حقوق الإنسان.

* تأخر تقديم هذه الوثيقة.

الرجاء إعادة الاستعمال

المحتويات

		الفقرات	الصفحة
أولاً –	مقدمة	١-٦	٣
ثانياً –	أنشطة المقرر الخاص	٧-١٠	٤
ثالثاً –	تطور تكنولوجيا المراقبة	١١-١٨	٥
رابعاً –	الإطار الدولي لحقوق الإنسان	١٩-٣٢	٧
	ألف– أوجه الترابط بين الحق في الخصوصية والحق في حرية الرأي والتعبير	٢٤-٢٧	٨
	باء – القيود التي يجوز فرضها على الخصوصية وحرية التعبير	٢٨-٢٩	١٠
	جيم– الاستعراضات الأخيرة التي أجرتها الآليات الدولية لحماية حقوق الإنسان	٣٠-٣٢	١١
خامساً –	طرائق مراقبة الاتصالات	٣٣-٤٩	١٢
	ألف– مراقبة محددة الهدف للاتصالات	٣٤-٣٧	١٢
	باء – مراقبة وسائل الاتصال الجماهيري	٣٨-٤٠	١٤
	جيم– إمكانية الاطلاع على بيانات الاتصال	٤١-٤٣	١٥
	دال – ترشيح الإنترنت ورقابتها	٤٤-٤٦	١٦
	هاء – القيود المفروضة على إغفال الهوية	٤٧-٤٩	١٦
سادساً –	الشواغل المتعلقة بالمعايير القانونية الوطنية	٥٠-٧١	١٧
	ألف– انعدام الرقابة الفضائية	٥٤-٥٧	١٨
	باء – الاستثناءات المتعلقة بالأمن القومي	٥٨-٦٠	٢٠
	جيم– الاطلاع غير المنظم على محتوى بيانات الاتصالات	٦١	٢٠
	دال – المراقبة القانونية الإضافية	٦٢-٦٣	٢١
	هاء – تطبيق قوانين المراقبة خارج الإقليم	٦٤	٢٢
	واو – الاحتفاظ الإلزامي بالبيانات	٦٥-٦٧	٢٣
	زاي– قوانين الكشف عن الهوية	٦٨-٧٠	٢٣
	حاء– القيود المفروضة على التشفير وقوانين الكشف عن مفتاح التشفير	٧١	٢٥
سابعاً –	دور القطاع الخاص ومسؤولياته	٧٢-٧٧	٢٥
ثامناً –	الاستنتاجات والتوصيات	٧٨-٩٩	٢٧
	ألف– تحديث القانون والمعايير القانونية وتعزيزها	٨١-٨٧	٢٧
	باء – تيسير الاتصالات الخاصة والمؤمَّنة والمجهولة الهوية	٨٨-٩٠	٢٨
	جيم– زيادة إمكانية اطلاع الجمهور على المعلومات وفهم التهديدات للخصوصية والتوعية بها	٩١-٩٤	٢٩
	دال – تنظيم الاتجار بتكنولوجيا المراقبة	٩٥-٩٧	٢٩
	هاء – تعزيز تقييم الالتزامات الدولية ذات الصلة في مجال حقوق الإنسان	٩٨-٩٩	٣٠

أولاً- مقدمة

١- يحلل هذا التقرير تداعيات مراقبة الدول للاتصالات على ممارسة حقوق الإنسان في الخصوصية وفي حرية الرأي والتعبير. ويشدد التقرير، في معرض بحث أثر التطورات التكنولوجية الهامة التي حدثت في مجال الاتصالات، على الحاجة الملحة إلى تناول الطرائق الجديدة المتبعة في المراقبة بمزيد من الدراسة، وإلى تنقيح القوانين الوطنية التي تنظم هذه الممارسات بما يتماشى مع معايير حقوق الإنسان.

٢- لقد زادت الابتكارات التكنولوجية من إمكانيات التواصل وحماية حرية التعبير والرأي، فأتاحت إغفال الهوية والتبادل السريع للمعلومات والحوار بين الثقافات. وفي الوقت نفسه، زادت التغيرات التكنولوجية من فرص الدولة في مراقبة الاتصالات الخاصة بالأفراد والتدخل فيها.

٣- وقد تصلح الشواغل المتعلقة بالأمن القومي والنشاط الإجرامي مبرراً لاستخدام تكنولوجيات مراقبة الاتصالات بصورة استثنائية. غير أن القوانين الوطنية التي تنظم ما يمكن أن يشكل تدخلاً ضرورياً ومشروعاً ومتناسباً من الدولة في مراقبة الاتصالات هي إما قاصرة أو منعدمة في أغلب الأحيان. وقصور الأطر القانونية الوطنية يوفر مرتعا لارتكاب انتهاكات تعسفية ومخالفات يعاقب عليها القانون تطال الحق في خصوصية الاتصالات، وبذلك، يهدد أيضا حماية الحق في حرية الرأي والتعبير.

٤- وقد حلل المقرر الخاص في التقريرين السابقين (A/HRC/17/27 وA/66/290)، أثر الإنترنت غير المسبوق على زيادة إمكانيات ممارسة الفرد لحقه في حرية الرأي والتعبير. وأعرب عن قلقه إزاء اتخاذ الدول تدابير متعددة لمنع انسياب المعلومات عبر شبكة الإنترنت أو تقييده، وسلط الضوء على التقصير الحاصل في مجال حماية الحق في الخصوصية على الإنترنت.

٥- وينطلق هذا التقرير من التحليل السابق بهدف تحديد مخاطر الوسائل والطرائق الجديدة المعتمدة في مراقبة الاتصالات على حقوق الإنسان، بما في ذلك الحق في الخصوصية وحرية الرأي والتعبير.

٦- ويستخدم التقرير المصطلحات التالية لوصف طرائق مراقبة الاتصالات الأكثر شيوعاً:

(أ) مراقبة الاتصالات: رصد المعلومات التي تم إيصالها أو نقلها أو توليدها عبر شبكات الاتصالات، واعتراض هذه المعلومات وجمعها وحفظها واستبقاؤها؛

(ب) بيانات الاتصال: المعلومات المتعلقة باتصالات الأفراد (رسائل البريد الإلكتروني، والمكالمات الهاتفية، والرسائل النصية المرسلة والواردة، والرسائل والمشاركات المبثوثة على شبكات التواصل الاجتماعي)، والهوية، وحسابات الربط الشبكي، والعناوين،

والمواقع التي جرى تصفحها، والكتب وغيرها من المواد المقروءة والمسموعة والمشاهدة، وعمليات البحث التي أجريت والمصادر التي استخدمت، والتفاعلات (مصدر الاتصال ووجهته، والأشخاص الذين تم التفاعل معهم، والأصدقاء والأقارب والمعارف)، والمواقيت وأماكن تواجد الشخص، بما في ذلك مدى قربه من الآخرين؛

(ج) ترشيح الإنترنت: الرصد الآلي أو اليدوي لمحتوى الإنترنت (بما في ذلك المواقع الشبكية، والمدونات ومصادر الإعلام الإلكتروني، وكذلك البريد الإلكتروني) من أجل تقييد أو خطر الوصول إلى نصوص أو صور أو مواقع شبكية أو شبكات أو بروتوكولات شبكية أو خدمات أو أنشطة بعينها.

ثانياً- أنشطة المقرر الخاص

٧- شارك المقرر الخاص، خلال الفترة المشمولة بالتقرير، في مناسبات دولية ووطنية متعددة لها صلة بالقضايا التي تناولها في تقاريره السابقة مثل حرية التعبير على الإنترنت، ومنع خطاب الكراهية، وحماية الصحفيين. وقد أولى اهتماماً خاصاً للمبادرات الوطنية الرامية إلى تعزيز حماية الصحفيين؛ وشارك بهذا الخصوص في اجتماعات تتعلق بالمبادرات التي وضعتها كل من البرازيل وكولومبيا وهندوراس والمكسيك. وشارك أيضا في "اجتماع الأمم المتحدة المشترك بين الوكالات بشأن سلامة الصحفيين ومسألة الإفلات من العقاب"، الذي عقد في تشرين الثاني/نوفمبر ٢٠١٢ في فيينا.

٨- وركز في تقريره الأخير المقدم إلى الجمعية العامة للأمم المتحدة على منع خطاب الكراهية ومنع التحريض عليها[١]. وعولج نفس الموضوع في نشاط اشترك في تنظيمه المقرر الخاص والمستشار الخاص المعني بمنع الإبادة الجماعية على هامش انعقاد الجمعية العامة في شباط/فبراير ٢٠١٣. وفي الشهر نفسه، عاود تناول هاتين المسألتين بمناسبة إطلاق "خطة عمل الرباط بشأن حظر الدعوة إلى الكراهية القومية أو العنصرية أو الدينية التي تشكل تحريضاً على التمييز أو العداء أو العنف" في جنيف، وأثناء انعقاد منتدى الأمم المتحدة العالمي الخامس لتحالف الحضارات، في فيينا.

٩- وقام المقرر الخاص ببعثة إلى هندوراس في الفترة من ٧ إلى ١٤ آب/أغسطس ٢٠١٢. ويمكن الاطلاع على أهم ما توصل إليه من استنتاجات وقدمه من توصيات بشأن هذه الزيارة في الإضافة المرفقة بهذا التقرير (A/HRC/20/40/Add.1). وتلقى دعوة من الحكومة الإندونيسية لزيارة البلاد في كانون الثاني/يناير ٢٠١٣. لكن الحكومة طلبت تأجيل الزيارة للأسف، ولم يتم حتى الآن تأكيد موعد الزيارة الجديد.

---

(١) A/67/357.

١٠- وعمد المقرر الخاص في إعداد هذا التقرير إلى مراجعة الدراسات ذات الصلة والتشاور مع خبراء في المسائل المتعلقة بمراقبة الاتصالات. وفي كانون الأول/ديسمبر ٢٠١٢، شارك في حلقة عمل نظمتها مؤسسة الحدود الإلكترونية بشأن موضوع المراقبة الإلكترونية وحقوق الإنسان. وفي شهر شباط/فبراير عام ٢٠١٣، نظم مشاورة خبراء لإعداد هذا التقرير، وتزامن عقد المشاورة مع أنشطة "اجتماع القمة العالمية لمجتمع المعلومات +١٠" الذي عقد في مقر منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) بباريس، حيث شارك أيضاً في المناقشة العامة التي جرت في الجلسة العامة الافتتاحية.

ثالثاً- تطور تكنولوجيا المراقبة

١١- سمحت الابتكارات التكنولوجية بزيادة فرص التواصل وحرية التعبير، فأتاحت إغفال الهوية، والتبادل السريع للمعلومات، والحوار بين الثقافات. وفي الوقت عينه، خلقت التغيرات التي طرأت في مجال التكنولوجيا أيضاً فرصاً جديدة لتمارس الدولة الرقابة على الحياة الخاصة للأفراد والتدخل فيها.

١٢- وقد سعت الدول منذ بداية ظهور أول شكل من أشكال الاتصال عن بعد، إلى اعتراض الاتصالات الخاصة للأفراد ومراقبتها لخدمة إنفاذ القانون ومصالح الأمن القومي. فمن خلال الاتصالات يمكن كشف معلومات شخصية جداً وفي غاية الخصوصية، بما في ذلك المعلومات المتعلقة بالأنشطة التي قام بها في الماضي أو سيقوم بها في المستقبل فرد أو جماعة ما. وتمثل الاتصالات مصدراً قيما لاستقاء الأدلة التي قد تستند إليها الدولة لمنع الجرائم الخطيرة أو ملاحقة مرتكبيها أو لاستباق حالات الطوارئ التي قد تهدد الأمن القومي.

١٣- وقد أحدثت الابتكارات التكنولوجية طوال القرن العشرين تغييراً في طبيعة مراقبة الاتصالات وآثارها. فطرأت طفرة على الوسائل التي تتيح للناس التواصل فيما بينهم وعلى وتيرة هذا التواصل. وأدى التحول من نظم خطوط الهاتف الثابتة إلى الاتصالات السلكية واللاسلكية المتنقلة وتراجع تكاليف خدمات الاتصالات إلى الإقبال بقوة على استخدام الهاتف. وظهرت مع ظهور الإنترنت أدوات وتطبيقات جديدة تتيح الاتصال مجاناً، أو بمقابل معقول جداً. وزادت هذه التطورات من القدرة على الاتصال ويسَّرت انسياب المعلومات والأفكار على نطاق العالم، وتنامت بفضلها فرص تحقيق النمو الاقتصادي والتغيير في المجتمعات.

١٤- وتطورت تكنولوجيا المعلومات والاتصالات مثلما تطورت الوسائل التي تسعى الدول من خلالها إلى رصد الاتصالات الخاصة. ومع زيادة الإقبال على استخدام الهواتف ظهر التنصت على المكالمات الهاتفية من خلال تثبيت جهاز لاستراق السمع في أسلاك الهاتف بهدف التنصت على المكالمات الهاتفية الخاصة. وعندما استعيض عن أنظمة الهاتف التناظرية

بالألياف الضوئية ومفاتيح التحويل الرقمي في التسعينيات، أعادت الدول تصميم تكنولوجيا الربط الشبكي لتشمل القدرة على الاعتراض ("الأبواب الخلفية") لكي يتسنى للدولة القيام بالمراقبة، وهو ما أتاح إمكانية النفاذ إلى الشبكات الهاتفية الحديثة والتحكم فيها عن بعد.

١٥- وقد أدى الطابع الديناميكي للتكنولوجيا إلى تغيير الأسلوب المعتمد في المراقبة فضلاً عن تغيير "المادة" القابلة للرصد. وبفضل شبكة الإنترنت التي أتاحت فرصاً شتى للاتصال وتبادل المعلومات، بات من اليسير إعداد كميات كبيرة من بيانات المعاملات التي يقدمها الأفراد أو التي تتعلق بهم. وتشمل هذه المعلومات التي تعرف باسم بيانات الاتصال أو البيانات الفوقية المعلومات الشخصية عن الأفراد ومكان وجودهم ونشاطهم على شبكة الإنترنت، والسجلات وما يتصل بها من معلومات تتعلق بالبريد الإلكتروني ورسائلهم الواردة والصادرة. ويمكن تخزين بيانات الاتصال والاطلاع عليها والبحث فيها، وهناك نقص كبير في الضوابط التي تنظم كشفها للسلطات الحكومية واستخدام هذه السلطات لها. ويمكن لتحليل هذه البيانات أن يكون كاشفاً عن الكثير من المعلومات واقتحامياً في آن معاً، لا سيما عندما يتم تجميع البيانات ومراكمتها. ولذلك تعتمد الدول أكثر فأكثر على بيانات الاتصال في دعم إنفاذ القانون أو التحقيقات المتعلقة بالأمن القومي. كما تفرض الدول حفظ بيانات الاتصال واستبقاءها ليتسنى لها المراقبة استناداً إلى بيانات سابقة.

١٦- وواكبت التغييرات التكنولوجية تغييرات في المواقف من مراقبة الاتصالات. فعندما شُرع في التنصت على المكالمات الهاتفية بشكل رسمي في الولايات المتحدة الأمريكية لأول مرة، كان نطاقه محدودا، ولم يؤيده القضاء إلا على مضض[٢]. واعتُبر الأمر تهديداً للحق في الخصوصية يبلغ من الخطورة ما يستدعي حصره في نطاق الكشف عن أخطر الجرائم وملاحقة مرتكبيها. غير أن الدول عملت مع مرور الزمن، على توسيع نطاق صلاحيات المراقبة المخولة لها، فوضعت معايير أقل صرامة وأكثرت من المبررات التي تسوغ هذه المراقبة.

١٧- ولم تخضع التشريعات السارية والممارسات المتبعة في كثير من البلدان للتنقيح والتحديث من أجل التصدي للتهديدات والتحديات التي ظهرت في مجال مراقبة الاتصالات في العصر الرقمي. فقد اقتبست القوانين التي تجيز النفاذ إلى الحواسيب الشخصية وغيرها من تكنولوجيات المعلومات والاتصالات، دون مراعاة لاتساع نطاق استخدام هذه الأجهزة وآثار ذلك على حقوق الأفراد، مفاهيم تقليدية تتعلق بالاطلاع على المراسلات الخطية، على

(٢) عندما صدق القضاء على التنصت على المكالمات الهاتفية للمرة الأولى، كتب المستشار القضائي في المحكمة العليا للولايات المتحدة السيد برانديز رأياً مخالفاً ينتقد بشدة ممارسة التنصت على المكالمات الهاتفية فقال: إن التنصت هو "من أكثر الوسائل دهاء وأبعدها أثراً لانتهاك الخصوصية" ولا يمكن تبريرها بموجب الدستور. وكانت توقعات هذا الفقيه القانوني البارز مذهلة في دقتها، إذ قال: "يمكن أن تُطوَّر يوما ما أساليب تمكِّن الحكومة من نسخ وثائق وعرضها على المحكمة دون أخذها من أدراج سرية، وتمكنها من إطلاع المحلفين على أكثر التفاصيل خصوصية في البيوت. وقد يحرز علم النفس وما يتصل به من علوم تقدماً يتيح سبر القناعات والأفكار والانفعالات المكتومة". *أولمستيد ضد الولايات المتحدة*، 277 U.S. 438 (1928).

سبيل المثال. وفي الوقت نفسه، أدى عدم وجود قوانين تنظم مراقبة الاتصالات العالمية وترتيبات لتقاسم المعلومات إلى ظهور ممارسات مرتجلة تتخطى نطاق الإشراف من أي هيئة مستقلة. فقد بات بمقدور مجموعة واسعة من الهيئات العامة في كثير من الدول، الاطلاع على بيانات الاتصال لأغراض شتى. وغالباً ما يحدث ذلك دون الحصول على إذن قضائي ودون إشراف جهة مستقلة. وبالإضافة إلى ذلك، تسعى الدول إلى اعتماد ترتيبات للمراقبة يمكن أن يمتد أثرها إلى خارج أراضيها.

١٨- كذلك تراخت آليات حقوق الإنسان عن تقييم تداعيات الإنترنت والمستجدات التكنولوجية في عالم مراقبة الاتصالات والنفاذ إلى بيانات الاتصال على حقوق الإنسان. ولم يجر مجلس حقوق الإنسان والمكلفون بولايات في إطار الإجراءات الخاصة وهيئات معاهدات حقوق الإنسان حتى الآن دراسة شاملة لعواقب توسيع صلاحيات المراقبة المخولة للدول وممارساتها على الحق في الخصوصية والحق في حرية الرأي والتعبير، وعلى ترابط هذين الحقين. ويسعى هذا التقرير إلى تدارك هذا الأمر.

رابعاً- الإطار الدولي لحقوق الإنسان

١٩- إن الحق في حرية الرأي والتعبير مكفول بموجب المادة ١٩ في كل من الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية، إذ تؤكد هاتان المادتان حق كل إنسان في اعتناق آراء دون مضايقة، وفي التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين بأية وسيلة ودونما اعتبار للحدود. وعلى المستوى الإقليمي، ينص كل من الميثاق الأفريقي لحقوق الإنسان والشعوب (المادة ٩)، والاتفاقية الأمريكية لحقوق الإنسان (المادة ١٣) واتفاقية حماية حقوق الإنسان والحريات الأساسية (المادة ١٠) على حماية هذا الحق.

٢٠- وهناك أيضاً اعتراف لا لبس فيه على الصعيدين الدولي والإقليمي، بأن الخصوصية حق أساسي من حقوق الإنسان. والحق في الخصوصية كرسه الإعلان العالمي لحقوق الإنسان (المادة ١٢)، والعهد الدولي الخاص بالحقوق المدنية والسياسية (المادة ١٧)، واتفاقية حقوق الطفل (المادة ١٦)، والاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم (المادة ١٤). وعلى المستوى الإقليمي، تنص الاتفاقية الأوروبية لحقوق الإنسان (المادة ٨)، والاتفاقية الأمريكية لحقوق الإنسان (المادة ١١) على حماية الحق في الخصوصية.

٢١- ورغم الاعتراف الواسع النطاق بوجود التزام يقضي بحماية الخصوصية، فإن الآليات الدولية المعنية بحماية حقوق الإنسان لم تعمد لدى إدراج هذا الحق في صكوك حقوق الإنسان الآنفة الذكر، إلى توضيح تفاصيل مضمون هذا الحق على وجه التحديد. وقد ساهم

عدم صياغة مضمونه صياغة واضحة في الصعوبات المتعلقة بتطبيقه وإنفاذه[٣]. وبما أن الحق في الخصوصية هو حق مشروط، فإن تفسيره ينطوي على صعوبات تتعلق بتحديد نطاق الحيز الخاص وبإرساء مفهوم الصالح العام. كما أن التغيرات المتسارعة والهائلة التي طرأت في مجال الاتصالات وتكنولوجيا المعلومات خلال العقود الأخيرة خلفت أثرا دائما على فهمنا للحدود الفاصلة بين الحيز الخاص والحيز العام.

٢٢- ويمكن تعريف الخصوصية على أنها افتراض وجود ضرورة لأن يتوفر للفرد مجال للنماء والتفاعل والحرية في استقلالية، وهو "حيز خاص" يتفاعل فيه مع الآخرين أو لا يتفاعل معهم بعيداً عن تدخل الدولة وعن التطفل المتمادى فيه من الأشخاص غير المرغوب فيهم[٤]. والحق في الخصوصية يعني أيضاً قدرة الفرد على تقرير من يحفظ المعلومات المتعلقة به وطريقة استعمال هذه المعلومات.

٢٣- ولكي يتسنى للأفراد ممارسة حقهم في خصوصية الاتصالات، يجب أن يكون بإمكانهم التحقق من بقاء هذه الاتصالات سرية، ومؤمَّنة، ومجهولة الهوية إن رغبوا في ذلك. وخصوصية الاتصالات يُستنتج منها أن الأفراد بإمكانهم تبادل المعلومات والأفكار في حيز لا يصل إليه باقي أفراد المجتمع، ولا القطاع الخاص، ولا الدولة نفسها في النهاية. ويقصد بأمن الاتصالات أن يكون الفرد قادراً على التحقق من وصول مراسلاته إلى الشخص المرسل إليه فقط دون تدخل أو تحوير فيها، ومن عدم التطفل على ما يرده من رسائل أيضاً. وتعد الاتصالات مجهولة الهوية من أهم التطورات التي جاءت بها الإنترنت، فهي تتيح للفرد التعبير عن نفسه بحرية دون خشية الاقتصاص منه أو إدانته.

ألف- أوجه الترابط بين الحق في الخصوصية والحق في حرية الرأي والتعبير

٢٤- غالباً ما يُنظر إلى الحق في الخصوصية باعتباره شرطا أساسيا لإعمال الحق في حرية التعبير. وقد ينطوي أي تدخل لا لزوم له في خصوصية الأفراد على تقييد مباشر وغير مباشر لتوليد الأفكار وتبادلها بحرية. فالقيود المفروضة على إغفال الهوية في الاتصالات، على سبيل المثال، لها أثر سلبي واضح على ضحايا كافة أشكال العنف وسوء المعاملة، الذين قد يترددون في الإبلاغ خوفاً من الوقوع ضحية مرتين. وفي هذا الصدد، تتضمن المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية إشارة مباشرة إلى حماية الشخص من التدخل في "مراسلاته"، وتفسير هذه العبارة ينبغي أن يشمل كافة أشكال الاتصال، سواء بواسطة الإنترنت أو أي وسيلة أخرى دون الاتصال بها[٥]. وكما لاحظ المقرر الخاص في تقرير

(٣) اليونسكو، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، ٢٠١٢، ص ٥١.

(٤) Lord Lester and D. Pannick (eds.). *Human Rights Law and Practice.* London, Butterworth, 2004, para. 4.82.

(٥) ICCPR commentary, p.401.

سابق[٦]، فإن الحق في خصوصية المراسلات ينشئ التزاماً شاملاً يقتضي من الدولة ضمان تسليم الرسائل الإلكترونية وغيرها من أشكال الاتصال على شبكة الإنترنت إلى المستلم المقصود فعليا دون أن تتدخل فيها أجهزة الدولة أو أطراف ثالثة أو تتفحصها[٧].

٢٥- وقد حللت اللجنة المعنية بحقوق الإنسان مضمون الحق في الخصوصية (المادة ١٧) في تعليقها العام رقم ١٦(١٩٨٨)، فاعتبرت أن المادة ١٧ تتوخى حماية حق كل شخص في عدم التعرض، على نحو تعسفي أو غير قانوني، للتدخل في خصوصياته أو في شؤون أسرته أو بيته أو مراسلاته. ورأت أن الأطر القانونية الوطنية يجب أن تنص على حماية هذا الحق. وتفرض هذه المادة التزامات محددة تتعلق بحماية خصوصية الاتصالات، إذ تشدد على ضرورة "أن تسلم المراسلات إلى المرسل إليه دون مصادرتها أو فتحها أو قراءتها. وعلى "حظر الرقابة، بالوسائل الإلكترونية أو بغيرها على السواء، وحظر اعتراض طريق الاتصالات الهاتفية والبرقية وغيرها من أشكال الاتصالات والتنصت على المحادثات وتسجيلها"[٨]. ويشير التعليق العام أيضا إلى أنه "يجب أن ينظم القانون عمليات جمع وحفظ المعلومات الشخصية باستخدام الحاسوب ومصارف البيانات وغيرها من الوسائل، سواء أكانت تجريها السلطات العامة أم الأفراد العاديون أو الهيئات الخاصة"[٩]. وعندما اعتُمد هذا التعليق العام كان أثر التطورات المستجدة في مجال تكنولوجيا المعلومات والاتصالات على الحق في الخصوصية بالكاد معروفاً.

٢٦- وأشارت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم ٣٤(٢٠١١) بشأن الحق في حرية التعبير إلى أنه ينبغي للدول الأطراف أن تأخذ في الحسبان مدى تأثير التطورات التي طرأت على تكنولوجيا المعلومات والاتصالات في إحداث تغيير كبير في الممارسات المتبعة في مجال الاتصال. ودعت اللجنة كذلك، إلى أن تتخذ الدول الأطراف جميع التدابير الضرورية لتعزيز استقلال هذه الوسائط الإعلامية الجديدة. وتضمَّن التعليق العام أيضاً تحليلاً للعلاقة بين حماية الخصوصية وحرية التعبير، وتوصية للدول الأطراف بأن تحترم أحد عناصر الحق في حرية التعبير والذي يشمل الامتياز المقيد المكفول للصحفيين بعدم الكشف عن مصادر المعلومات[١٠].

٢٧- ويحدث التعارض أيضاً بين الحق في الخصوصية والحق في حرية التعبير عندما تنشر وسائل الإعلام على سبيل المثال معلومات تعد ذات طابع شخصي. وبهذا المعنى، تنص المادة ١٩(٣) على قيود على حرية التعبير وتداول المعلومات لحماية حقوق الآخرين. على أنه من الضروري، كما هو الحال بالنسبة لجميع حالات التقييد الجائزة فيما يتعلق بالحق في حرية

---

(٦) A/HRC/17/23.

(٧) ICCPR commentary, p.401.

(٨) مركز الحقوق المدنية والسياسية، التعليق العام رقم ١٦ (التعليقات العامة)، الفقرة ٨.

(٩) المرجع نفسه، الفقرة ١٠.

(١٠) العهد الدولي الخاص بالحقوق المدنية والسياسية، التعليق العام رقم ٣٤.

التعبير (انظر أدناه)، التقيد الشديد بمبدأ التناسب، لأن عدم التقيد به ينطوي على خطر تقويض حرية التعبير. ففي المجال السياسي بوجه خاص، يجب ألا يكون المس بسمعة السياسيين الطيبة مسموحاً في جميع الحالات، وإلا فقدت حرية التعبير وتداول المعلومات أهميتها القصوى في عملية تكوين الآراء السياسية[١١]، والمناداة بالشفافية ومكافحة الفساد. وتشير السوابق القضائية الدولية على المستوى الإقليمي إلى ضرورة الاحتكام في حالات التعارض بين الخصوصية وحرية التعبير، إلى الصالح العام ككل في المسائل المبلغ عنها[١٢].

باء- القيود التي يجوز فرضها على الخصوصية وحرية التعبير

٢٨- يخول إطار المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية فرض قيود ضرورية مشروعة ومتناسبة على الحق في الخصوصية بإجراءات تقييد جائزة. وخلافاً لأحكام الفقرة ٣ من المادة ١٩ التي تحدد عناصر معيار القيود الجائزة[١٣]، لا تتضمن صيغة المادة ١٧ حكماً تقييدياً. وعلى الرغم من هذه الاختلافات في الصياغة، فإنه من المفهوم أن المادة ١٧ من العهد ينبغي أن تفسر أيضاً على أنها تتضمن عناصر معيار القيود الجائزة التي ورد وصفها بالفعل في تعليقات عامة أخرى للجنة المعنية بحقوق الإنسان[١٤].

٢٩- ويتمثل موقف المقرر الخاص في هذا الصدد في أن الحق في الخصوصية ينبغي أن يخضع لنفس معيار القيود الجائزة المتعلق بالحق في حرية التنقل، على نحو ما أوضحه التعليق العام رقم ٢٧[١٥]. ويشمل المعيار حسبما ورد في التعليق، جملة من العناصر منها ما يلي:

(أ) يجب أن تكون القيود منصوصاً عليها في القانون (الفقرتان ١١ و١٢)؛

(ب) لا يخضع جوهر حق من حقوق الإنسان لقيود (الفقرة ١٣)؛

(ج) يجب أن تكون القيود ضرورية في مجتمع ديمقراطي (الفقرة ١١)؛

(د) يجب عدم ممارسة السلطة التقديرية بشكل مطلق عند تطبيق القيود (الفقرة ١٣)؛

---

(١١) Nowak, Manfred, United Nations Covenant on Civil and Political Rights: CCPR Commentary (1993), p. 462.

(١٢) اليونسكو، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، ٢٠١٢، الصفحتان ٥٣ و٩٩.

(١٣) توجد قوائم بالقيود التي يجيزها العهد في المادة ١٢(٣) المتعلقة بحق الفرد في حرية التنقل وحرية اختيار مكان إقامته؛ والمادة ١٨(٣) المتعلقة بالحق في حرية الفكر والوجدان والدين؛ والمادة ٢١ المتعلقة بالحق في التجمع السلمي؛ والمادة ٢٢(٢) المتعلقة بالحق في حرية تكوين الجمعيات.

(١٤) المرجع نفسه.

(١٥) انظر أيضاً العهد الدولي الخاص بالحقوق المدنية والسياسية، التعليق العام رقم ٣٤.

(هـ) لكي تكون القيود مسموحا بها، فإنه لا يكفي أن تخدم أحد الأهداف المشروعة المذكورة؛ بل يجب أن تكون ضرورية لتحقيق الغرض المشروع (الفقرة ١٤)؛

(و) يجب أن تتماشى التدابير التقييدية مع مبدأ التناسب؛ وأن تكون مناسبة لتحقيق وظيفتها الحمائية؛ وأن تكون أقل الوسائل تطفلاً مقارنة بغيرها من الوسائل الكفيلة بتحقيق النتيجة المنشودة؛ ويجب أن تتناسب مع المصلحة المراد حمايتها (الفقرتان ١٤ و١٥).

جيم- الاستعراضات الأخيرة التي أجرتها الآليات الدولية لحماية حقوق الإنسان

٣٠- أجرى المقرر الخاص في التقارير السابقة تقييما لأثر الإنترنت على إعمال الحق في حرية الرأي والتعبير (A/HRC/17/27 وA/66/290). وأشار إلى أن المستخدمين يمكنهم إلى حد ما استخدام الإنترنت دون كشف أسمائهم لكن الدول والجهات الفاعلة في القطاع الخاص تستطيع بدورها الحصول على تكنولوجيات حديثة لرصد وجمع المعلومات التي تتعلق باتصالات الأفراد وأنشطتهم. ومن المحتمل أن ينطوي استخدام هذه التكنولوجيا على انتهاك للحق في الخصوصية مما يقوض شعور الناس بالثقة والأمان على الإنترنت ويعيق الانسياب الحر للمعلومات والأفكار عبرها. وقد حث المقرر الخاص الدول على اعتماد قوانين فعالة لحماية الخصوصية والبيانات وفقاً لمعايير حقوق الإنسان، وعلى اتخاذ جميع التدابير المناسبة لضمان تمكن الأفراد من التعبير عن أنفسهم عبر الإنترنت دون الإفصاح عن هويتهم[١٦].

٣١- وقام آخرون من المكلفين بولايات في إطار الإجراءات الخاصة بالنظر في مسألة التدخل في الحق في الخصوصية. فقد أجرى المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب دراسة للتطورات المستجدة في مجال الممارسات والتقنيات المعتمدة في المراقبة التي نالت من الحق في الخصوصية بذريعة مكافحة الإرهاب[١٧]. وأكد المقرر الخاص أن هذه التدابير أدت إلى انتهاك الحق في الخصوصية فضلاً عن تأثيرها على الحق في المعاملة وفق الأصول القانونية والحق في حرية التنقل وحرية تكوين الجمعيات وحرية التعبير. وحث الحكومات على أن تبين بالتفصيل كيفية تقيدها، فيما تعتمده من سياسات للمراقبة، بمبدأي التناسب والضرورة وفقاً للمعايير الدولية لحقوق الإنسان، وماهية التدابير المتخذة لمنع التجاوزات. ودعا المقرر الخاص أيضا إلى اعتماد قوانين شاملة تقضي بحماية البيانات والخصوصية وإنشاء هيئات رقابية تتمتع بالقوة والاستقلالية لتتولى إعادة النظر في استخدام تقنيات المراقبة التطفلية ومعالجة المعلومات الشخصية. ودعا أيضاً إلى تخصيص موارد للبحوث والتطوير في مجال التكنولوجيات التي تعزز الخصوصية.

---

(١٦) A/HRC/17/27، ص ٢٩.

(١٧) A/HRC/13/37.

٣٢- وفي الآونة الأخيرة، أبدت آليات أخرى معنية بحماية حقوق الإنسان اهتمامها أيضاً بأثر مراقبة الاتصالات على حماية الحق في الخصوصية والحق في حرية التعبير. فأعربت اللجنة المعنية بحقوق الإنسان على سبيل المثال عن قلقها إزاء الادعاءات المتعلقة بلجوء الدولة إلى مراقبة استخدام الإنترنت وحجب مواقع معينة[١٨]، وأوصت بتنقيح التشريعات التي تخول السلطة التنفيذية صلاحيات واسعة في مراقبة الاتصالات الإلكترونية[١٩]. وشمل الاستعراض الدوري الشامل أيضاً تقديم توصيات تدعو على سبيل المثال، إلى ضمان احترام التشريعات المتعلقة بالإنترنت وباقي تكنولوجيات الاتصال الحديثة للالتزامات الدولية في مجال حقوق الإنسان[٢٠].

خامساً- طرائق مراقبة الاتصالات

٣٣- تنذر تكنولوجيات وترتيبات المراقبة الحديثة التي تمكِّن الدول من التدخل في الحياة الخاصة للأفراد بطمس الحد الفاصل بين الحيز الخاص والحيز العام. فهي تسهل رصد الأفراد رصداً ينطوي على تعسف واقتحام الخصوصية، حتى أنه قد يتعذر على الفرد أن يعرف حتى أنه مراقب، فما بالك بالاعتراض على هذه المراقبة. وإحراز التقدم التكنولوجي يعني أن القدرة الفعالة للدولة على المراقبة لم تعد مقيدة بنطاق أو مدة. فمع تراجع تكاليف استخدام التكنولوجيا وتخزين البيانات، لم تعد هناك عوائق مالية أو عملية تحول دون إجراء المراقبة. وبذلك، أصبحت الدولة اليوم أكثر قدرة من أي وقت مضى على إجراء مراقبة متزامنة واقتحامية ومحددة الهدف على نطاق واسع.

ألف- مراقبة محددة الهدف للاتصالات

٣٤- تستطيع الدول الحصول على أنواع مختلفة من التقنيات والتكنولوجيا لمراقبة الاتصالات على المراسلات الخاصة بالشخص المستهدف. فالقدرة على الاعتراض الآني تمكِّن الدول من التنصت على المكالمات الهاتفية التي يجريها أي شخص عن طريق جهاز الهاتف الثابت أو المحمول وتسجيلها، وذلك عبر تسخير قدرات الاعتراض التي يطلب من جميع شبكات الاتصالات إدماجها في منظوماتها، لممارسة الرقابة من قبل الدولة[٢١]. ويمكن التحقق

(١٨) CCPR/C/IRN/CO/3.

(١٩) CCPR/C/SWE/CO/6.

(٢٠) A/HRC/14/10.

(٢١) انظر على سبيل المثال: قانون الولايات المتحدة لعام ١٩٩٤ بشأن المساعدة في مجال الاتصالات لأغراض إنفاذ القانون (الولايات المتحدة)؛ وقانون الاتصالات لعام ١٩٩٧، الجزء ١٥ (أستراليا)؛ وقانون تنظيم صلاحيات إجراء التحقيقات لعام ٢٠٠٠، المواد ١٢-١٤ (المملكة المتحدة)؛ وقانون (قدرات اعتراض) الاتصالات لعام ٢٠٠٤.

من مكان وجود الشخص وقراءة رسائله النصية وتسجيلها. ويمكن لسلطات الدولة أيضاً أن ترصد نشاط الشخص على شبكة الإنترنت بما في ذلك المواقع التي يتصفحها وذلك عن طريق تثبيت جهاز تنصت على كابل الإنترنت الذي يستخدمه موقع أو شخص ما.

٣٥- وقد يكون النفاذ إلى مضمون البريد الإلكتروني والرسائل التي يخزنها الشخص بالإضافة إلى بيانات الاتصال الأخرى ذات الصلة، أمرا متاحا من خلال شركات الإنترنت ومقدمي خدمة الإنترنت. ويسود القلق بشأن مبادرة المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية، وهو هيئة أوروبية مكلفة بوضع المعايير، لإجبار مقدمي الخدمات السحابية[٢٢] على دمج "قدرات الاعتراض القانوني" في التكنولوجيا السحابية لتمكين السلطات الحكومية من النفاذ المباشر إلى المحتوى الذي يخزنه مقدمو هذه الخدمة، بما في ذلك البريد الإلكتروني والرسائل النصية والبريد الصوتي[٢٣].

٣٦- وبمقدور الدول تعقب حركة هواتف محمولة محددة، وتحديد هوية جميع الأشخاص الذين يملكون هاتفا محمولا ضمن منطقة معينة، واعتراض الاتصالات والرسائل النصية، باعتماد أساليب مختلفة. وتستخدم بعض الدول الأجهزة الخاصة بمراقبة الهاتف المحمول وهي مقفلة، والتي تعرف بصائد رقم التعريف العالمي للمشترك في اتصالات الهاتف المحمول (IMSI)، وهي أجهزة قابلة للتركيب في موقع من المواقع بصورة مؤقتة (كالموقع الذي تنظم فيه مظاهرة أو مسيرة) أو بصورة دائمة (كالمطار أو غيره من المعابر الحدودية). وتحاكي الأجهزة الصائدة هذه برج الهاتف المحمول عن طريق إرسال إشارات الهاتف المحمول والاستجابة لها من أجل استخراج الرقم الفريد لبطاقة تحديد هوية المشترك (SIM) من جميع الهواتف المحمولة داخل منطقة معينة.

٣٧- ويتزايد إقبال الدول أيضاً على حيازة البرامجيات التي يمكن استخدامها لاختراق الحاسوب أو الهاتف المحمول أو غيره من الأجهزة الرقمية الخاصة بشخص ما[٢٤]. ويمكن استخدام برامجيات التطفل الهجومية، بما في ذلك تلك التي يطلق عليها "حصان طروادة" (وتعرف أيضاً باسم برامجيات التجسس أو البرامجيات الخبيثة)، لتشغيل ميكروفون أو كاميرا الجهاز، لتتبع العمليات التي أجريت من الجهاز، والوصول إلى أي معلومات مخزنة عليه أو تحويرها أو محوها. وهذه البرمجيات تمكِّن الدولة من التحكم تماما في الجهاز الذي تم اختراقه، ولا يمكن كشفها عملياً.

---

(٢٢) يقدم موفر الحوسبة السحابية خدمات التخزين الشبكي للبيانات عبر الإنترنت.

(٢٣) ETSI DTR 101 567 VO.0.5 (2012-14), Draft Technical Report: Lawful Interception (LI); Cloud/Virtual Services (CLI).

(٢٤) توبي مندل، وأندرو بوديفات، وبن واغنر، وديكسي هوتن، وناتاليا توريس، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، *سلسلة اليونسكو بشأن حرية الإنترنت* (٢٠١٢)، ص ٤١.

باء- مراقبة وسائل الاتصال الجماهيري

٣٨- لا تزال تكاليف المراقبة على نطاق واسع والعوائق اللوجستية التي تحول دونها تتراجع باطراد، مع انتشار التكنولوجيات التي تتيح توسيع نطاق اعتراض الاتصالات ورصدها وتحليلها. وبمقدور بعض الدول اليوم تعقب وتسجيل الاتصالات عبر الإنترنت والاتصالات الهاتفية على النطاق الوطني. إذ إن تثبيت أجهزة تنصت على كابلات الألياف الضوئية، التي تنساب من خلالها معظم معلومات الاتصالات الرقمية، واستخدام تطبيقات تمييز النصوص والتعرف على الصوت والكلام، يمكِّن الدول من إحكام سيطرتها بشكل كامل تقريباً على الاتصالات السلكية واللاسلكية وعبر الإنترنت. وقد أفيد بأن الحكومة المصرية والحكومة الليبية، على سبيل المثال، قد اعتمدتا هذه النظم في الفترة التي سبقت الربيع العربي[٢٥].

٣٩- ويسهِّل الاستبقاء الإلزامي للبيانات في كثير من الدول، جمع عدد هائل من بيانات الاتصال التي يمكن ترشيحها وتحليلها في وقت لاحق. وبفضل التكنولوجيا، تستطيع الدولة إجراء مسح للمكالمات الهاتفية والرسائل النصية لتمييز استخدام بعض كلمات أو أصوات أو عبارات معينة، أو ترشيح النشاط على شبكة الإنترنت لتحديد الوقت الذي يقوم فيه الشخص بتصفح مواقع معينة أو الدخول إلى مصادر معلومات محددة على الشبكة. وقد تُصمَّم "صناديق سوداء" لتفحص البيانات المنسابة عبر شبكة الإنترنت ليتم من خلالها ترشيح وتفكيك جميع المعلومات عن الأنشطة التي تجرى على الشبكة. وهذه الطريقة التي تعرف باسم "التفتيش العميق في رزم البيانات" تتيح للدولة ما هو أكثر من مجرد معرفة المواقع الشبكية التي قام الأشخاص بتصفحها، إذ تمكنها من تحليل محتوى هذه المواقع. ويقال إن الدول التي شهدت مؤخراً انتفاضات شعبية في الشرق الأوسط ومنطقة شمال أفريقيا قد لجأت على سبيل المثال، إلى التفتيش في أعماق رزم البيانات[٢٦].

٤٠- ويعد رصد وسائل التواصل الاجتماعي أداة أخرى من الأدوات التي تلجأ الدول إلى استخدامها بانتظام اليوم. فالدول قادرة فعلياً على رصد الأنشطة على مواقع التواصل الاجتماعي على الإنترنت والمدونات والمنافذ الإعلامية، لرسم خريطة للصلات والعلاقات، والآراء والتجمعات، وحتى للمواقع. وبإمكان الدول أيضاً تطبيق تكنولوجيات التنقيب في البيانات، المتطورة جداً، على المعلومات المتاحة للعموم أو على بيانات الاتصال التي توفرها الأطراف الثالثة المقدمة للخدمة. وبصورة أعم، اقتنت الدول أيضا وسائل تقنية للحصول على أسماء المستخدمين وكلمات السر من مواقع التواصل الاجتماعي كالفيسبوك[٢٧].

---

(٢٥) European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), pp. 9-10.

(٢٦) مندل وآخرون، المرجع الآنف الذكر، ص ٤٣.

(٢٧) European Parliament، المرجع الآنف الذكر، ص ٦.

جيم- إمكانية الاطلاع على بيانات الاتصال

٤١- تسعى الدول، بالإضافة إلى اعتراض وتتبع محتوى الاتصالات التي يجريها الأفراد، إلى الاطلاع على بيانات الاتصال المحفوظة لدى الأطراف الثالثة المقدمة للخدمة وشركات الإنترنت. وتتزايد قيمة الاطلاع على بيانات الاتصال باعتباره من تقنيات المراقبة التي تستخدمها الدول في ظل تزايد كميات ما يجمعه القطاع الخاص يوما بعد يوم من بيانات شتى تكشف معلومات حساسة عن حياة الناس اليومية، وتفضيل الأفراد والشركات لتخزين محتوى اتصالاتهم، كرسائل البريد الصوتي والبريد الإلكتروني والوثائق، لدى الأطراف الثالثة المقدمة للخدمة.

٤٢- ويمكن أن تستخدم الدولة بيانات الاتصال التي تجمعها الأطراف الثالثة المقدمة للخدمة، بما في ذلك كبريات شركات الإنترنت، لإنشاء ملف تعريف موسع للأشخاص المعنيين. وحتى الاطلاع على سجلات حركة الاتصالات التي تبدو في ظاهرها خالصة من كل هدف وتحليلها قد يتيح في مجمله إنشاء ملف تعريفي عن حياة الشخص الخاصة، ويشمل ذلك وضعه الصحي وآراءه و/أو انتماءاته السياسية والدينية، وصلاته واهتماماته، مما يكشف قدراً من التفاصيل يوازي ما يتيحه محتوى الاتصالات وحده إن لم يكن أكثر[٢٨]. وتستطيع الدول من خلال تجميع المعلومات عن علاقات الشخص ومكانه وهويته ونشاطه، تتبع حركته ونشاطاته في مجالات مختلفة تشمل المكان الذي يسافر منه والمكان الذي يدرس فيه وما يقرأ ومع من يتفاعل.

٤٣- وتتزايد حالات اطلاع الدول على بيانات الاتصال بوتيرة متسارعة. ففي السنوات الثلاث التي أبلغت شركة غوغل خلالها عن عدد ما يردها من طلبات للحصول على بيانات الاتصالات، تضاعف عدد هذه الطلبات تقريبا، إذ قفز من ١٢ ٥٣٩ طلباً في الأشهر الستة الأخيرة من عام ٢٠٠٩، إلى ٢١ ٣٨٩ في الأشهر الستة الأخيرة من عام ٢٠١٢[٢٩]. وفي المملكة المتحدة، حيث سلطات إنفاذ القانون مخولة أن تأذن لنفسها بتقديم طلبات للحصول على معلومات عن الاتصالات، أُبلغ عن تقديم حوالي ٥٠٠ ٠٠٠ طلب من هذا النوع سنوياً[٣٠]. وفي جمهورية كوريا التي يناهز عدد سكانها ٥٠ مليون نسمة، يتم الإبلاغ عن تقديم حوالي ٣٧ مليون طلب للحصول على بيانات الاتصال في كل عام[٣١].

---

(٢٨) Alberto Escudero-Pascual and Gus Hosein, "Questioning lawful access to traffic data", *Communications of the ACM*, Volume 47 Issue 3, March 2004, pp. 77–82.

(٢٩) انظر العنوان التالي: http://www.google.com/transparencyreport/userdatarequests/.

(٣٠) انظر العنوان التالي: http://www.intelligencecommissioners.com/docs/0496.pdf.

(٣١) Money Today, 23 October, 2012، في إشارة إلى ما أفصحت عنه لجنة الاتصالات الكورية في سياق المراجعة السنوية الوطنية لعام ٢٠١٣ لعضو البرلمان السيدة يو سونغ - صموي، انظر العنوان التالي: http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1.

دال- ترشيح الإنترنت ورقابتها

٤٤- لم يقتصر أثر التطورات التكنولوجية على تسهيل اعتراض الاتصالات وإمكانية الاطلاع عليها في حالات محددة، وإنما تعدى ذلك إلى تمكين الدول من ترشيح النشاط الشبكي على نطاق واسع، حتى على الصعيد الوطني. ويلجأ كثير من البلدان إلى ترشيح الانترنت تحت غطاء الحفاظ على الوئام الاجتماعي أو القضاء على خطاب الكراهية، لكنها تستخدمه في الواقع للقضاء على المعارضين أو المنتقدين أو الناشطين.

٤٥- وتكنولوجيات الترشيح الآنفة الذكر تسهل أيضاً مراقبة النشاط الشبكي لكي يتسنى للدولة كشف المحظور من الصور أو العبارات أو عناوين المواقع أو غيرها من المحتويات، وممارسة الرقابة عليها أو تحريفها. وقد تلجأ الدول إلى استخدام هذه التكنولوجيات لرصد استخدام كلمات وعبارات محددة، من أجل إخضاع استخدامها للرقابة أو التنظيم، أو تحديد من يستخدمها. وقد أفيد بأن ترشيح شبكة الإنترنت في البلدان التي يبلغ فيها معدل انتشار استخدامها مستويات عالية يتيح فرض رقابة على محتوى المواقع الشبكية والاتصالات، ويسهِّل مراقبة المدافعين عن حقوق الإنسان والنشطاء في هذا المجال[٣٢].

٤٦- وبالإضافة إلى التكنولوجيات التي تسهل ممارسة الترشيح والرقابة، يلجأ كثير من الدول إلى ترشيح الإنترنت يدوياً، عن طريق إنشاء مفتشين وشرطة إلكترونية تتولى الرصد المادي لمحتوى المواقع الشبكية، والشبكات الاجتماعية، والمدونات وغيرها من وسائط الإعلام. وفي بعض الدول، تُكلَّف "شرطة الفضاء الإلكتروني" بتفتيش محتوى الإنترنت ومراقبته، والبحث في المواقع الشبكية والعقد الأساسية ضمن المواقع الشبكية (لا سيما منتديات النقاش على الإنترنت)، وذلك بهدف منع أو إغلاق المواقع الشبكية كلما كان محتواها لا يروق للحكومة أو يتضمن انتقاداً للقيادة في البلاد. ويلقى بعبء حفظ النظام بهذا الأسلوب على كاهل الوسطاء في القطاع الخاص، مثل محركات البحث ومنتديات التواصل الاجتماعي على شبكة الإنترنت، وذلك من خلال اعتماد قوانين توسِّع نطاق تحميل المسؤولية عما تتضمنه المواقع الشبكية من محتويات ممنوعة لتشمل الأشخاص الذين عبروا عنها في الأصل وجميع الوسطاء.

هاء- القيود المفروضة على إغفال الهوية

٤٧- حقّق ظهور شبكة الإنترنت أشكالاً من التقدم، من أهمها قدرة المستعمل على الوصول إلى المعلومات وإذاعتها دون الكشف عن هويته، وإجراء اتصالات مأمونة دون الاضطرار للتعريف بهويته. وكان ذلك ممكناً في البداية نظراً لغياب "عملية تحديد الهوية" على

(٣٢) European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), p. 12.

شبكة الإنترنت؛ حيث لم يكن ممكناً التعرف على الجهة الكامنة وراء اتصال أو عنوان بريد إلكتروني محدد أو حتى حاسوب معيّن. لكن، وباسم الأمن وإنفاذ القوانين، ألغت الدول تدريجياً إمكانية إجراء المستعمل اتصالاً دون الكشف عن هويته. فبات الأفراد ملزمين، في العديد من الدول، بالتعريف بأنفسهم في مقاهي الإنترنت وتسجيل أنشطتهم في الحواسيب العمومية. وتتزايد المطالبة بتحديد الهوية وتسجيلها عند شراء "بطاقة تحديد هوية المشترك" (SIM) أو شراء جهاز هاتف محمول، أو عند زيارة بعض المواقع الرئيسية على شبكة الإنترنت، أو عند إبداء تعليقات على مواقع وسائط الإعلام أو المدونات.

٤٨- وتيسّر القيود المفروضة على إغفال الهوية مراقبة الدولة للاتصالات بتبسيط التعرّف على هوية الأفراد الذين يطلعون على محتوى محظور أو ينشرونه، وتجعل هؤلاء الأفراد أكثر عُرضة لأشكال أخرى من مراقبة الدولة.

٤٩- وفي هذا الصدد، فإن للقيود المفروضة على إغفال الهوية أثراً رادعاً لحرية الإعلام والتعبير عن الأفكار. وقد تؤدي أيضاً بحكم الأمر الواقع إلى استبعاد أفراد من المجالات الاجتماعية الحيوية، وتقوّض حقهم في التعبير وتلقي المعلومات، وتزيد من تفاقم أوجه التفاوت الاجتماعي. وفضلاً عن ذلك، تمكّن القيود المفروضة على إغفال الهوية القطاع الخاص من جمع كميات كبيرة من المعلومات وخزنها، بما يفرض أعباء ومسؤوليات هامة على الشركات لحماية سرية هذه البيانات وأمنها.

سادساً- الشواغل المتعلقة بالمعايير القانونية الوطنية

٥٠- لم تواكب التشريعات، بصورة عامة، وتيرة التغييرات التي تشهدها التكنولوجيا. وفي أكثرية الدول، فإن المعايير القانونية غير موجودة أو غير مناسبة للتعامل مع البيئة الحديثة لمراقبة الاتصالات. لذلك، تسعى الدول، على نحو متزايد، لتبرير استخدام تكنولوجيات جديدة، في الأُطر القانونية القديمة، دون الاعتراف بأن ما يتوفّر لديها من قدرات هامة حالياً يتجاوز بكثير ما تخوله تلك الأُطر. ويعني ذلك تذرع العديد من البلدان بأحكام قانونية مُبهمة وذات مفهوم عام لإخفاء المشروعية على استعمال تقنيات تطفلية خطيرة وإقراره. ودون سنّ قوانين واضحة تخوّل استعمال هذه التكنولوجيات والتقنيات وتعرّف نطاق استعمالها، لا يمكن للأفراد أن يتوقعوا تطبيقاتها - أو حتى يعرفوا بوجودها. وفي الوقت نفسه، تُعتمد قوانين بهدف توسيع نطاق الاستثناءات تحت بند الأمن القومي، أو لإضفاء الصبغة الشرعية على تقنيات المراقبة التطفلية دون رقابة أو مراجعة مستقلة.

٥١- وتزيد المعايير القانونية غير المناسبة من احتمال تعرّض الأفراد لانتهاك حقوق الإنسان المكفولة لهم، بما في ذلك الحق في الخصوصية والحق في حرية التعبير. ولهذه المعايير أيضاً آثار سلبية على فئات معينة من الأفراد - مثل أعضاء بعض الأحزاب السياسية أو النقابيين

أو الأقليات القومية والإثنية واللغوية – الذين قد يتعرّضون أكثر من غيرهم لمراقبة الدولة لاتصالاتهم. وبدون وضع أشكال حماية قانونية قوية، يمكن أن يتعرّض الصحفيون والمدافعون عن حقوق الإنسان والناشطون السياسيون للمراقبة التعسفية.

٥٢- وتوثّق مراقبة المدافعين عن حقوق الإنسان توثيقاً جيداً في العديد من البلدان، حيث يبلغ المدافعون عن حقوق الإنسان والناشطون السياسيون في تلك الحالات عن رصد هواتفهم المحمولة وبريدهم الإلكتروني، وعن تعقّب تنقلهم. ويتعرّض الصحفيون تحديداً أيضاً لمراقبة اتصالاتهم بسبب اعتمادهم على الاتصال عبر شبكة الإنترنت. ولكي يتلقى الصحفيون المعلومات ويتابعونها من مصادر سرية، من بينها المُبلغون عن المخالفات، يجب أن يتمكنوا من الاعتماد على الخصوصية والأمن وعدم إمكانية الكشف عن الهوية في اتصالاتهم. ولا يمكن لبيئة تنتشر فيها مراقبة واسعة النطاق، لا تُقيَّد بأصول قانونية أو بإشراف قضائي، أن تتحمّل افتراض حماية المصادر. بل يمكن أن يكون للمراقبة الضيقة وغير الشفافة وغير الموثّقة على أرض الواقع أثر رادع إذا لم يرافق استخدامها توثيق حذر وعلني وكذلك ضوابط وموازين معروفة تمنع إساءة استخدامها.

٥٣- وتتضمن الأجزاء الفرعية التالية الشواغل المشتركة إزاء القوانين التي تمكّن الدول من مراقبة الاتصالات فتُهدد الحق في حرية التعبير والحق في الخصوصية.

ألف- انعدام الرقابة القضائية

٥٤- كانت مراقبة الاتصالات تخضع سابقاً لإذن السلطة القضائية. لكن هذا الشرط بات يتضاءل، بل يجنح إلى الانقراض، حيث أصبح بإمكان وزير حكومة في بعض البلدان أو أحد نوابه أو إحدى اللجان منح الإذن باعتراض الاتصالات. ففي المملكة المتحدة، على سبيل المثال، يأذن وزير من وزراء الحكومة[٣٣] باعتراض الاتصالات؛ ويتولّى ذلك في زمبابوي وزير النقل والاتصالات[٣٤]. ويمكن أن تُخوَّل مراقبة الاتصالات تدريجياً على نطاق واسع ودون تمييز، ودون الحاجة إلى قيام السلطات المكلفة بإنفاذ القوانين بإثبات الأساس الوقائعي للمراقبة على أساس كل حالة بمفردها.

٥٥- وتخلّت دول عديدة عن ضرورة قيام الوكالات المكلفة بإنفاذ القوانين بمراجعة المحاكم لمواصلة الرقابة بعد إصدار أمر اعتراض الاتصالات. فبموجب القانون المتعلق بمنع الإرهاب في كينيا لعام ٢٠١٢، على سبيل المثال، يمكن اعتراض الاتصالات لفترة غير محددة، دون اشتراط قيام الوكالات المكلَّفة بإنفاذ القوانين بمراجعة المحاكم أو السعي لتمديد فترة المراقبة. وتفرض بعض الدول قيوداً زمنية على تنفيذ أوامر الاعتراض بيد أنها تمكِّن السلطات المكلفة بإنفاذ القوانين من تجديد هذه الأوامر مراراً وتكراراً دون تحديد المدة.

(٣٣) المادة ٥، قانون عام ٢٠٠٠ المتعلق باللوائح المنظمة لسلطات التحقيق.

(٣٤) المادة ٥، قانون عام ٢٠٠٦ المتعلق باعتراض الاتصالات.

٥٦- حتى وإن نص القانون على استصدار إذن قضائي، كثيراً ما يتم ذلك بحكم الأمر الواقع بموافقة تعسفية على طلبات الهيئات المكلفة بإنفاذ القوانين. ويسري ذلك بصورة خاصة عندما تكون الشروط المطلوبة من هذه الهيئات ميسّرة. وعلى سبيل المثال، لا يطالب القانون المتعلق بلوائح اعتراض الاتصالات في أوغندا لعام ٢٠١٠ السلطات المكلفة بإنفاذ القوانين إلا بإثبات أن هناك مبررات "معقولة"، لتمكينها من الاعتراض. وفي هذه الحالات، فإن عبء إثبات لزوم المراقبة ضحل للغاية بالنظر إلى احتمال أن تؤدي المراقبة إلى إجراء تحقيقات أو القيام بأعمال تمييزية أو انتهاكات لحقوق الإنسان. وفي بلدان أخرى، تجيز مجموعة قوانين معقدة الاطلاع على فحوى الاتصالات ومراقبتها في ظل ظروف متباينة. ففي إندونيسيا، على سبيل المثال، يتضمن القانون المتعلق بالمؤثّرات العقلية والقانون المتعلق بالمخدرات والقانون المتعلق بالمعلومات والمعاملات الإلكترونية والقانون المتعلق بالاتصالات السلكية واللاسلكية والقانون المتعلق بمكافحة الفساد كافة أحكاماً تتعلق بمراقبة الاتصالات. وفي المملكة المتحدة، يُسمح لما يربو على ٢٠٠ وكالة وقوات الشرطة وسلطات السجون بالحصول على بيانات الاتصالات بموجب القانون المتعلق بلوائح سلطات التحقيق لعام ٢٠٠٠. ونتيجة لذلك، يصعب على الأفراد توقع وقف خضوعهم للمراقبة ومعرفة أي وكالة من وكالات الدولة تجريها.

٥٧- وفي العديد من الدول، تُجبَر الجهات المقدمة لخدمات الاتصالات على تعديل هياكلها الأساسية بما يمكّن من المراقبة المباشرة، بما يقضي على إمكانية الرقابة القضائية. وفي عام ٢٠١٢، على سبيل المثال، أصدرت وزارة العدل ووزارة تكنولوجيا المعلومات والاتصالات في كولومبيا مرسوماً يطالب الجهات المقدِّمة لخدمات الاتصالات بوضع هياكل أساسية تُمكّن الشرطة القضائية من الاطلاع مباشرة على فحوى الاتصالات، دون استصدار أمر من المدعي العام[٣٥]. ويقضي القانون السالف الذكر المتعلق بلوائح اعتراض الاتصالات لعام ٢٠١٠ في أوغندا (المادة ٣) بإنشاء مركز رصد، ويكلف الجهات المقدمة لخدمات الاتصالات السلكية واللاسلكية بضمان تحويل الاتصالات المعترَضة إلى مركز الرصد (المادة ٨(١)(و)). وتقترح حكومة الهند إنشاء نظام رصد مركزي يحوِّل جميع الاتصالات إلى الحكومة المركزية، بما يمكِّن وكالات الأمن من تجاوز التفاعل مع الجهات المقدمة للخدمات[٣٦]. وتنأى هذه الترتيبات بمراقبة الاتصالات عن الإذن القضائي وتسمح بمراقبة سرية غير منظمة، بما يقضي على أي قدر من الشفافية أو المساءلة من جانب الدولة.

---

(٣٥) مرسوم وزارة العدل ووزارة تكنولوجيا المعلومات والاتصالات رقم ١٧٠٤. ويندرج محتوى المرسوم في قانون الإجراءات الجنائية لعام ٢٠٠٤.

(٣٦) وزارة الاتصالات. حكومة الهند. التقرير السنوي للفترة ٢٠١١-٢٠١٢، ص. ٥٨ - (http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf).

باء- الاستثناءات المتعلقة بالأمن القومي

٥٨- أصبحت المفاهيم المبهمة وغير المحددة "للأمن القومي" تبريراً مقبولاً لاعتراض الاتصالات والاطلاع على فحواها في العديد من البلدان. ففي الهند، على سبيل المثال، يسمح القانون المتعلق بتكنولوجيا المعلومات لعام ٢٠٠٨ باعتراض الاتصالات بما يخدم أموراً منها "سيادة الهند وسلامتها والدفاع عنها، أو العلاقات الودية مع الدول الأجنبية، أو النظام العام، أو التحقيق في أي جريمة" (المادة ٦٩).

٥٩- وفي العديد من الحالات، تتمتع وكالات الاستخبارات الوطنية كذلك باستثناءات عامة لشرط الإذن القضائي. وفي الولايات المتحدة، على سبيل المثال، يمكِّن القانون المتعلق بمراقبة الاستخبارات الأجنبية وكالة الأمن القومي من اعتراض الاتصالات دون إذن قضائي عندما يكون أحد الأطراف في الاتصال خارج الولايات المتحدة ويُعتقد بصورة معقولة أن أحد المشاركين في الاتصال ينتمي إلى منظمة تعتبرها الدولة منظمة إرهابية. وتمكِّن التشريعات الألمانية من تنصت دوائر الاستخبارات الحكومية آلياً دون إذن على الاتصالات المحلية والدولية لأغراض حماية النظام الديمقراطي الحر أو وجود الدولة أو أمنها[٣٧]. وفي السويد، يجيز القانون المتعلق باستخبارات الإشارات في عمليات الدفاع لوكالة الاستخبارات السويدية اعتراض جميع الاتصالات عبر الهاتف وشبكة الإنترنت التي تجري داخل حدود السويد دون أي إذن أو أمر صادر عن المحاكم. وفي جمهورية تنزانيا المتحدة، يمكِّن القانون المتعلق بدوائر الاستخبارات والأمن لعام ١٩٩٦ دوائر الاستخبارات من إجراء أي تحقيقات بشأن أي شخص أو هيئة يُعتقد بصورة معقولة أنه يُشكل خطراً أو مصدر خطر على أمن الدولة أو تهديداً له.

٦٠- ويُعتبر اللجوء إلى المفهوم الضبابي للأمن القومي لتبرير القيود الاقتحامية على التمتع بحقوق الإنسان مصدر قلق بالغ[٣٨]. ويُعرَّف المفهوم بصورة واسعة حيث تتلاعب به الدول كأداة لتبرير الأعمال التي تستهدف الفئات الضعيفة مثل المدافعين عن حقوق الإنسان أو الصحفيين أو الناشطين. ويستخدم أيضاً لتأمين السرية غير اللازمة عادة للتحقيقات أو أنشطة المكلفين بإنفاذ القوانين، بما يقوِّض مبادئ الشفافية والمساءلة.

جيم- الاطلاع غير المنظم على محتوى بيانات الاتصالات

٦١- إن الاطلاع على محتوى بيانات الاتصالات لدى الجهات المحلية المقدمة لخدمات الاتصالات عادة ما يقره تشريع أو شرط مرتبط بإصدار التراخيص. وعليه، تتاح عادة للدول الحرية التامة للاطلاع على بيانات الاتصالات بقليل من الرقابة أو التنظيم. فقانون

(٣٧) القانون رقم زاي-١٠.

(٣٨) القرارات الصادرة عن مجلس حقوق الإنسان بشأن مكافحة الإرهاب.

عام ٢٠١٢ المتعلق بغسل الأموال في البرازيل، على سبيل المثال، يمنح الشرطة سلطة الاطلاع على معلومات التسجيل لدى الجهات المقدمة لخدمات الإنترنت والاتصالات دون استصدار أمر قضائي[٣٩]. وعلى المستوى الدولي، تنظِّم إتاحة الاطلاع على محتوى بيانات الاتصالات معاهداتٌ ثنائية للمساعدة القانونية المتبادلة. وبالرغم من ذلك، كثيراً ما يجري هذا الشكل من التعاون خارج إطار القانون على أساس الامتثال الطوعي من الجهة المقدمة للخدمات أو شركة الإنترنت. وبذلك، يمكن الاطلاع على بيانات الاتصالات في العديد من الدول دون إذن مستقل وفي ظلّ قدر محدود من الرقابة.

دال- المراقبة القانونية الإضافية

٦٢- يندرج عدد من قدرات المراقبة المذكورة سلفاً خارج الأطر القانونية القائمة، رغم اعتماد الدول لها على نطاق واسع. وتولّد البرامجيات التطفلية الهجومية مثل حصان طروادة، أو قدرات الاعتراض الواسع النطاق، صعوبات خطيرة لمفاهيم المراقبة التقليدية إلى درجة أنه لا يمكن التوفيق بينها وبين قوانين المراقبة والاطلاع على محتوى المعلومات الخاصة. وهي ليست مجرّد أساليب جديدة لإجراء المراقبة، بل أشكال مراقبة جديدة. ويثير استخدام هذه التكنولوجيا، من منظور حقوق الإنسان، إزعاجاً بالغاً. فبرامجيات حصان طروادة، على سبيل المثل، لا تمكّن الدول من الوصول إلى الأجهزة فحسب، بل تمكنها أيضاً من تغيير محتوى معلوماتها - بصورة غير مقصودة أو عن عمد. ولا يقتصر هذا الأمر على تهديد الحق في الخصوصية والحقوق المرتبطة بعدالة الإجراءات فيما يتعلق باللجوء إلى هذه الأدلة في الدعاوى القضائية. ولا تراعي تكنولوجيا الاعتراض الواسع النطاق أي اعتبار للتناسب، بما يمكّن من مراقبة عشوائية، وتمكّن الدولة من استنساخ أي اتصال ورصده في بلد بذاته أو منطقة معينة، دون استصدار إذن للقيام بكل عملية اعتراض.

٦٣- وكثيراً ما لا تعترف الحكومات باستخدام هذه التكنولوجيات لأغراض المراقبة، أو تحاجج بشرعية استخدام هذه التكنولوجيات بموجب تشريعات المراقبة القائمة. وبينما يتضح أن للعديد من الدول برامجيات تطفلية هجومية، مثل تكنولوجيا حصان طروادة، لم يُناقَش علناً في أي دولة، باستثناء ألمانيا أساسُ استخدامها القانوني. وفي هذا السياق، اعتمدت مقاطعة راين - ويستفاليا الشمالية تشريعاً في عام ٢٠٠٦ يأذن "بالاطلاع سراً على محتوى أنظمة تكنولوجيا المعلومات" (المادة ٥-٢ رقم ١١، القانون المتعلق بحماية الدستور، لمقاطعة راين - ويستفاليا الشمالية) الذي يفهم منه أنه اختراق تقني إما عن طريق وضع برنامج تجسس أو الاستفادة من ثغرات النظام الأمنية. وألغت المحكمة الدستورية الاتحادية في ألمانيا القانون في شباط/فبراير ٢٠٠٨، ورأت أن هذه التدابير لن تتسق مع حقوق الإنسان

(٣٩) القانون الاتحادي البرازيلي ٢٠١٢/١٢٦٨٣. المادة ١٧-باء. متاح على العنوان التالي: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm.

إلا إذا خضعت لإذن ومراجعة قضائيين، وأُخذ بها فقط في حالات تتضمن احتمال وجود خطر ملموس يتربص بمصلحة ذات طابع قانوني وأهمية كبيرة[٤٠].

هاء- تطبيق قوانين المراقبة خارج الإقليم

٦٤- استجابة لزيادة تدفق البيانات عبر الحدود وخزن أكثرية الاتصالات لدى أطراف أجنبية ثالثة مقدمة للخدمات، بادرت بعض الدول إلى اعتماد قوانين تمنحها الإذن بإجراء المراقبة خارج الإقليم أو اعتراض اتصالات في إطار ولايات قضائية أجنبية. ويثير ذلك شواغل بالغة تتعلق بانتهاك حقوق الإنسان خارج الإقليم، وعدم قدرة الأفراد على معرفة احتمال تعرضهم لمراقبة أجنبية أو الاعتراض على قرارات تتعلق بمراقبة أجنبية أو التماس سبل الانتصاف. ففي جنوب أفريقيا، على سبيل المثال، يمكّن مشروع تعديل قوانين الاستخبارات العامة من فرض المراقبة على الاتصالات الأجنبية خارج جنوب أفريقيا أو التي تمر عبر أراضيها[٤١]. وفي تشرين الأول/أكتوبر ٢٠١٢، اقترح وزير العدل والأمن في هولندا تعديلات تشريعية على البرلمان تمكّن الشرطة من اختراق الحواسيب والهواتف المحمولة داخل هولندا وخارجها لتثبيت برامجيات تجسس والبحث عن بيانات وإتلافها[٤٢]. وفي كانون الأول/ديسمبر ٢٠١٢، اعتمدت الجمعية الوطنية في باكستان القانون المتعلق بالمحاكمة العادلة لعام ٢٠١٢، الذي ينص في الفقرة ٣١ منه على تنفيذ أوامر المراقبة في ولايات قضائية أجنبية. وفي وقت لاحق من ذلك الشهر، جددت الولايات المتحدة قانون تعديل مراقبة الاستخبارات الأجنبية لعام ٢٠٠٨ بما يوسع سلطة الحكومة في مراقبة غير الأمريكيين المقيمين خارج الولايات المتحدة (المادة ١٨٨١-أ) بما في ذلك أي شخص أجنبي تستضيف اتصالاته الجهات المقدمة للخدمات السحابية الموجودة في الولايات المتحدة (مثل غوغل وغيرها من كبرى شركات الإنترنت)[٤٣]. وفي عام ٢٠١٢ أيضاً، أنشأ المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية مشروع معايير يمكّن الحكومات الأوروبية من اعتراض الخدمات السحابية الأجنبية[٤٤]. وتشير هذه التطورات إلى اتجاه يبعث على الانزعاج نحو توسيع سلطات المراقبة

---

(٤٠) متاح بالألمانية، على العنوان التالي: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 67), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

(٤١) المادة ١-ج. مشروع تعديل قوانين الاستخبارات العامة. متاح على العنوان التالي: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf.

(٤٢) انظر http://www.edri.org/edrigram/number10.20/dutch-proposal-state-spyware.

(٤٣) انظر European Parliament Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, Fighting crime and protecting privacy in the cloud: study, 2012.

(٤٤) Draft ESTI DTR 101 567 Lawful Interception (LI) Vo.1.0 (2012 - 05); Cloud/Virtual Services (CLI). متاح على الموقع التالي: www.3gpp.org.

خارج حدود إقليم الدولة، فيزيد من احتمال إبرام اتفاقات تعاون بين الجهات المكلفة بإنفاذ القوانين ووكالات الأمن التابعة للدولة بما يمكّن من التهرب من القيود القانونية المحلية.

واو- الاحتفاظ الإلزامي بالبيانات

٦٥- تعتمد بعض الدول، من أجل زيادة خزن بيانات الاتصالات التي تتمكن من الاطلاع عليها، قوانين للاحتفاظ الإلزامي بالبيانات تقضي بمطالبة الجهات المقدمة لخدمات الإنترنت والاتصالات السلكية واللاسلكية (تُسمَّى عامة "الجهات المقدمة لخدمات الاتصالات") بجمع وخزن محتوى الاتصالات والمعلومات المتعلقة بأنشطة مستعملي الشبكة بصفة مستمرة. وتمكّن هذه القوانين من تجميع سجلات على مدى الزمن بشأن البريد الإلكتروني للأفراد ورسائلهم وأماكن وجودهم وتفاعلهم مع الأصدقاء والأسرة وما إلى ذلك.

٦٦- وعند إتاحة الجهات السالفة الذكر هذه الخدمات لمستعمليها، فإنها تمنح أجهزة أو شبكات المشتركين عناوين بروتوكول الإنترنت[٤٥] تُغيَّر دورياً. ويمكن استعمال المعلومات المتعلقة بعنوان بروتوكول الإنترنت للتّأكّد من هوية فرد ما وموقعه وتعقب أنشطته على الشبكة. وتجبر قوانين الاحتفاظ الإلزامي بالبيانات الجهات المقدمة لخدمات الاتصال على الاحتفاظ بسجلات تخصيص عناوين بروتوكول الإنترنت لفترة معينة من الوقت، بما يمكّن الدول من تعزيز قدرتها على مطالبة هذه الجهات بالتعرف على هوية فرد ما على أساس تحديد الشخص الذي كان لديه عنواناً معيناً من عناوين بروتوكول الإنترنت في تاريخ وزمن معينين. وتسعى بعض الدول حالياً لإجبار الأطراف الثالثة من مقدمي الخدمات على جمع معلومات لا تجمعها عادةً، والاحتفاظ بها.

٦٧- وتعتبر القوانين الوطنية للاحتفاظ بالبيانات اقتحامية ومكلفة، وتهدد الحق في الخصوصية والحق في حرية التعبير. وبإجبار مقدمي خدمات الاتصالات على إنشاء قواعد بيانات ضخمة للمعلومات عن هوية المتصلين ببعضهم عبر الهاتف أو الإنترنت ومكانهم ومدة الاتصال، والاحتفاظ بهذه المعلومات (لسنوات أحياناً)، تكون قوانين الاحتفاظ الإلزامي بالبيانات قد عززت بصورة كبيرة من نطاق مراقبة الدولة وبالتالي من نطاق خرق حقوق الإنسان. وتتعرض قواعد بيانات الاتصالات للسرقة والاحتيال والكشف عنها بشكل غير مقصود.

زاي- قوانين الكشف عن الهوية

٦٨- تنص القوانين في العديد من الدول على تقديم مستخدم مقاهي الإنترنت بطاقة هويته. وتثير هذه القوانين مشاكل بصورة خاصة في البلدان التي تنخفض فيها نسبة ملكية

(٤٥) عنوان بروتوكول الإنترنت هو شفرة رقمية فريدة تعرّف كل حاسوب أو غيره من الأجهزة المتصلة بشبكة الإنترنت.

الحواسيب ويعتمد الأفراد أساساً على الحواسيب المتاحة للجمهور. وفي الهند، على سبيل المثال، تقضي قواعد عام ٢٠١١ لتكنولوجيا المعلومات (المبادئ التوجيهية لمقاهي الإنترنت) بحصول أصحاب مقاهي الإنترنت على وثائق هوية أي فرد يزور مقهى الإنترنت، والاحتفاظ بهذه السجلات لفترة لا تقل عن سنة (المادة ٤(٢)). ويجب على مقهى الإنترنت أن يحتفظ بسجل يتضمن معلومات منها موعد بداية ونهاية استعمال الحاسوب والتعريف بالحاسوب الطرفي لفترة لا تقل عن سنة (المادة ٥(١) و٥(٢))؛ وخزن النسخ الاحتياطية لسجلات الاستخدام لكل عملية من جانب المستعمل والاحتفاظ بها لفترة لا تقل عن سنة (المادة ٥(٤)).

٦٩- ويُطالَب الأفراد حالياً كذلك باستخدام أسمائهم الحقيقية على الشبكة في العديد من الدول، وتقديم هوية رسمية تُعرِّف بهم. وفي جمهورية كوريا، يقضي قانون المعلومات والاتصالات لعام ٢٠٠٧، بأن يسجل المستعملون أسماءهم الحقيقية قبل دخول المواقع الشبكية التي يزورها أكثر من ١٠٠ ٠٠٠ زائر يومياً، للحد من التحرش وخطاب الكراهية على الشبكة حسب الظاهر. بيد أن المحكمة الدستورية ألغت القانون مؤخراً على أساس تقييده حرية التعبير وتقويضه دعائم الديمقراطية[٤٦]. واعتمدت الصين مؤخراً "قرار تعزيز حماية المعلومات على الشبكة"، الذي يُطالب الجهات المقدمة لخدمات الإنترنت والاتصالات السلكية واللاسلكية بجمع المعلومات الشخصية عن المستعملين عند تسجيل الدخول إلى شبكة الإنترنت أو خطوط الهاتف الثابت أو خدمات الهاتف المحمول. وتُطالَب الجهات المقدمة للخدمات التي تمكّن المستعملين من النشر على الشبكة بأن تكون قادرة على ربط الأسماء المستخدمة على الشاشة بهوية المستعملين الحقيقيين. وتُمكّن شروط تسجيل الأسماء الحقيقية هذه السلطات من تيسير التعرف على المعلقين على الشبكة أو ربط استعمال الهاتف المحمول بشخص معين، بما يقضي على التعبير في كنف الكتمان[٤٧].

٧٠- وتتمثَّل مبادرة أخرى تحول دون إغفال الهوية أثناء الاتصالات في اعتماد تدريجي لسياسات تستوجب تسجيل بطاقات تحديد هوية المشترك باسمه الحقيقي أو بوثيقة هوية صادرة عن الحكومة. وتفيد التقارير بأن القوانين التي تطالب الأفراد، في ٤٨ بلداً في أفريقيا، بتسجيل بياناتهم الشخصية لدى مقدمي خدمة الاشتراك في الشبكة قبل تفعيل بطاقات تحديد هوية المشترك المدفوعة مقدّماً، تيسِّر وضع قواعد بيانات كبيرة تتضمَّن المعلومات المتعلِّقة بالمستخدمين، وتلغي إمكانية إغفال هوية أصحاب الاتصالات، وتمكِّن من تعقُّب المواقع،

---

(٤٦) قرار المحكمة الدستورية 2010Hun-Ma47 (قرار "الأسماء الحقيقية")، المؤرخ ٢٣ آب/أغسطس ٢٠١٢. ويتضمن الموقع الشبكي للمحكمة موجزاً رسمياً لقرارها على العنوان التالي: http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp بالكورية فقط.

(٤٧) "China to Strengthen Internet Information Protection"، متاح على العنوان التالي: http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm.

وتبسّط مراقبة الاتصالات[٤٨]. وفي عدم وجود تشريع لحماية البيانات، يمكن تبادل المعلومات المتعلِّقة بمستعملي بطاقات تحديد هوية المشترك مع الإدارات الحكومية ومقارنتها بغيرها من قواعد البيانات الخاصة والعامة، بما يمكِّن الدولة من إعداد نبذات شاملة عن فرادى المواطنين. وقد يتعرَّض الأفراد أيضاً للاستبعاد من استعمال خدمات الهاتف المحمول (التي لا تمكّن من إجراء اتصالات فحسب بل أيضاً من الوصول إلى خدمات مالية) إذا لم يتمكّنوا من تقديم بطاقة هوية لأغراض التسجيل أو لا يرغبون في ذلك.

حاء- القيود المفروضة على التشفير وقوانين الكشف عن مفتاح التشفير

٧١- إن القوانين التي تحدّ من استخدام أدوات تعزيز الخصوصية التي يمكن اللجوء إليها لحماية الاتصالات، مثل التشفير، تقوِّض أمن الاتصالات وإغفال هوية المتصلين. فقد اعتمدت دول عديدة قوانين تلزم الأفراد بفك الشفرات عند أمرهم بذلك. فقانون جنوب أفريقيا لعام ٢٠٠٢ المتعلِّق بتنظيم اعتراض الاتصالات وتوفير المعلومات المتعلِّقة بها، يقضي بتقديم أي شخص، يملك مفتاح فك التشفير، المساعدة على فكّه[٤٩]. وتوجد قوانين مماثلة في فنلندا (المادة ٤(٤)(أ) من قانون التدابير القسرية ١٩٨٧/٤٥٠)، وبلجيكا (المادة ٩، القانون المتعلِّق بالجرائم الحاسوبية المؤرَّخ ٢٨ تشرين الثاني/نوفمبر ٢٠٠٠)، وأستراليا (المادتان ١٢ و٢٨ من القانون المتعلِّق بالجرائم الحاسوبية لعام ٢٠٠١).

سابعاً- دور القطاع الخاص ومسؤولياته

٧٢- شهد القطاع الخاص في المقام الأول تطوّرات حيوية في مجال التكنولوجيا مكَّنت من ظهور أشكال جديدة ودينامية للاتصالات. وفي هذا الصدد، يستند العديد من التغييرات في الطريقة التي نتواصل بها ونتلقى بها المعلومات وننشرها إلى البحث والابتكار لدى الجهات التابعة للشركات.

٧٣- كما يضطلع القطاع الخاص بدور حيوي في تيسير رقابة الدولة على الأفراد بعدد من الطرائق. وكان على الجهات التابعة للشركات أن تستجيب لشروط تصميم الشبكات الرقمية والهياكل الأساسية للاتصالات بما يمكِّن الدولة من اختراقها. واعتمدت الدول هذه

---

(٤٨) Kevin P. Donovan and Aaron K. Martin, “The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance,” Information Systems and Innovation Group Working Paper Series, no. 186, London School of Economics and Political Science (20012).

(٤٩) المادة ٢٩، قانون جنوب أفريقيا لعام ٢٠٠٢ المتعلِّق بتنظيم اعتراض الاتصالات وتوفير المعلومات المتعلِّقة بها. متاح على العنوان التالي: http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.

الشروط أصلاً في التسعينات فباتت ملزمة لجميع الجهات المقدِّمة لخدمات الاتصالات. ويتزايد اعتماد الدول لتشريعات توجب على هذه الجهات تمكين الدول من الاطّلاع مباشرة على بيانات الاتصالات، أو تغيير الهياكل الأساسية بما ييسِّر الأشكال الجديدة لتدخل الدولة.

٧٤- في سياق عمل الجهات التابعة للشركات على تطوير ونشر تكنولوجيات وأدوات اتصال جديدة بطرائق محدَّدة، تتخذ هذه الجهات أيضاً تدابير طوعية تيسِّر مراقبة الدولة للاتصالات. واتخذ هذا التعاون في أبسط مظاهره شكل قرارات بشأن كيفية جمع الجهات التابعة للشركات المعلومات وتجهيزها، فتصبح لديها مخازن ضخمة للمعلومات الشخصية المتاحة للدول عند طلبها. واعتمدت هذه الجهات مواصفات تمكِّن الدول من الحصول على المعلومات أو التدخل فيها أو جمعها بقدر مفرط ومدلِّل، أو تقييد تطبيق التشفير وغيره من التقنيات التي يمكن أن تحدَّ من حصول كل من الشركات والحكومات على المعلومات. وكثيراً ما لم يعمل القطاع الخاص على نشر تكنولوجيات تعزيز الخصوصية، أو طبق هذه التكنولوجيات بأساليب لا ترقى إلى المستوى المطلوب من الأمن ولا تُعدّ من أحدث المكتشفات.

٧٥- وفي أخطر الظروف، تواطأ القطاع الخاص على تطوير تكنولوجيات تمكِّن من المراقبة الجماعية أو الاقتحامية بما يتعارض مع المعايير القانونية القائمة[٥٠]. وولَّد قطاع الشركات صناعة عالمية تركِّز على تبادل تكنولوجيات المراقبة. وكثيراً ما تُباع هذه التكنولوجيات إلى بلدان يتزايد فيها احتمال استخدامها لانتهاك حقوق الإنسان، ولا سيما حقوق المدافعين عن حقوق الإنسان أو الصحفيين أو غيرهم من الفئات الضعيفة. وتكاد هذه الصناعة لا تخضع للتنظيم بسبب عدم مواكبة الدول التطوّرات التكنولوجية والسياسية.

٧٦- ولا تتضمن التزامات الدول في مجال حقوق الإنسان احترام الحق في حرية التعبير والحق في الخصوصية وتعزيزهما فحسب، بل أيضاً حماية الأفراد من انتهاكات الجهات التابعة للشركات لحقوق الإنسان. وينبغي للدول كذلك أن تمارس الرقابة الكافية للوفاء بالتزاماتها الدولية في مجال حقوق الإنسان عندما تتعاقد مع الجهات المذكورة أو تصدر تشريعات بشأنها، حيثما ينال ذلك من التمتع بحقوق الإنسان[٥١]. وتنطبق التزامات حقوق الإنسان في هذا الصدد عندما تقوم تلك الجهات بأنشطتها في الخارج[٥٢].

---

(٥٠) من بين أمثلة تكنولوجيا المراقبة التي صمّمها القطاع الخاص واستخدمتها كل من ليبيا والبحرين والجمهورية العربية السورية ومصر وتونس، انظر: European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), pp. 9-10.

(٥١) مبادئ توجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون "الحماية والاحترام والانتصاف" إطار العمل، المبدأ ٥.

(٥٢) اللجنة المعنية بحقوق الإنسان، الملاحظات الختامية، ألمانيا، كانون الأول/ديسمبر ٢٠١٢.

٧٧- ويجب على الدول أن تكفل قدرة القطاع الخاص على أداء مهامه بصورة مستقلة وعلى نحو يعزز حقوق الإنسان للأفراد. وفي الوقت نفسه، لا يمكن أن يُسمح للجهات التابعة للشركات بالمشاركة في أنشطة تنتهك حقوق الإنسان، والدول مسؤولة عن مساءلة الشركات في هذا الصدد.

ثامناً- الاستنتاجات والتوصيات

٧٨- تطورت تقنيات الاتصالات وتكنولوجياتها تطوراً كبيراً، وغيّرت الطريقة التي تراقب بها الدول الاتصالات. وعليه، يجب على الدول أن ترتقي بفهمها وتنظيمها لمراقبة الاتصالات وأن تعدل ممارساتها من أجل ضمان احترام حقوق الإنسان للأفراد وحمايتها.

٧٩- ولا يمكن للدول أن تضمن تمكن الأفراد بحرية البحث عن المعلومات وتلقيها أو التعبير عن آرائهم، دون احترام حقهم في الخصوصية وحمايته وتعزيزه. ويترابط هذا الحق مع الحق في حرية التعبير ويعتمد كل منهما على الآخر بصورة متبادلة؛ ويمكن لانتهاك أحدهما أن يكون سبباً لانتهاك الآخر ونتيجة له. وبدون تشريعات ومعايير قانونية مناسبة لضمان خصوصية الاتصالات وأمنها وإغفال هوية أصحابها، لا يمكن للصحفيين والمدافعين عن حقوق الإنسان والمبلغين عن المخالفات، على سبيل المثال، الاطمئنان لعدم تعرض اتصالاتهم للتتبع من الدول.

٨٠- ومن أجل وفاء الدول بالتزاماتها في مجال حقوق الإنسان، يجب عليها أن تضمن إدراج الحق في حرية التعبير والحق في الخصوصية في صميم أطرها لمراقبة الاتصالات. لذلك، يوصي المقرر الخاص بما يلي:

ألف- تحديث القانون والمعايير القانونية وتعزيزها

٨١- ينبغي أن يُنظَر إلى مراقبة الاتصالات كعمل تطفلي بدرجة كبيرة ربما يتعارض مع الحق في حرية التعبير والحق في الخصوصية ويهدد دعائم المجتمع الديمقراطي. ويجب للتشريعات أن تنص على وجوب ألا تقوم الدولة بمراقبة الاتصالات إلا في الظروف الاستثنائية جداً، وأن يكون ذلك حصراً تحت إشراف سلطة قضائية مستقلة. ويجب أن يتضمن القانون ضمانات واضحة عن طبيعة التدابير الممكنة ونطاقها ومدتها، والأسس اللازمة للأمر بها، والسلطات المختصة بالإذن بها وتنفيذها والإشراف عليها، ونوع الانتصاف الذي تتضمنه التشريعات الوطنية.

٨٢- وينبغي أن يكون للأفراد الحق بموجب القانون في إخطارهم بتعرضهم لمراقبة اتصالاتهم، أو باطلاع الدولة على بيانات اتصالاتهم. ومع الإقرار بأن الإخطار المسبق أو المتزامن يمكن أن يهدد فعالية المراقبة، ينبغي أن يُخطر الأفراد رغم ذلك فور إتمام

المراقبة، وأن تُتاح لهم إمكانية السعي للانتصاف من اللجوء إلى تدابير مراقبة اتصالاتهم بعد تنفيذها.

٨٣- وفيما يتعلق بتدابير مراقبة الاتصالات، يجب أن تضمن الأطر القانونية ما يلي:

(أ) أن ينص القانون عليها، وأن تفي بمعياري الوضوح والدقة الكافيين لضمان إخطار الأفراد مسبقاً بها وإمكانية توقعهم تطبيقها؛

(ب) أن تكون ضرورية على نحو محدد وظاهر لتحقيق غرض شرعي؛

(ج) أن تتقيد بمبدأ التناسب وألا تُستخدم عندما تكون التقنيات الأقل اقتحاماً متاحة أو لم تستنفد بعد.

٨٤- وينبغي للدول أن تُجرّم المراقبة غير القانونية من جانب الجهات الفاعلة العامة أو التابعة للقطاع الخاص. ويجب ألا تستخدم هذه القوانين لاستهداف المبلغين عن المخالفات أو غيرهم من الأفراد الذين يسعون للكشف عن انتهاكات حقوق الإنسان، وألا تُعيق رقابة المواطنين المشروعة لنشاط الحكومة.

٨٥- وينبغي أن يخضع توفير القطاع الخاص بيانات الاتصالات إلى الدول للتنظيم الكافي من أجل ضمان إعطاء الأولوية إلى حقوق الإنسان للأفراد دوماً. وينبغي ألا يُلتمس الاطلاع على بيانات الاتصالات الموجودة لدى الجهات المحلية التابعة للشركات إلا في الظروف التي يُستنفد فيها المتاح من التقنيات الأقل اقتحاماً.

٨٦- وينبغي أن تَرصد توفيرَ بيانات الاتصالات إلى الدولة هيئةٌ مستقلة، من قبيل محكمة أو آلية رقابة. وعلى الصعيد الدولي، ينبغي للدول أن تبرم معاهدات المساعدة القانونية المتبادلة لتنظيم الاطلاع على بيانات الاتصالات الموجودة لدى الجهات الأجنبية التابعة للشركات.

٨٧- ويجب أن تخضع للرقابة التشريعية تقنيات وممارسات المراقبة المستخدمة خارج إطار القانون، حيث يقوّض هذا الاستخدام المبادئ الأساسية للديمقراطية ويرجَّح أن تكون له آثار سياسية واجتماعية ضارة.

باء- تيسير الاتصالات الخاصة والمؤمَّنة والمجهولة الهوية

٨٨- ينبغي للدول أن تمتنع عن حمل المستعملين على التعريف بهويتهم كشرط مسبق لإجراء اتصالاتهم، بما في ذلك عن طريق خدمات الإنترنت أو مقاهي الإنترنت أو الهاتف المحمول.

٨٩- وينبغي أن يتمتع الأفراد بحرية استعمال التكنولوجيا التي يختارونها لتأمين اتصالاتهم. وينبغي للدول ألا تتدخل في استخدام تكنولوجيات التشفير وألا تُجبر المستخدم على توفير مفاتيح فك التشفير.

٩٠- وينبغي للدول ألا تحتفظ بمعلومات محددة لأغراض المراقبة البحتة أو أن تطالب بالاحتفاظ بها.

جيم- زيادة إمكانية اطلاع الجمهور على المعلومات وفهم التهديدات للخصوصية والتوعية بها

٩١- ينبغي للدول أن تلتزم الشفافية التامة بشأن استخدام تقنيات وسلطات مراقبة الاتصالات ونطاقها. وينبغي لها أن تنشر، على الأقل، معلومات إجمالية عن عدد الطلبات المقبولة والمرفوضة، ومعلومات مبوَّبة عن الطلبات حسب الجهة المقدِّمة للخدمات وحسب التحقيقات والأغراض.

٩٢- وينبغي للدول أن توفِّر للأفراد ما يكفي من المعلومات لتمكينهم من الاستيعاب الكامل لنطاق القوانين التي تسمح بمراقبة الاتصالات وطبيعة هذه القوانين وتطبيقها. وينبغي للدول أن تمكِّن الجهات المقدِّمة للخدمات من نشر الإجراءات التي تطبِّقها عندما تتعامل مع مراقبة الدولة للاتصالات واحترام هذه الإجراءات، ونشر سجلات مراقبة الدولة للاتصالات.

٩٣- وينبغي للدول أن تنشئ آليات رقابة مستقلة قادرة على ضمان الشفافية والمساءلة بشأن مراقبة الدولة للاتصالات.

٩٤- وينبغي للدول أن تعزز وعي الجمهور باستخدامات التكنولوجيات الجديدة للاتصالات من أجل دعم الأفراد في تقييم المخاطر ذات الصلة بالاتصالات على النحو المناسب وإدارتها والتخفيف من آثارها واتخاذ قرارات مستنيرة بشأنها.

دال- تنظيم الاتجار بتكنولوجيا المراقبة

٩٥- ينبغي للدول أن تضمن اتِّساق بيانات الاتصالات التي تجمعها الجهات التابعة للشركات في توفير خدمات الاتصالات مع أعلى معايير حماية البيانات.

٩٦- ويجب على الدول أن تمتنع عن إجبار القطاع الخاص على تنفيذ تدابير تنال من الخصوصية والأمن وإغفال الهوية في خدمات الاتصالات، بما في ذلك المطالبة بوضع قدرات اعتراض لأغراض مراقبة الدولة أو حظر استخدام التشفير.

٩٧- ويجب على الدول أن تتخذ تدابير تمنع الاتجار بتكنولوجيا المراقبة، وأن تولي عناية خاصة للبحث والتطوير بشأن هذه التكنولوجيات والاتجار بها وتصديرها واستخدامها، نظراً لقدرتها على تيسير انتهاك حقوق الإنسان بصورة منهجية.

هاء- تعزيز تقييم الالتزامات الدولية ذات الصلة في مجال حقوق الإنسان

٩٨- ثمة حاجة ماسة إلى تعزيز الفهم الدولي لحماية الحق في الخصوصية في ضوء التطوُّرات التكنولوجية. وينبغي للجنة المعنية بحقوق الإنسان أن تنظر في إصدار تعليق عام جديد بشأن الحق في الخصوصية، يحلّ محل التعليق العام رقم ١٦(١٩٨٨).

٩٩- وينبغي لآليات حقوق الإنسان أن تعزِّز تقييم التزامات الجهات الفاعلة الخاصة التي تطوِّر تكنولوجيات المراقبة وتورّدها.