الأمم المتحدة

A/HRC/29/32

الجمعية العامة

Distr.: General
22 May 2015
Arabic
Original: English

مجلس حقوق الإنسان

الدورة التاسعة 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، ديفيد كاي*

موجز

يتناول المقرر الخاص، في هذا التقرير المقدّم وفقاً لقرار مجلس حقوق الإنسان ٢/٢٥، مسألة استخدام التشفير وإخفاء الهوية في الاتصالات الرقمية. ويخلص التقرير، استناداً إلى البحوث المتعلقة بالمعايير والسوابق القضائية الدولية والوطنية والمعلومات المقدمة من الدول والمجتمع المدني، إلى أن التشفير وإخفاء الهوية يستحقان حماية قوية لأنهما يمكّنان الأفراد من ممارسة حقهم في حرية الرأي والتعبير في العصر الرقمي.

* تأخر تقديم هذا التقرير.

120615 150615 GE.15-07497 (A)

1507497

المحتويات

أولاً- مقدمة

١- تتيح التكنولوجيات الرقمية المعاصرة لكل من الحكومات والشركات والمجرمين والعابثين قدرات غير مسبوقة على التدخّل في الحقوق المتعلقة بحرية الرأي والتعبير. إن الرقابة على شبكة الإنترنت، والمراقبة وجمع البيانات بشكل جماعي ومحدد الهدف، والهجمات الرقمية على المجتمع المدني، والقمع بسبب التعبير عن الرأي على شبكة الإنترنت، تدفع الأفراد في جميع أنحاء العالم إلى التماس الأمن الذي يمكّنهم من اعتناق آراء دون تدخّل، ومن التماس جميع أنواع المعلومات والأفكار وتلقيها ونقلها. ويسعى الكثيرون إلى حماية أمنهم عن طريق التشفير، وهو عملية تعمية للبيانات بحيث لا يصل إليها إلا المتلقين المستهدفين، ويجوز تطبيق التشفير على البيانات العابرة (مثل البريد الإلكتروني، والرسائل، والاتصال الهاتفي عبر الإنترنت)، وعلى البيانات المخزنة رقمياً على وسائط ثابتة (مثل الأقراص الحاسوبية الصلبة، والخدمات السحابية). ويلتمس آخرون حماية إضافية عن طريق إخفاء الهوية، باستخدام تكنولوجيات متقدمة بهدف عدم الكشف عن هويتهم وبصمتهم الرقمية. ويتيح التشفير وإخفاء الهوية، وهما الوسيلتان المعاصرتان الرئيسيتان لتحقيق الأمن على شبكة الإنترنت، للأفراد حماية خصوصيتهم، مما يمكّنهم من تصفّح الأفكار والمعلومات وقراءتها وإبدائها وتبادلها دون تدخّل، ويمكّن الصحفيين، ومنظمات المجتمع المدني، وأفراد الفئات العرقية والدينية، والأشخاص المضطهدين بسبب ميلهم الجنسي أو هويتهم الجنسانية، والناشطين، والعلماء، والفنانين، وغيرهم، من ممارسة حقوقهم في حرية الرأي والتعبير.

٢- ومع ذلك، فمثلما يمكن استخدام الهاتف في إبلاغ الشرطة بجريمة أو في التآمر على ارتكاب جريمة، يمكن أيضاً إساءة استخدام الإنترنت بالتدخّل في حقوق الآخرين أو في الأمن القومي أو النظام العام. وتؤكد دوائر إنفاذ القانون والاستخبارات أن الاتصالات المخفية الهوية أو المشفرة تجعل من الصعب التحقيق في الجرائم المالية، وعمليات الاتجار بالمخدرات، واستغلال الأطفال في البغاء، والإرهاب. ويعرب الأفراد عن بواعث قلق مشروعة بشأن كيفية استخدام المتسلطين والمجرمين للتكنولوجيات الحديثة في تيسير التحرش. وتقيّد بعض الدول أو تحظر التشفير وإخفاء الهوية على هذه الأسس وعلى أسس أخرى، في حين تقترح دول أخرى أو تتخذ طرقاً أخرى تتيح لجهات إنفاذ القانون التحايل على إجراءات الحماية هذه والوصول إلى اتصالات الأفراد.

٣- وفي ضوء هذه التحديات، يتناول هذا التقرير سؤالين مترابطين. أولاً، هل يحمي الحق في الخصوصية والحق في حرية الرأي والتعبير الاتصال الآمن على الإنترنت، وتحديداً عن طريق التشفير أو إخفاء الهوية؟ وثانياً، إن كانت الإجابة عن هذا السؤال بالإيجاب، إلى أي مدى يجوز للحكومات، وفقاً لقانون حقوق الإنسان، أن تفرض قيوداً على التشفير وإخفاء الهوية؟ ويسعى هذا التقرير إلى الإجابة عن هذين السؤالين، واستعراض أمثلة لممارسات الدول، واقتراح توصيات. ولا يهدف هذا التقرير إلى تناول جميع المسائل التقنية أو القانونية التي تثيرها التكنولوجيات الرقمية، وإنما يحدد المسائل المهمة من أجل تناولها مستقبلاً.

٤- وفي سياق إعداد التقرير، وزّع المقرر الخاص استبياناً على الدول التمس فيه معلومات عن قوانينها ولوائحها وسياساتها وممارساتها المحلية. وفي ١ نيسان/أبريل ٢٠١٥، كانت ١٦ دولة

قد استجابت لهذا الطلب[1]. ووجّه المقرر الخاص دعوة أيضاً للجهات المعنية غير الحكومية لتقديم معلومات، كما عقد اجتماعاً للخبراء في جنيف في آذار/مارس ٢٠١٥. وقد أسهمت الردود المقدمة من الحكومات، والمعلومات المقدمة من أكثر من ٣٠ منظمة من منظمات المجتمع المدني والأفراد، المتاحة على الموقع الشبكي للمكلف بالولاية، إسهاماً كبيراً في إعداد هذا التقرير.

٥- ويرد في الموقع الشبكي للمقرر الخاص استعراض كامل للأنشطة التي اضطلع بها منذ بداية فترة ولايته في آب/أغسطس ٢٠١٤. ويهدف هذا التقرير، وهو أول تقرير للمكلف بالولاية الحالي، إلى مواصلة العمل المتعلق بمواجهة التحديات التي تعترض حرية التعبير في العصر الرقمي.

ثانياً- الاتصال الآمن والخاص في العصر الرقمي

ألف- التشفير وإخفاء الهوية في الوقت الراهن

٦- تستفيد النُهج الحديثة المتعلقة بالاتصال الخاص والآمن من الأفكار التي تبنتها الإنسانية منذ آلاف السنين. وقد بيّن نشوء الحفظ الإلكتروني للبيانات، والإنترنت، وجمع البيانات الجماعية والاحتفاظ بها، الحاجة إلى وسائل معقدة لحماية بيانات الأفراد والشركات والحكومات. ونتيجة لتحوّل كل من البريد الإلكتروني والرسائل النصية الفورية، وعملية نقل الصوت باستخدام الإنترنت، والمؤتمرات الفيديوية، ووسائط الإعلام الاجتماعية، من إطار الخدمات المخصصة إلى أنماط اتصال سائدة وسهلة الرصد، أصبح الأفراد في حاجة إلى التمتع بالأمن على الإنترنت، بحيث يمكنهم التماس المعلومات وتلقيها ونقلها دون التعرّض لخطر القمع أو الكشف أو الرصد أو أي استخدام غير سليم آخر لآرائهم وتعبيرهم.

٧- ويحمي التشفير - وهو "عملية رياضية لتحويل الرسائل أو المعلومات أو البيانات إلى شكل لا يمكن أن يقرأه إلا المتلقي المستهدف"[2] - سرية وسلامة المحتوى من وصول أي طرف ثالث إليه أو تلاعبه به. وأصبح التشفير القوي، الذي كان في يوم من الأيام حكراً على المؤسسات العسكرية ودوائر الاستخبارات، متاحاً الآن للجمهور، ومتاحاً في كثير من الأحيان دون قيود لأغراض تأمين البريد الإلكتروني، والاتصال الصوتي، والصور، والأقراص الحاسوبية الصلبة، وبرامج تصفح الإنترنت. وفي حالة "التشفير بالمفتاح العام"، وهو الشكل السائد لتوفير أمن البيانات العابرة من نقطة انطلاقها إلى نقطة وصولها، يستخدم مُرسل البيانات المفتاح العام للمتلقي في تشفير الرسالة ومرفقاتها، ويستخدم المتلقي مفتاحه الخاص لفك شفرة البيانات ومرفقاتها. وقد يُستخدم التشفير أيضاً لإنشاء توقيعات رقمية للتأكد من مصداقية الوثيقة ومرسلها، وللتثبّت والتحقّق من هوية الخادوم، ولحماية سلامة الاتصالات بين العملاء من العبث أو التلاعب بمسارها من جانب أطراف ثالثة (مثل الهجمات التي يشنها

(١) وردت إجابات من ألمانيا، وأيرلندا، وبلغاريا، وتركيا، وسلوفاكيا، والسويد، وغواتيمالا، وقطر، وكازاخستان، وكوبا، ولبنان، وجمهورية مولدوفا، والنرويج، والنمسا، والولايات المتحدة الأمريكية، واليونان.

(٢) انظر SANS Institute, "History of encryption" (2001).

"شخص وسيط"). ونظراً إلى أن تشفير البيانات العابرة لا يمنع الهجمات على البيانات غير المشفرة في حال حفظها رقمياً في أية نقطة نهائية (ولا يحمي أيضاً أمن مفتاح التشفير الخاص بالشخص)، يمكن للشخص أيضاً تشفير البيانات المحفوظة رقمياً في الحواسيب المحمولة، والأقراص الحاسوبية الصلبة، وأجهزة الخادوم، والأجهزة اللوحية (tablets)، والهواتف المحمولة، وغيرها من الأجهزة. وربما تكون ممارسات الإنترنت أيضاً بصدد التخلي عن النظام المبيّن هنا، وتتجه نحو تكنولوجيا "السرية المتقدمة" أو "البالغة الخصوصية"، حيث يُحتفظ بمفاتيح التشفير لفترة قصيرة جداً، لا سيما لاستخدامات من قبيل الرسائل الفورية.

٨- وينادي البعض ببذل جهود لإضعاف أو تخفيف معايير التشفير، بحيث يُسمح فقط للحكومات بالوصول إلى الاتصالات المشفرة. غير أن التشفير المخفّف لا يمكن إبقاؤه سراً عن الجهات ذات المهارة في كشف واستغلال نقاط ضعفه، سواء أكانت جهات حكومية أم غير حكومية، وسواء أكانت شرعية أم إجرامية. ويبدو أن اختصاصيي التكنولوجيا أجمعوا على أنه لا يمكن إتاحة سبيل وصول خاص للسلطات الحكومية فقط، أو حتى للسلطات المعنية، من حيث المبدأ، بالمصلحة العامة. وفي البيئة التكنولوجية المعاصرة، يؤدي التخفيف المتعمّد لمعايير التشفير، ولو لأغراض يمكن اعتبارها مشروعة، إلى إضعاف أمن الجميع على الإنترنت.

٩- وجدير بالملاحظة أن التشفير يحمي محتوى الاتصالات ولكنه لا يحمي العوامل التي تحدد الهوية، مثل عنوان بروتوكول الإنترنت، المعروف باسم البيانات الوصفية. وقد تجمع أطراف ثالثة معلومات مهمة عن هوية أي شخص عن طريق تحليل البيانات الوصفية إن كان المستخدم لا يستعمل أدوات إخفاء الهوية. ويمثل إخفاء الهوية الشرط اللازم لتجنب الكشف عن هوية الشخص. وقد يتيح إخفاء الهوية، وهو رغبة مشتركة لدى البشر في حجب الهوية عن عامة الناس، للمستخدم مزيداً من الحرية في استكشاف ونقل الأفكار والآراء أكثر مما لو كان يستخدم هويته الحقيقية. وقد يتخذ الأفراد أسماء مستعارة على الإنترنت (أو، مثلاً، بريداً إلكترونياً غير حقيقي أو وسائط تواصل اجتماعية غير حقيقية) لإخفاء هويتهم وصورهم وصوتهم ومكانهم، وما إلى ذلك، غير أن الخصوصية التي يحصلون عليها عن طريق هذه البيانات المستعارة سطحية ويسهل كشفها من جانب الحكومات والأشخاص ذوي الخبرة اللازمة؛ وفي حال عدم استخدام مزيج من أدوات التشفير وإخفاء الهوية، يكون من السهل اكتشاف هويات المستخدمين عن طريق الآثار الرقمية التي يتركونها وراءهم. أما المستخدمون الذين يسعون إلى ضمان التشفير الكامل أو حجب هويتهم (مثل إخفاء عنوان بروتوكول الإنترنت الأصلي) عن الدولة أو لغرض تجنب التدخل الإجرامي، فقد يستخدمون أدوات من قبيل الشبكات الخاصة الافتراضية، والخدمات البديلة، وشبكات وبرمجيات حجب الهوية، وشبكات الربط بين الأقران[٣]. وتنشر شبكة Tor، وهي أداة شهيرة لإخفاء الهوية، أكثر من ٦ ٠٠٠ خادوم حاسوبي غير مركزي في

(٣) ترسل الخدمات البديلة البيانات عن طريق وسيط، أو "خادوم بديل"، يتولى إرسال هذه البيانات نيابة عن المستخدم، وبذلك يحجب بشكل فعال عنوان بروتوكول الإنترنت عن المتلقي المستهدف. وتقوم شبكات الربط بين الأقران بفصل وتخزين البيانات فيما بين أجهزة خادوم مترابطة، ثم تشفّر تلك البيانات المخزنة لكي يتعذر على أي خادوم مركزي التعرف على المعلومات. انظر، مثلاً، Freenet.

العالم من أجل تلقي وترحيل البيانات مرات عديدة بهدف إخفاء المعلومات التي تحدد الهوية عن النقاط النهائية، وبذلك تخفي بقوة هوية مستخدمي الشبكة.

١٠- ومن السمات الرئيسية للعصر الرقمي أن التكنولوجيا تتغير باستمرار لكي تلبي احتياجات المستخدمين. ورغم أن هذا التقرير يشير إلى التكنولوجيات المعاصرة التي تيسر التشفير وإخفاء الهوية، ينطبق التحليل المدرج في التقرير واستنتاجات التقرير بشكل عام على المفاهيم التي تقوم عليها التكنولوجيات المعاصرة، وينبغي أن يكون هذا التحليل والاستنتاجات قابلة للتطبيق كلما حلت تكنولوجيات جديدة محل القديمة.

باء- استخدامات التكنولوجيات

١١- للإنترنت قيمة كبيرة في إعمال حرية الرأي والتعبير، إذ تضخِّم الصوت وتضاعف المعلومات التي هي في متناول كل من يمكنه الوصول إليها. وأصبحت الإنترنت، خلال فترة قصيرة، هي المنتدى العام العالمي المركزي. ومن ثم ينبغي اعتبار الإنترنت المفتوحة والآمنة تندرج ضمن الشروط الأساسية للتمتع بحرية التعبير في عالم اليوم. غير أن شبكة الإنترنت معرضة لتهديد مستمر، وهي فضاء - لا يختلف عن العالم المادي - توجد فيه أيضاً مؤسسات إجرامية، وممارسات قمع محدد الهدف، وتجميع واسع النطاق للبيانات. ولذلك، من الأهمية بمكان أن يلتمس الأفراد طرقاً لتأمين أنفسهم على الإنترنت، وأن توفر الحكومات هذا الأمان بموجب القانون والسياسة العامة، وأن تصمم الشركات الفاعلة وتطور وتسوِّق منتجات وخدمات آمنة بطبيعتها. وهذه المتطلبات ليست جديدة. وقد اعترفت الحكومات، في مستهل العصر الرقمي، بالدور الأساسي الذي يؤديه التشفير في تأمين الاقتصاد العالمي وبأهمية استخدام التشفير أو تشجيع استخدامه لتأمين أرقام الهوية التي تصدرها الحكومات، وبطاقات الائتمان والمعلومات المصرفية، ووثائق ملكية الأعمال التجارية، ولضمان التحقيق في جرائم الإنترنت نفسها[٤].

١٢- ويؤدي التشفير وإخفاء الهوية، مجتمعان أو منفصلان، إلى إنشاء حيز من الخصوصية لحماية الرأي والمعتقد. فهما، مثلاً، يمكِّنان من تبادل الاتصالات الخاصة ويمكنهما أن يحجبا رأياً عن المراقبة الخارجية، ويكتسي ذلك أهمية خاصة في البيئات السياسية والاجتماعية والدينية والقانونية العدائية. وعندما تفرض دول رقابة غير قانونية عن طريق تصفية المعلومات وغيرها من التكنولوجيات، فإن التشفير وإخفاء الهوية قد يمكِّنان الأفراد من التحايل على العقبات، والوصول إلى المعلومات والأفكار دون تدخل من السلطات. ويعتمد الصحفيون والباحثون والمحامون والمجتمع المدني على التشفير وإخفاء الهوية لحماية أنفسهم (ومصادرهم وعملائهم وشركائهم) من المراقبة والمضايقة. وقد تكون القدرة على البحث في الإنترنت، وإبداء الأفكار، والتواصل الآمن هي السبيل الوحيد الذي يمكّن الكثيرين من تداول الجوانب الأساسية للهوية، مثل جنس الشخص أو دينيه أو أصله العرقي أو أصله القومي أو ميله الجنسي. ويعتمد الفنانون

(٤) انظر OECD, *Guidelines for Cryptography Policy* (1997).

على التشفير وإخفاء الهوية لضمان حقهم في التعبير وحمايته، لا سيما في الحالات التي لا تكون فيها الدولة هي فقط من يفرض قيوداً، وإنما أيضاً المجتمع الذي لا يتسامح مع الآراء غير التقليدية أو التعبير غير التقليدي.

١٣- ويبين الجانب "المظلم" للتشفير وإخفاء الهوية أن الأخطاء التي تُرتكب خارج الإنترنت ترتكب أيضاً على الإنترنت. ويعرب المكلفون بإنفاذ القانون ومكافحة الإرهاب عن قلقهم لأن الإرهابيين والمجرمين العاديين يستخدمون التشفير وإخفاء الهوية لإخفاء أنشطتهم، مما يجعل من الصعب على الحكومات أن تمنع الإرهاب وتجارة المخدرات والجريمة المنظمة واستغلال الأطفال في المواد الإباحية، وغير ذلك من أهداف الحكومات، وأن تجري تحقيقات فيها. وقد يعتمد التحرش والتسلط عبر الإنترنت على إخفاء الهوية كقناع جبان للتمييز، لا سيما ضد أفراد الفئات الضعيفة. غير أنه، في الوقت ذاته، كثيراً ما يستخدم المكلفون بإنفاذ القانون الأدوات نفسها لضمان الأمن في تنفيذ عملياتهم السرية، في حين قد يستخدم أفراد الفئات الضعيفة هذه الأدوات لضمان خصوصيتهم في مواجهة التحرش. وعلاوة على ذلك، لدى الحكومات مجموعة واسعة من الأدوات البديلة، مثل التصنت وتحديد المواقع الجغرافية والتتبع والتنقيب عن البيانات والمراقبة المادية التقليدية وأدوات أخرى كثيرة، مما يعزز الجهود المعاصرة لإنفاذ القانون ومكافحة الإرهاب[٥].

ثالثاً- التشفير وإخفاء الهوية والحق في حرية الرأي والتعبير والخصوصية

١٤- الإطار القانوني لحقوق الإنسان، فيما يتعلق بالتشفير وإخفاء الهوية، يتطلب أولاً تقييم نطاق الحقوق المطروحة وتطبيق هذه الحقوق على التشفير وإخفاء الهوية؛ وثانياً، تقييم إمكانية فرض قيود دون سند من القانون على استخدام التكنولوجيات التي تعزز وتحمي الحقوق في الخصوصية وحرية الرأي والتعبير، وتقييم نطاق هذه القيود، إن وُجدت.

١٥- وقُننت الحقوق في الخصوصية[٦] وفي حرية الرأي والتعبير[٧] في الصكوك العالمية والإقليمية لحقوق الإنسان، وفسَّرتها هيئات المعاهدات والمحاكم الإقليمية، وجرى تقييمها من جانب الإجراءات الخاصة التابعة لمجلس حقوق الإنسان وفي إطار الاستعراض الدوري الشامل. وترد المعايير العالمية للحقوق في الخصوصية والرأي والتعبير في العهد الدولي الخاص بالحقوق

(٥) انظر Center for Democracy and Technology, "'Going Dark' versus a 'Golden Age for Surveillance'" (2011).

(٦) المواد التالية تحمي حرية التعبير: المادة ١٢ من الإعلان العالمي لحقوق الإنسان، والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة ١٦ من اتفاقية حقوق الطفل، والمادة ٢٢ من اتفاقية حقوق الأشخاص ذوي الإعاقة، والمادة ١٤ من الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم، والمادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان، والمادة ١١ من الاتفاقية الأمريكية لحقوق الإنسان.

(٧) المواد التالية تحمي حرية التعبير: المادة ١٩ من الإعلان العالمي، والمادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة ٩ من الميثاق الأفريقي لحقوق الإنسان والشعوب، والمادة ١٣ من الاتفاقية الأمريكية لحقوق الإنسان، والمادة ١٠ من الاتفاقية الأوروبية لحقوق الإنسان.

المدنية والسياسية، الذي انضمت إليه ١٦٨ دولة. ويمثل العهد على أقل تقدير، حتى بالنسبة إلى الدول الأخرى غير الملتزمة به، معياراً أدنى للإنجاز وهو في كثير من الأحيان بمثابة معيار قانوني عرفي؛ وتلتزم الدول التي وقعت على العهد دون التصديق عليه باحترام هدفه وغرضه بموجب المادة ١٨ من اتفاقية فيينا لقانون المعاهدات. وتوفر النظم القانونية الوطنية أيضاً الحماية للحقوق في الخصوصية والرأي والتعبير، ويكون ذلك أحياناً عن طريق القانون الدستوري أو الأساسي، أو بتفسيرات للقانون. وقد بيَّن بوضوح عدد من المشاريع العالمية التي ينفذها المجتمع المدني القانون الذي ينبغي تطبيقه في سياق العصر الرقمي، مثل المبادئ الدولية بشأن تطبيق حقوق الإنسان في إطار مراقبة الاتصالات، والمبادئ العالمية بشأن الأمن القومي والحق في المعلومات. ورغم أن المعايير الخاصة قد تتفاوت من حق إلى آخر، أو من صك إلى آخر، فإن القاسم المشترك بين القوانين هو أنه إذا كان الحق في الخصوصية والحق في حرية التعبير عاملين أساسيين في الكرامة الإنسانية والحكم الديمقراطي، فيجب لهذا السبب تحديد القيود بدقة وترسيخها بحكم القانون وتطبيقها بصرامة في الظروف الاستثنائية فقط. وتتطلب حماية هذه الحقوق يقظة خاصة في العصر الرقمي.

ألف- الخصوصية كمدخل إلى حرية الرأي والتعبير

١٦- يوفر التشفير وإخفاء الهوية للأفراد والجماعات حيزاً من الخصوصية على الإنترنت يمكِّنهم من اعتناق الآراء وممارسة حرية التعبير دون تدخلات أو هجمات تعسفية أو غير قانونية. وقد لاحظ المكلف بالولاية السابق "الترابط بين الحق في الخصوصية والحق في حرية التعبير" وتبين له أن التشفير وإخفاء الهوية جديران بالحماية بسبب الدور المهم الذي يمكن أن يؤدياه في تأمين تلك الحقوق (A/HRC/23/40 وCorr.1). وتكفل المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، وهي تجسد المادة ١٢ من الإعلان العالمي لحقوق الإنسان، عدم تعريض أي شخص "على نحو تعسفي أو غير قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته"، ولا "لأي حملات غير قانونية تمس شرفه أو سمعته"، وتنص على أن "من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس". وقد اعترفت الجمعية العامة، ومفوضية الأمم المتحدة السامية لحقوق الإنسان، والمكلفون بولايات في إطار الإجراءات الخاصة بأن الخصوصية مدخل إلى التمتع بالحقوق الأخرى، لا سيما حرية الرأي والتعبير (انظر قرار الجمعية العامة ١٦٧/٦٨، والوثيقة A/HRC/13/37، وقرار مجلس حقوق الإنسان ٨/٢٠).

١٧- وللتشفير وإخفاء الهوية فائدة خاصة في بلورة الآراء والتشارك فيها، وهو ما يحدث في كثير من الأحيان في سياق المراسلات على الإنترنت، مثلاً عبر البريد الإلكتروني، والرسائل النصية، وغير ذلك من أشكال التفاعل على شبكة الإنترنت. ويوفر التشفير الأمن للأشخاص إذ يمكنهم من "التحقق من وصول اتصالاتهم إلى المتلقين المستهدفين فقط، دون تدخل أو تغيير، والتحقق من سلامة الاتصالات التي يتلقونها من أي تدخل" (انظر A/HRC/23/40 وCorr.1، الفقرة ٢٣). وبالنظر إلى القدرة التي ينطوي عليها تحليل البيانات الوصفية في تحديد

"سلوك الشخص، وعلاقاته الاجتماعية، وتفضيلاته الخاصة، وهويته" (انظر A/HRC/27/37، الفقرة ١٩)، قد يؤدي إخفاء الهوية دوراً مهماً في تأمين المراسلات. وإلى جانب المراسلات، فإن الآليات الدولية والإقليمية تفسّر الخصوصية بأنها تتضمن مجموعة من الظروف الأخرى أيضاً[٨].

١٨- ويتعرض الأشخاص والمجتمع المدني للتدخل والهجمات من جانب الدولة والجهات الفاعلة غير الحكومية، وهي أمور قد يوفر التشفير وإخفاء الهوية الحماية منها. وتلتزم الدول، بموجب المادة ١٧(٢) من العهد الدولي الخاص بالحقوق المدنية والسياسية، بحماية الخصوصيات من التدخلات والحملات غير القانونية والتعسفية. وينبغي للدول، بموجب هذا الالتزام الإيجابي، أن تكفل وجود تشريع محلي يحظر التدخلات والاعتداءات غير القانونية والتعسفية التي تستهدف الخصوصية، سواء ارتكبتها الحكومة أو جهات فاعلة غير حكومية. ويجب أن تغطي هذه الحماية الحق في سبيل انتصاف من أي انتهاك للحقوق[٩]. ولكي يكون الحق في سبيل انتصاف مجدياً، يجب إشعار الأشخاص بأي انتقاص في خصوصيتهم، مثلاً في شكل إضعاف التشفير أو الكشف الإجباري عن بيانات المستخدم.

باء- الحق في اعتناق الآراء دون تدخل

١٩- تعترف المادة الأولى من الإعلان العالمي لحقوق الإنسان بأن جميع الناس "وُهبوا العقل والوجدان"، وهو مبدأ بينه بإسهاب قانون حقوق الإنسان ليشمل، ضمن جملة أمور أخرى، حماية الرأي والتعبير والمعتقد والفكر. والمادة ١٩(١) من العهد الدولي الخاص بالحقوق المدنية والسياسية تجسد أيضاً الإعلان العالمي، إذ تنص على أن "لكل إنسان الحق في اعتناق آراء دون مضايقة". وثمة صلة وثيقة بين الرأي والتعبير، إذ إن فرض قيود على الحق في الحصول على المعلومات والأفكار قد يؤثر في القدرة على اعتناق الآراء، كما أن التدخل في اعتناق الآراء يقيد بالضرورة التعبير عن هذه الآراء. غير أن قانون حقوق الإنسان وضع تمييزاً مفاهيمياً بين الرأي والتعبير. ففي إطار المفاوضات المتعلقة بصياغة العهد، "اعتُبرت حرية تكوين الرأي وبلورته، عن طريق الاستدلال المنطقي، أمراً مطلقاً، ولا يجوز تقييد هذه الحرية بموجب القانون أو أية سلطة أخرى، على عكس حرية التعبير"[١٠]. واعتُبرت القدرة على اعتناق رأي ما بحرية عنصراً أساسياً للكرامة الأساسية وتدبير الشؤون الشخصية على نحو ديمقراطي، وهي ضمانة على قدر من الأهمية جعلت العهد يمنع أي تدخل أو تحديد أو تقييد. ومن ثم، فإن القيود المسموح بها في المادة ١٩(٣) تنطبق بشكل صريح على الحق في حرية التعبير فقط، على النحو المنصوص عليه

(٨) اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ١٦(١٩٨٨) بشأن حق الشخص في أن تُحترم خصوصياته وشؤون أسرته وبيته ومراسلاته، وفي التمتع بالحماية اللازمة لشخصه وسمعته. انظر أيضاً (http://www.echr.coe.int/documents/fs_data_eng.pdf) and right to protection of one's image (http://www.echr.coe.int/documents/fs_own_image_eng.pdf).

(٩) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ١٦ والتعليق العام رقم ٣١ بشأن طابع الالتزام القانوني العام المفروض على الدول الأطراف في العهد؛ والوثيقة CCPR/C/106/D/1803/2008.

(١٠) Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

في المادة ١٩(٢). وعلى النقيض من ذلك، فإن التدخل في الحق في اعتناق الآراء يشكل في حد ذاته انتهاكاً للمادة ١٩(١).

٢٠- وقد أولى المعلقون والمحاكم اهتماماً أقل للحق في اعتناق الآراء، بالمقارنة مع الحق في التعبير. غير أن الحق في اعتناق الرأي جدير بمزيد من الاهتمام، نظراً إلى أن آليات اعتناق الرأي تطورت في العصر الرقمي وباتت تعرّض الأشخاص لأوجه ضعف كبيرة. وعادةً ما يعتنق الأشخاص آراءهم في شكل رقمي كما يحفظون آراءهم وتاريخ البحث والتصفح، مثلاً، على الأقراص الحاسوبية الصلبة، وفي السحابة الإلكترونية، وفي ذاكرات البريد الإلكتروني، وهي وسائط عادةً ما تحتفظ بها السلطات الخاصة والعامة لفترات طويلة إن لم يكن إلى أجل غير محدد. وتقوم منظمات المجتمع المدني أيضاً بإعداد وحفظ المذكرات والأوراق والمنشورات بشكل رقمي، وهي جميعاً تنطوي على تكوين آراء واعتناقها. وبعبارة أخرى، لا يُعد اعتناق الآراء في العصر الرقمي مفهوماً مجرداً يقتصر على ما قد يحتفظ به المرء في ذهنه. ومع ذلك، فإن اعتناق الآراء في الحيز الرقمي معرَّض للاعتداء. والتدخل في الحق في اعتناق الرأي خارج الإنترنت قد يشمل التحرش المادي أو الاحتجاز أو السعي لمعاقبة الأشخاص على آرائهم (انظر CCPR/C/78/D/878/1999، المرفق، الفقرات ٢-٥ و٧-٢ و٧-٣). وقد يشمل التدخل أيضاً ممارسات مثل الرقابة المحددة الهدف، وشن هجمات لتعطيل الخدمة، والتخويف والتجريم والتحرش على الإنترنت وخارج الإنترنت. ويشكل التدخل الرقمي المحدد الهدف تحرشاً بالأشخاص ومنظمات المجتمع المدني بسبب الآراء التي يعتنقونها بأشكال متعددة. ومن شأن التشفير وإخفاء الهوية أن يجنب الأشخاص هذا التحرش أو يخفّف منه.

٢١- والحق في اعتناق الآراء دون تدخل يشمل أيضاً الحق في تكوين الآراء. وقد تقوض نظم المراقبة، سواء المحددة الهدف أو الجماعية، الحق في تكوين الرأي، إذ من المرجح أن يؤدي خوف الشخص من الكشف دون رغبته عن النشاط الذي يمارسه على الإنترنت، مثل البحث أو التصفح، إلى العزوف عن الوصول إلى المعلومات، لا سيما إذا كانت هذه المراقبة ستؤدي إلى عواقب قمعية. ولكل هذه الأسباب، يجب تقييم القيود المفروضة على التشفير وإخفاء الهوية من أجل تحديد ما إذا كانت تشكل تدخلاً غير مقبول في الحق في اعتناق الآراء.

جيم- الحق في حرية التعبير

٢٢- الحق في حرية التعبير بموجب المادة ١٩(٢) من العهد الدولي الخاص بالحقوق المدنية والسياسية، يوسع نطاق الضمانة التي يكفلها الإعلان العالمي، وهي حماية "حرية كل إنسان في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى الآخرين، دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني وبأية وسيلة أخرى يختارها". وتؤكد مجموعة كبيرة من السوابق القضائية، وتقارير المكلفين بإجراءات خاصة، وقرارات صادرة عن الأمم المتحدة والنظم الإقليمية لحقوق الإنسان أن حرية التعبير "جوهرية للتمتع بسائر حقوق الإنسان والحريات، ودعامة أساسية لإقامة مجتمع ديمقراطي ولتعزيز الديمقراطية" (قرار مجلس حقوق الإنسان ٢/٢٥). ويؤكد مجلس حقوق الإنسان والجمعية العامة وفرادى الدول، على نحو

منتظم، أهمية تمتع الأشخاص على الإنترنت بالحقوق نفسها التي يتمتعون بها خارج الشبكة[١١]. ولن يكرر هذا التقرير جميع عناصر هذا التوافق في الآراء. وفي سياق التشفير وإخفاء الهوية، يجدر التركيز بشكل خاص على ثلاثة جوانب من النص (انظر الفقرات من ٢٣ إلى ٢٦ أدناه).

٢٣- **حرية التماس المعلومات والأفكار وتلقيها ونقلها:** في البيئات التي تسودها الرقابة، قد يُضطر الأشخاص إلى الاعتماد على التشفير وإخفاء الهوية من أجل التحايل على القيود وممارسة الحق في التماس المعلومات وتلقيها ونقلها. وتستخدم بعض الدول أدوات متنوعة لمنع الوصول إلى المعلومات. فالرقابة التي تفرضها الدولة، مثلاً، تشكل أحياناً عقبات كؤود أمام إعمال الحق في الحصول على المعلومات. وتفرض بعض الدول قيوداً قائمة على المحتوى، وهي قيود تمييزية في كثير من الأحيان، أو تجرِّم التعبير عبر الإنترنت، وتخيف المعارضين السياسيين والمخالفين، وتطبق قوانين للمعاقبة على التشهير والعيب في الذات الملكية، بهدف إسكات الصحفيين والمدافعين والناشطين. وقد يكون استخدام الشبكات الخاصة الافتراضية أو شبكة Tor أو خادوم وكيل، بالإضافة إلى التشفير، هو الطريق الوحيد الذي يمكّن الشخص من الوصول إلى المعلومات وتبادلها في مثل هذه البيئة.

٢٤- ويجدر التشديد على أن قانون حقوق الإنسان يحمي أيضاً الحق في التماس المعلومات والأفكار العلمية وتلقيها ونقلها. ويكفل الإعلان العالمي والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية حماية الحقوق في التعليم وفي "الإسهام في التقدم العلمي وفي الفوائد التي تنجم عنه". وتمكّن تكنولوجيات التشفير وإخفاء الهوية الأفراد من الإسهام في هذه المعلومات في الحالات التي قد يُحرمون فيها من ذلك لولا التشفير وإخفاء الهوية، والتي يكونون فيها هم أنفسهم أمثلة على التقدم العلمي. ومن شأن استخدام هذه التكنولوجيات أن يمكّن الأفراد من قطف ثمار التقدم العلمي الذي قد تقيّده الحكومات. وقد لاحظ المقرر الخاص المعني بالحقوق الثقافية أنه "ينبغي أن يُنظر إلى الحق في العلم والحق في الثقافة باعتبارهما ينطويان على حق المرء في الاستفادة من تكنولوجيا المعلومات والاتصالات وغيرها من أنواع التكنولوجيا واستخدامها بما يمنحه الاستقلالية والتمكين" (انظر A/HRC/20/26، الفقرة ١٩).

٢٥- **عدم التقيد بالحدود الجغرافية:** الصكوك الرئيسية التي تكفل حرية التعبير تعترف صراحةً بأن هذا الحق عابر للحدود. ويتمتع الأفراد بالحق في تلقي جميع أنواع المعلومات والأفكار ونقلها إلى أماكن تتجاوز حدود بلدانهم[١٢]. غير أن بعض الدول تعمد إلى ترشيح أو حجب البيانات باستخدام كلمات مفتاحية، وتمنع الوصول إليها بواسطة تكنولوجيات تعتمد على مطالعة النصوص. ويمكّن التشفير من تجنب ترشيح المعلومات، مما يسمح بتدفق المعلومات

(١١) انظر قرار الجمعية العامة ١٦٧/٦٨، وقرار مجلس حقوق الإنسان ١٣/٢٦، وتوصية اللجنة الوزارية لمجلس أوروبا، CM/REC (2014) إلى الدول الأعضاء بشأن وضع دليل لحقوق الإنسان لمستخدمي الإنترنت.

(١٢) اعترفت المحكمة الأوروبية لحقوق الإنسان بهذه النقطة. انظر See *Ahmet Yildirim* v. *Turkey*,(2012); *Cox* v. *Turkey*, (2010); *Case of Groppera Radio AG and Others* v. *Switzerland* (1990).

عبر الحدود. وعلاوة على ذلك، لا يمكن للأشخاص التحكم في كيفية عبور اتصالاتهم للحدود – ولا يدرون عادة هذه الكيفية – أو ما إذا كانت اتصالاتهم تعبر الحدود أم لا. وقد يحمي التشفير وإخفاء الهوية معلومات جميع الأشخاص أثناء مرورها عبر أجهزة الخادوم الموجودة في بلدان ثالثة تقوم بترشيح المحتوى.

٢٦- **الاستفادة من أي وسيلة أخرى** : صيغت المادة ١٩ من الإعلان العالمي والمادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية بحيث تستوعب أوجه التقدم التكنولوجي مستقبلاً (A/HRC/17/27). واختارت الدول الأطراف في العهد أن تعتمد العبارة العامة "بأي وسيلة أخرى" عوضاً عن تعديد الوسائل القائمة في ذلك الوقت. وانطلاقاً بشكل جزئي من هذا الأساس، اعترفت الآليات الدولية مراراً بأن سبل حماية حرية التعبير تنطبق على الأنشطة الجارية على الإنترنت. كما اعترفت المحاكم الإقليمية بأن سبل الحماية تنطبق على الأنشطة أثناء الاتصال بالإنترنت[١٣]. وقد أشارت المحكمة الأوروبية لحقوق الإنسان، لدى مناقشة السبل المماثلة لحماية التعبير في إطار الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، إلى أن الأشكال والوسائل المستخدمة لنقل المعلومات وتلقيها تتمتع هي نفسها بالحماية، إذ إن أي قيد يُفرض على هذه الوسائل يتدخل بالضرورة في الحق في تلقي المعلومات ونقلها[١٤]. ومن ثم، فإن تكنولوجيات التشفير وإخفاء الهوية تشكل وسائل محددة يمارس الأفراد من خلالها حريتهم في التعبير.

دال- أدوار الشركات

٢٧- تؤدي الشركات في مختلف القطاعات أدواراً في النهوض بالخصوصية وحرية الرأي والتعبير أو في التدخل فيها، بطرق منها التشفير وإخفاء الهوية. وتُنقل الكثير من الاتصالات عبر الإنترنت (وجميع الاتصالات تقريباً في بعض البلدان) بواسطة شبكات تمتلكها وتشغلها شركات خاصة، في حين تمتلك شركات أخرى وتدير مواقع شبكية ذات محتوى كبير يغذيه المستخدمون. وتنشط شركات أخرى في أسواق المراقبة وبرامج التجسس الحاسوبي، إذ توفر أجهزة الحاسوب والبرمجيات للحكومات من أجل اختراق أمن الأفراد على الإنترنت. وتقوم شركات أخرى بإعداد وتقديم خدمات من أجل حفظ البيانات على الإنترنت بشكل آمن وخاص. وتقوم كيانات الاتصالات السلكية واللاسلكية، ومقدمو خدمات الإنترنت، ومحركات البحث، والخدمات السحابية، وشركات فاعلة أخرى عديدة، توصف في كثير من الأحيان بأنها وسيطة، بتعزيز أو تنظيم

(١٣) European Commission of Human Rights, *Neij and Sunde Kolmisoppi* v. *Sweden*, (2013); European Court of Human Rights, *Perrin* v. *United Kingdom*, (2005); African Court on Human and Peoples' Rights, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Meldrum)* v. *Zimbabwe* (2009); *Case of Herrera Ulloa* v. *Costa Rica*, *Herrera Ulloa* v. *Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Series C No. 107, IHRL 1490 (IACHR 2004).

(١٤) انظر *Autronic AG* v. *Switzerland* (1990); *De Haes and Gijsels* v. *Belgium* (1997), para. 48; *News Verlags GmbH and Co.KG v. Austria* (2000).

الخصوصية والتعبير على الإنترنت أو الانتقاص منهما. وقد يحفظ الوسطاء أحجاماً كبيرة من بيانات المستخدمين، التي عادة ما تطلب الحكومات الوصول إليها. وقد تؤدي كل شركة من هذه الشركات الفاعلة دوراً في تعزيز التشفير وإخفاء الهوية أو الانتقاص منهما.

٢٨- ويضيق نطاق هذا التقرير عن العرض الكامل لدور الشركات في حماية أمن مستخدميها على الإنترنت، فهو يركز على واجبات الدولة. ومع ذلك، يجدر التركيز على أن "المسؤولية عن احترام حقوق الإنسان تنطبق على جميع مراحل العمليات العالمية لأية شركة، أياً كان موقع مستخدمي خدمات هذه الشركة، وأن هذه المسؤولية قائمة بشكل مستقل، بغض النظر عن وفاء الدولة بالتزاماتها تجاه حقوق الإنسان أو عدمه "(انظر الوثيقة A/HRC/27/37، الفقرة ٤٣). وعلى أقل تقدير، ينبغي للشركات أن تطبق القواعد المدرجة، مثلاً، في المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان، ومبادئ مبادرة الشبكة العالمية بشأن حرية التعبير والخصوصية، ودليل قطاع تكنولوجيا المعلومات والاتصالات الذي وضعته المفوضية الأوروبية بشأن تنفيذ مبادئ الأمم المتحدة التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان، والمبادئ التوجيهية المتعلقة بحوار قطاع الاتصالات السلكية واللاسلكية، وكلها مبادئ تشجع الشركات على الالتزام بحماية حقوق الإنسان، وعلى بذل العناية الواجبة لضمان التأثير الإيجابي لأعمالها على حقوق الإنسان، وعلى علاج الآثار السلبية لأعمالها على حقوق الإنسان. وسيركز المقرر الخاص، في المستقبل، على الأدوار التي ينبغي أن تؤديها الشركات في حفظ أمن الأفراد بما يمكنهم من ممارسة حرية الرأي والتعبير.

رابعاً- تقييم القيود المتعلقة بالتشفير وإخفاء الهوية

ألف- الإطار القانوني

٢٩- ينبغي الاطلاع بعناية على القيود المسموح بفرضها على الحق في الخصوصية، لا سيما في عصر الرقابة الواسعة النطاق على الإنترنت - سواء أكانت سلبية أم نشطة، جماعية أم محددة الهدف - وبغض النظر عن كون المعايير المطبقة "غير قانونية وتعسفية" بموجب المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، أو "تعسفية" بموجب المادة ١٢ من الإعلان العالمي، أو "تعسفية أو جائرة" بموجب المادة ١١ من الاتفاقية الأمريكية لحقوق الإنسان، أو "ضرورية لأي مجتمع ديمقراطي" بموجب المادة ٨ من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية (انظر الوثيقة A/HRC/13/37، الفقرات من ١٤ إلى ١٩). ولا يجب لعمليات التدخل في الخصوصية، التي تقيد ممارسة حرية الرأي وحرية التعبير، مثل عمليات التدخل المذكورة في هذا التقرير، أن تمس بأي حال من الأحوال الحق في اعتناق الآراء، ويجب أن يُنص في القانون على عمليات التدخل التي تقيد حرية التعبير، وأن تكون هذه العمليات ضرورية ومتناسبة لتحقيق هدف من مجموعة قليلة من الأهداف المشروعة.

٣٠- ولا يمكن فرض أية قيود على الحق في اعتناق الآراء دون تدخل؛ أما القيود المنصوص عليها في المادة ١٩(٣) من العهد فلا تنطبق إلا على التعبير بموجب المادة ١٩(٢). وفي البيئات التي تؤدي فيها آراء الشخص، وإن أُبديت على الإنترنت، إلى رقابة أو مضايقة، قد يؤدي التشفير وإخفاء الهوية إلى التمتع بالخصوصية اللازمة. وقد تؤثر القيود المفروضة على هذه الأدوات الأمنية على قدرة الأشخاص على اعتناق الآراء.

٣١- ويجب أن تمتثل القيود المفروضة على التشفير وإخفاء الهوية، بوصفهما عاملين يمكِّنان من التمتع بالحق في حرية التعبير، للاختبار المعروف الثلاثي الأجزاء، وهو: أن أي تقييد للتعبير يجب أن يُنص عليه في القانون؛ وأن التقييد لا يجوز فرضه إلا على أسس مشروعة (على النحو المدرج في المادة ١٩(٣) من العهد)؛ وأن التقييد يجب أن يمتثل للاختبارات الصارمة المتعلقة بالضرورة والتناسب.

٣٢- أولاً، لكي يكون أي تقييد للتشفير أو إخفاء الهوية "منصوصاً عليه في القانون"، يجب أن يتسم بالدقة والعمومية والشفافية، وأن يتجنب منح السلطات الحكومية سلطة تقديرية غير محددة لتطبيق التقييد (انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٣٤(٢٠١١)). ويجب طرح المقترحات المتعلقة بفرض قيود على التشفير أو إخفاء الهوية للتعليق العام عليها، وألا تُعتمد هذه القيود، إذا حدث ذلك، إلاّ في إطار عملية تشريعية عادية. وينبغي أيضاً تطبيق ضمانات إجرائية وقضائية قوية لكفالة الحق في الإجراءات القانونية الواجبة لأي شخص قُيّد حقه في التشفير أو إخفاء الهوية. وينبغي، تحديداً، أن تشرف محكمة أو هيئة قضائية أو هيئة تحكيم أخرى مستقلة على تطبيق التقييد[١٥].

٣٣- وثانياً، لا يُسوَّغ فرض قيود إلا لحماية مصالح محددة، مثل: حقوق الآخرين أو سمعتهم؛ أو الأمن القومي؛ أو النظام العام؛ أو الصحة العامة؛ أو الأخلاقيات. وحتى عندما تحظر دولة، بموجب القانون، "الدعوة إلى الكراهية القومية أو العرقية أو الدينية التي تشكل تحريضاً على التمييز أو العداوة أو العنف، على النحو المنصوص عليه في المادة ٢٠ من العهد، يجب أن تتوافق أية قيود تُفرض على التعبير مع المادة ١٩(٣) (A/67/357). ولا توجد أسس أخرى تبرر فرض قيود على حرية التعبير. وعلاوة على ذلك، يجب تطبيق القيود نفسها بدقة، لأن الأهداف المشروعة كثيرا ما تستخدم كذريعة لتحقيق أغراض غير مشروعة[١٦].

٣٤- وثالثاً، يجب على الدول تبيان أن فرض أي قيد على التشفير وإخفاء الهوية "ضروري" لتحقيق هدف مشروع[١٧]. وقد استنتجت المحكمة الأوروبية لحقوق الإنسان، على نحو سليم،

---

(١٥) انظر العهد الدولي الخاص بالحقوق المدنية والسياسية، المادة ٢(٣)(ب)؛ والوثيقة CCPR/C/79/Add.110، الفقرة ٢٢؛ ومبادئ جوهانسبرغ بشأن الأمن القومي وحرية التعبير والحصول على المعلومات.

(١٦) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٣٤ بشأن حرية الرأي والتعبير، الفقرة ٣٠، والتعليق العام رقم ٣١.

(١٧) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٣٤، الفقرة ٢، والبلاغ رقم ٢٠١٢/٢١٥٦، الآراء المعتمدة في ١٠ تشرين الأول/أكتوبر ٢٠١٤.

أن كلمة "ضروري" الواردة في المادة ١٠ من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية تعني أن التقييد يجب أن يكون أكثر من "مفيد" أو "معقول" أو "مرغوب"[١٨]. فإذا تحقق الهدف المشروع، لا يجوز استمرار تطبيق التقييد. وبالنظر إلى الحقوق الأساسية المطروحة، لا يجوز فرض القيود إلا من قبل سلطة قضائية مستقلة ونزيهة، لا سيما لحفظ حقوق الأفراد في الإجراءات القانونية الواجبة.

٣٥- وتنطوي الضرورة أيضاً على تقييم مدى تناسب التدابير التي تقيد استخدام الأمن على الإنترنت والحصول عليه[١٩]. وينبغي أن يكفل تقييم التناسب أن يكون التقييد هو "الأداة الأقل تدخلاً من بين الأدوات الأخرى التي يمكن أن تحقق النتيجة المنشودة"[٢٠]. ويجب أن يرمي التقييد إلى تحقيق هدف محدد، لا التدخل دون مبرر في الحقوق الأخرى للأشخاص المستهدفين، كما يجب أن يكون التدخل في حقوق أشخاص آخرين محدوداً وله مبرراته في ضوء المصلحة التي يدعمها التدخل. ويجب أيضاً أن يكون التقييد "متناسباً مع المصلحة التي يُرجى حمايتها"[٢١]. وقد يكون الضرر الشديد الذي من المرجح أن يصيب مصلحة مهمة ومشروعة للدولة هو المبرر لتدخلات محدودة في حرية التعبير. ومن ناحية أخرى، إذا كان للتقييد تأثير واسع النطاق على أفراد لا يشكلون تهديداً لمصلحة مشروعة للحكومة، فإن العبء الملقى على عاتق الدولة لتبرير التقييد سيكون ثقيلاً جداً[٢٢]. وعلاوة على ذلك، يجب أن يُراعى في أي تحليل للتناسب وجود احتمال قوي باستخدام التشفير وإخفاء الهوية من قبل الشبكات الإجرامية أو الإرهابية نفسها التي تهدف القيود إلى ردعها. وعلى أية حال، لا غنى عن تقديم "تبرير عام مفصّل ومدعوم بالأدلة" لكي يمكن إجراء نقاش عام وشفاف بشأن القيود المتعلقة بحرية التعبير والتي من الممكن أن تقوِّضها (انظر الوثيقة A/69/397، الفقرة ١٢).

باء- الممارسة الحكومية: الأمثلة وبواعث القلق

٣٦- تثير الاتجاهات المتعلقة بالأمن والخصوصية على الإنترنت قلقاً بالغاً. فعادة ما تفشل الدول في تقديم مبرر عام لدعم القيود المفروضة. وقد يؤدي تشفير وإخفاء هوية الاتصالات إلى شعور مسؤولي إنفاذ القانون ومكافحة الإرهاب بالإحباط، وهو ما يؤدي أيضاً إلى تعقد عملية المراقبة، غير أن السلطات الحكومية لم تحدد بشكل عام - ولو بعبارات عامة، بسبب الحاجة المحتملة إلى الخصوصية - الحالات التي استلزمت فرض قيود من أجل تحقيق هدف مشروع.

---

(١٨) انظر *Case of The Sunday Times* v. *United Kingdom*, judgement of 26 April 1979, para. 59.

(١٩) انظر African Court Human and Peoples' Rights, *Lohe Issa Konate* v. *Burkina Faso*, application No. 004/2013, paras. 148 and 149 (2014); European Court of Human Rights, *Case of The Sunday Times*, para. 62.

(٢٠) انظر اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٢٧(١٩٩٩) بشأن حرية التنقل، الفقرة ١٤.

(٢١) انظر المرجع نفسه، الفقرة ١٤.

(٢٢) انظر Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134.

وتقلل الدول من قيمة الأدوات التقييدية غير الرقمية في إطار جهود إنفاذ القانون ومكافحة الإرهاب، بما في ذلك التعاون عبر الوطني[٢٣]. ونتيجة لذلك، لا تُتاح للجمهور فرصة تقييم ما إذا كانت القيود المفروضة على أمنه على الإنترنت يمكن تبريرها بأي مكاسب فعلية في الأمن القومي ومنع الجريمة. وغالباً ما تكون الجهود الرامية إلى تقييد التشفير وإخفاء الهوية ردود فعل سريعة لمواجهة الإرهاب، بما في ذلك عندما لا يُدَّعى أن المهاجمين أنفسهم استخدموا التشفير وإخفاء الهوية للتخطيط لاعتداء أو لتنفيذه. وعلاوة على ذلك، عندما يوصف التقييد بأنه يحقق مصلحة مشروعة، فإن العديد من القوانين والسياسات لا تستوفي في كثير من الأحيان معايير الضرورة والتناسب، ويكون لهذه القوانين والسياسات تأثيرات واسعة النطاق وضارة تؤثر في قدرة جميع الأشخاص على ممارسة حقوقهم في الخصوصية وحرية الرأي والتعبير دون قيود.

٣٧- والجدير بالملاحظة أيضاً أن الأمم المتحدة نفسها لا توفر لموظفيها ولا لزائري مواقعها الشبكية أدوات قوية لتأمين اتصالاتهم، مما يجعل من الصعب على الأشخاص المعرضين للخطر الوصول الآمن إلى آليات حقوق الإنسان التابعة للأمم المتحدة على الإنترنت[٢٤].

١- التشفير

٣٨- تسعى بعض الحكومات إلى حماية التشفير أو التشجيع عليه لضمان خصوصية الاتصالات. فمثلاً[٢٥]، يكفل القانون المدني الخاص بالإنترنت في البرازيل، الذي اعتُمد في عام ٢٠١٤، حرمة وسرية اتصالات المستخدمين على الإنترنت، ولا يسمح باستثناءات إلا بأمر من المحكمة. ولا يقيد قانون التجارة الإلكترونية وقانون الاتصالات في النمسا التشفير، وقد نظمت الحكومة حملات توعية عامة لتثقيف الجمهور في مجال الأمن الرقمي. ويشجع القانون واللوائح التنظيمية في اليونان الاستخدام الفعال لأدوات التشفير وإخفاء الهوية. وفي ألمانيا وأيرلندا والنرويج، يُتاح ويُشجع استخدام تكنولوجيات التشفير، ويُعترض على أي محاولات لإضعاف بروتوكولات التشفير. وبالمثل، لا تقيد قوانين السويد وسلوفاكيا استخدام التشفير على الإنترنت. وتشجع الولايات المتحدة الأمريكية على استخدام التشفير، ومن المقرر أن ينظر الكونغرس الأمريكي في قانون أُحيل إليه بشأن أمن البيانات، يحظر على الحكومة أن تلزم الشركات بإضعاف أمن المنتجات أو بوضع تدابير للدخول من الباب الخلفي. وتمول عدة حكومات، منها حكومات السويد وكندا والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية وهولندا والولايات المتحدة، الجهود الرامية إلى التشارك في المعلومات المتعلقة باستخدام

(٢٣) انظر Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015). https://ourinternet-files.s3.amazonaws.com/publications/gcig_social_compact.pdf.

(٢٤) مثلاً، لا يُتاح لموظفي مفوضية الأمم المتحدة السامية لحقوق الإنسان في جنيف إمكانية تشفير البريد الإلكتروني من بداية السلسلة إلى نهايتها، كما أن الموقع الشبكي للمفوضية غير مشفر.

(٢٥) استُمدت أمثلة عديدة من الأمثلة الواردة في هذه الفقرة من معلومات قدمتها الحكومات المعنية.

تكنولوجيات التشفير وإخفاء الهوية والتدريب في هذا المجال من أجل مساعدة الأفراد على تجنب الرقابة وحماية أمنهم على الإنترنت. وبالإضافة إلى ذلك، يجب أن تيسر اللوائح المنظمة للتصدير عملية نقل تكنولوجيات التشفير، كلما أمكن. ورغم أن هذا التقرير لا يجري تقييماً قانونياً شاملاً لجميع النهج الوطنية المتعلقة بالتشفير، فإن هذه العناصر المشار إليها – وهي عدم التقييد أو الحماية الشاملة، واشتراط صدور أوامر من المحكمة لتطبيق أي قيد محدد، وتثقيف الجمهور – تستحق التطبيق على نطاق واسع كوسائل لحماية وتعزيز الحقوق في حرية الرأي والتعبير.

٣٩- ورغم ذلك، عادة ما لا تفي عملية تنظيم التشفير بمعايير حرية التعبير، وذلك من جانبين رئيسيين. أولاً، لم يثبت بشكل عام أن القيود ضرورية لتحقيق مصلحة مشروعة معينة. وهذا هو الحال بشكل خاص بالنظر إلى نطاق وعمق الأدوات الأخرى، مثل العمل التقليدي للشرطة والاستخبارات والتعاون عبر الوطني، وهي الأدوات التي قد تقدم بالفعل معلومات مهمة لإنفاذ قانون معين أو لأغراض أخرى مشروعة. وثانياً، تؤثر هذه القيود بشكل غير متناسب على الحق في حرية الرأي والتعبير الذي يتمتع بها الأشخاص المستهدفون أو عامة السكان.

حظر الاستخدام الفردي للتشفير

٤٠- يؤدي الحظر الكامل للاستخدام الفردي لتكنولوجيا التشفير إلى تقييد غير متناسب لحرية التعبير، إذ يحرم هذا الحظر جميع مستخدمي الإنترنت، في ولاية قانونية معينة، من الحق في تهيئة مساحة خاصة للرأي والتعبير، دون وجود أي ادعاء محدد باستخدام التشفير لأغراض غير قانونية.

٤١- وقد يكون تنظيم عملية التشفير من جانب الدولة مماثلاً للحظر، ومن أمثلة ذلك وضع قواعد (أ) تشترط الحصول على تراخيص لاستخدام التشفير؛ (ب) تحدد معايير تقنية ضعيفة للتشفير؛ (ج) تراقب استيراد وتصدير أدوات التشفير. وتتمكن الدول، عن طريق إخضاع أدوات التشفير إلى معايير معتمدة من الحكومة ومراقبة صادرات وواردات تكنولوجيات التشفير، من إبقاء جوانب الضعف في برمجيات التشفير بحيث يتسنى للحكومات الوصول إلى محتوى الاتصالات. فمثلاً، في الوقت الذي قد يكون فيه القانون في تغير دائم، اشترطت الهند ألا يستخدم مقدمو الخدمات "التشفير الكامل" على شبكاتهم، كما يمنع القانون الأفراد من استخدام تشفير يزيد طوله عن مفتاح التشفير ٤٠ بت الذي يسهل تفكيكه، إلا بعد الحصول على إذن مسبق، ويشترط القانون على أي شخص يستخدم تشفيراً أقوى من ذلك أن يزود الحكومة بنسخة من مفاتيح الشفرة[٢٦]. وتشير التقارير إلى أن أجهزة التشفير في الصين قد يُشترط امتثالها لخوارزميات التشفير المعتمدة من الحكومة والتي لم تخضع من الناحية الأمنية لمراجعة النظراء[٢٧]. وتشترط هيئة الاتصالات في باكستان الموافقة المسبقة قبل استخدام

(٢٦) Government of India, Ministry of Communications and IT, Licence Agreement for Provision of Internet Services, (2007). Available from http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. See especially sect. 2.2 (vii).

(٢٧) انظر، مثلاً، Counter-terrorism Law, art. 15 (initial draft of 8 November 2014). Available from http://chinalawtranslate.com/en/ctldraft/.

الشبكات الخاصة الافتراضية والتشفير[٢٨]. وتشترط كوبا حصول مستخدمي التشفير على إذن من الجهة التنظيمية[٢٩]. وفي إثيوبيا، تحتفظ الحكومة بسلطة وضع معايير تقنية للتشفير، ووضعت مؤخراً نظماً تجرّم تصنيع أو تجميع أو استيراد أي معدات للاتصالات السلكية واللاسلكية دون تصريح[٣٠]. وهذه اللوائح تتدخل بشكل غير جائز في الاستخدام الفردي للتشفير في سياق الاتصالات السلكية واللاسلكية.

إضعاف التشفير على الصعيد الدولي

٤٢- نفذَّت بعض الدول، أو اقترحت تنفيذ، ما يُطلق عليه الدخول من الباب الخلفي في المنتجات المتاحة تجارياً، فتجبر المنتجين على تضمين الأجهزة جوانب ضعف تسمح للسلطات الحكومية بالوصول إلى الاتصالات المشفرة. وقامت بعض الحكومات بتطوير أو شراء أدوات تسمح بهذا الوصول لأغراض المراقبة المحلية[٣١]. ويبدو أن كبار المسؤولين في المملكة المتحدة والولايات المتحدة يطالبون بإتاحة الدخول من الباب الخلفي[٣٢]. وكثيراً ما تدعي الدول التي تدعم هذه التدابير الحاجة إلى وضع إطار قانوني ينظم الدخول من الباب الخلفي، من أجل اعتراض الاتصالات المشفرة. غير أن الحكومات التي تقترح الدخول من الباب الخلفي لم تثبت أن الاستخدام الإجرامي أو الإرهابي للتشفير يشكل عقبة أمام تحقيق أهداف إنفاذ القانون. وعلاوة على ذلك، واستناداً إلى التكنولوجيا القائمة، فإن أوجه القصور المتعمدة تقوِّض دائماً أمن جميع مستخدمي الإنترنت، إذ إن الباب الخلفي، حتى وإن كان الغرض منه هو دخول الحكومة فقط، قد تدخل منه كيانات غير مأذون لها، منها الدول الأخرى أو الجهات الفاعلة غير الحكومة. ونظراً إلى التأثير الواسع النطاق وغير التمييزي للدخول من الباب الخلفي، فإن من شأنه أن يؤثر على جميع مستخدمي الإنترنت بشكل غير متناسب.

٤٣- ويسلِّط النقاش المتعلق بهذه المسألة الضوء على نقطة مهمة هي: أن اشتراط الوصول إلى التشفير من الباب الخلفي، ولو لأغراض مشروعة، يهدد الخصوصية الضرورية للممارسة الحرة للحق في حرية التعبير. وثمة قيود عملية تقيّد الوصول من الباب الخلفي؛ فمن الممكن أن يؤدي استغلال أوجه الضعف المتعمدة إلى تعرض المحتوى المشفر للاعتداء، حتى ولو كان القصد الوحيد من إتاحة الوصول هو السماح للحكومة أو للقضاء بالمراقبة. ومن المؤكد أن الحكومات تواجه معضلة عندما يتعارض التزامها بحماية حرية التعبير مع التزاماتها بمنع انتهاكات الحق في

(٢٨) انظر www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

(٢٩) معلومات مقدمة من كوبا.

(٣٠) انظر Ethiopia Telecom Fraud Offence Proclamation 761/2012, sects. 3–10.

(٣١) انظر Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

(٣٢) انظر كلمة رئيس الوزراء، ديفيد كاميرون، في ١٢ كانون الثاني/يناير ٢٠١٥ أمام مؤتمر حزب المحافظين لجمع تبرعات من أجل الانتخابات العامة لعام ٢٠١٥، والكلمة التي ألقاها أمام مؤسسة بروكنز، بواشنطن العاصمة، جيمس كومي، مدير مكتب التحقيقات الاتحادي، في ١٦ تشرين الأول/أكتوبر ٢٠١٤، بعنوان التزام الصمت: "هل التكنولوجيا والخصوصية وسلامة الجمهور تسير في اتجاه التصادم؟".

الحياة أو السلامة البدنية، اللذين يتعرضان للخطر من جراء الإرهاب وغيره من أشكال السلوك الإجرامي. ومع ذلك، تُتاح للدول سبل أخرى لطلب الكشف عن المعلومات المشفرة، منها الأوامر القضائية. وفي هذه الحالات، يجب على الدول أن تثبت أن القيود العامة على الأمن الذي يوفره التشفير ضرورية ومتناسبة. ويجب على الدول أن تبين، بشكل علني وشفاف، أن السبل الأخرى الأقل تدخلاً غير متاحة أو لم تنجح، وأن تدابير التدخل على نطاق واسع، مثل الأبواب الخلفية، هي فقط التي ستحقق الهدف المشروع. وبغض النظر عن ذلك، فإن التدابير التي تفرض قيوداً قابلة للتطبيق بشكل عام على أعداد كبيرة من الأشخاص، دون تقييم لكل حالة على حدة، ستفشل بشكل شبه مؤكد في الوفاء بمبدأ التناسب.

ضمانات مفاتيح الشفرة

٤٤- يسمح أي نظام لضمان مفاتيح الشفرة بوصول الأفراد إلى الشفرة، ولكن يطلب من المستخدمين إتاحة مفاتيحهم الخاصة بفك الشفرة للحكومة أو لأي "طرف ثالث موثوق به". ورغم ذلك، فإن ضمانات مفاتيح الشفرة تكتنفها أوجه ضعف كبيرة. فمثلاً، يعتمد نظام ضمان مفاتيح الشفرة على نزاهة الشخص أو الإدارة أو النظام، المكلفين بحماية مفاتيح الشفرة الخاصة، وقد تكون قواعد البيانات الرئيسية نفسها معرضة للاعتداء، مما يقوِّض أمن وخصوصية اتصالات أي مستخدم. ويُشار إلى أن نظم ضمانات مفاتيح الشفرة، التي رُفضت (هي ونظام الدخول من الباب الخلفي) بعد نقاش مستفيض في الولايات المتحدة في إطار ما يُسمى حروب التشفير في تسعينات القرن الماضي، باتت الآن مُنفذة في عدد من البلدان واقتُرح تنفيذها في بلدان أخرى. وفي عام ٢٠١١، أقرت تركيا لوائح تطالب مقدمي خدمات التشفير بتقديم نسخ من مفاتيح الشفرة للجهات التنظيمية الحكومية قبل تقديم أدوات التشفير للمستخدمين(٣٣). ومن شأن أوجه الضعف الكامنة في نظم ضمان مفاتيح الشفرة أن تجعل هذه النظم تهديداً خطيراً للأمن في سياق ممارسة حرية التعبير.

الكشف الإجباري عن مفاتيح الشفرة مقابل أوامر فك الشفرة المحددة الهدف

٤٥- في الحالات التي قد تبرر فيها حجج إنفاذ القانون أو الأمن القومي طلبات الوصول إلى الاتصالات، قد يُتاح خياران للسلطات، وهما: الأمر بفك شفرة اتصالات معينة أو، بسبب الافتقار إلى الثقة في أن يمتثل الطرف المستهدَف لأمر فك الشفرة، الكشف عن مفتاح فك الشفرة. وقد يُنظر إلى أوامر فك الشفرة المحددة الهدف باعتبارها أكثر محدودية وأقل احتمالاً في أن تثير شواغل تتعلق بمسألة التناسب، بالمقارنة مع الكشف عن مفتاح الشفرة، إذ تركز هذه الأوامر على اتصالات معينة لا على مجموعة كاملة من اتصالات الشخص المشفرة بمفتاح معين. وعلى النقيض من ذلك، فإن كشف مفتاح الشفرة قد يعرِّض البيانات الخاصة لأكثر مما يقتضيه الوضع(٣٤). وعلاوة على ذلك، عادة ما يدفع الكشف عن مفتاح الشفرة، أو أوامر فك الشفرة،

(٣٣) القانون رقم ٥٦٥١ بشأن تنظيم البث على الإنترنت ومكافحة الجرائم المرتكبة عن طريق البث على الإنترنت.

(٣٤) حث منسق مكافحة الإرهاب لدى المفوضية الأوروبية على النظر في الكشف الإجباري عن مفتاح الشفرة. انظر مجلس الاتحاد الأوروبي، الأمانة العامة، وثيقة اجتماع D1035/15 (٢٠١٥).

الشركات إلى التعاون مع الحكومات، مما يخلق تحديات جسيمة تؤثر على فرادى مستخدمي الإنترنت. وينص القانون في عدد من بلدان أوروبا على الكشف عن مفتاح الشفرة[٣٥]. غير أنه في كلتا الحالتين ينبغي أن تستند هذه الأوامر إلى قانون يُتاح الاطلاع عليه من جانب الجمهور، وأن تكون ذات نطاق محدود وتركز على هدف محدد، وأن تُنفذ تحت إشراف سلطة قضائية مستقلة ونزيهة، لا سيما لحفظ حقوق الأشخاص المستهدفين في الإجراءات القانونية الواجبة، وأن تُعتمد هذه الأوامر عند الضرورة فقط وعند عدم توفر وسائل أخرى أقل تدخلاً. ولا يمكن تبرير هذه التدابير إلا إذا استُخدمت لاستهداف مستخدم محدد أو مستخدمين محددين، مع إخضاعها لإشراف قضائي.

الافتراضات القانونية

٤٦- قد ترى بعض الدول أن مجرد استخدام تكنولوجيات التشفير هو سلوك غير مشروع. فمثلاً، تنم التهم الموجهة إلى كاتبي مدونة Zone 9 في إثيوبيا عن أن مجرد التدريب في مجال أمن الاتصالات دليل على السلوك الإجرامي[٣٦]. ولا تستوفي هذه الافتراضات معايير القيود المسموح بها. وبالمثل، عندما تعاقب الدول منتجي وموزعي الأدوات التي تيسر وصول الناشطين إلى الإنترنت، فإنها تقوِّض بذلك الحقوق في الخصوصية وحرية التعبير.

٢- إخفاء الهوية

٤٧- جرى الاعتراف بأهمية دور إخفاء الهوية في حماية وتعزيز الخصوصية، وحرية التعبير، والمساءلة السياسية، ومشاركة الجمهور، والنقاش[٣٧]. ولا يتناول الإعلان العالمي ولا العهد الدولي الخاص بالحقوق المدنية والسياسية موضوع إخفاء الهوية. وكان قد اقتُرح، أثناء التفاوض بشأن العهد، أن تتضمن المادة ١٩(١) منه العبارة التالية: "لا يُسمح بإخفاء الهوية". غير أن هذا الاقتراح رُفض "لأسباب منها أن إخفاء الهوية قد يكون ضرورياً في بعض الأحيان لحماية المؤلف" وأن "هذه العبارة قد تمنع استخدام الأسماء المستعارة"[٣٨]. وأشار المقرر الخاص المعني بحرية التعبير لدى لجنة البلدان الأمريكية لحقوق الإنسان إلى أن "الحق في حرية الفكر والتعبير والحق في الحياة الخاصة يحميان الخطاب دون الإفصاح عن الهوية، من القيود التي

(٣٥) انظر، مثلاً، United Kingdom, Regulation of Investigatory Powers Act (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure).

(٣٦) انظر http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

(٣٧) انظر، مثلاً، Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134; United States, *McIntyre* v. *Ohio Elections Commission* (1995); Lord Neuberger, speech to RB Conference on the Internet, entitled, "What's a name? Privacy and Anonymous Speech on the Internet" (2014).

(٣٨) Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (1987), pp. 379-80.

تفرضها الحكومات"[٣٩]. وهناك عدة دول لديها تقاليد راسخة في ثقافاتها السياسية تشجع على إخفاء الهوية، غير أن قلة قليلة جداً من الدول توفر الحماية العامة بموجب قوانينها للتعبير دون الإفصاح عن الهوية. وتمارس بعض الدول ضغطاً كبيراً لمنع إخفاء الهوية، سواء على الإنترنت أم خارجها. ومع ذلك، ونظراً إلى أن إخفاء الهوية ييسر اعتناق الآراء والتعبير عنها بصراحة كبيرة عبر الإنترنت، ينبغي للدول أن تحميه وألا تقيد بشكل عام التكنولوجيات المستخدمة لإخفاء الهوية. وتحمي النظم القضائية في عدد من الدول إخفاء الهوية، على الأقل في حالات محدودة. فمثلاً، أبطلت المحكمة العليا في كندا، مؤخراً، إمكانية حصول المستخدم على هوية مخفية على الإنترنت دون إذن قضائي[٤٠]. وأبطلت المحكمة الدستورية لجمهورية كوريا القوانين التي تمنع إخفاء الهوية، باعتبارها قوانين غير دستورية[٤١]. وما زالت المحكمة العليا للولايات المتحدة تحمي الحق في التعبير دون الإفصاح عن الهوية[٤٢]. واعترفت المحكمة الأوروبية لحقوق الإنسان بأهمية إخفاء الهوية في حرية التعبير، ولكنها تسمح بفرض قيود في الحالات التي تقتضي تحقيق أهداف مشروعة.

٤٨- وتعترف بلدان عديدة بمشروعية إخفاء هوية مصادر الصحفيين. وتعترف المحكمة العليا في المكسيك وقانون الإجراءات الجنائية المكسيكي بحق الصحفيين في إخفاء هوية مصادرهم؛ ومع ذلك يتعرض الصحفيون في الواقع لضغوط شديدة[٤٣]. وتكفل دساتير الأرجنتين وإكوادور وباراغواي والبرازيل الحماية الصريحة للمصادر؛ أما أوروغواي وبنما وبيرو والسلفادور وشيلي وفنزويلا (جمهورية - البوليفارية) فتكفل حماية المصادر بموجب القانون[٤٤]. ويحمي دستور موزامبيق المصادر، في حين تسعى أنغولا إلى ذلك بموجب نظامها الأساسي[٤٥]. ووضعت أستراليا وكندا ونيوزيلندا واليابان اختبارات الموازنة القضائية لكل حالة على حدة لتحليل عملية حماية المصادر، وإن كان الضغط الذي يتعرض له الصحفيون قد يقوِّض عمليات الحماية هذه بمرور الوقت[٤٦]. وعادة ما تنتهك الدول إخفاء هوية المصادر في الواقع العملي، حتى وإن كان منصوصاً عليه في القانون.

---

(٣٩) انظر Organization of American States, press release 17/15.

(٤٠) *R.* v. *Spencer* (2014).

(٤١) Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.

(٤٢) *McIntyre* v. *Ohio Elections Commission* (1995), pp. 342 and 343.

(٤٣) انظر new Federal Code of Criminal Procedures, art. 244.

(٤٤) انظر Argentina, Constitution, art. 43; Brazil, Constitution, title II, chap. I, art. 5, XIV; Ecuador, Constitution, art. 20; Paraguay, Constitution, art. 29 (1). See also Chile, Law 19,733; El Salvador, Criminal Procedure Code; Panama, Law 67, art. 21; Peru, Criminal Procedure Code; Uruguay, Law 16.099; Bolivarian Republic of Venezuela, Law for Journalism 4.819, art. 8.

(٤٥) انظر Mozambique, Constitution, art. 48(3); Angola, Press Law 7/06, art. 20(1).

(٤٦) Australia Evidence Amendment (Journalists' Privilege) Act 2007; Canada, Court of Queen's Bench of Alberta, *Wasylyshen* v. *Canadian Broadcasting Corporation* (2005); Japan, Case 2006 (Kyo) No. 19 (2006); New Zealand Evidence Act, sect. 68 (2006).

حظر إخفاء الهوية

٤٩- يتدخل حظر إخفاء الهوية على الإنترنت في الحق في حرية التعبير. فالعديد من الدول تحظره بغض النظر عن أية مصلحة محددة للحكومة. وتحظر المادة ٥ من دستور البرازيل الخطاب دون الإفصاح عن الهوية. وبالمثل، تحظر المادة ٥٧ من دستور جمهورية فنزويلا البوليفارية إخفاء الهوية. وفي عام ٢٠١٣ حظرت فييت نام استخدام الأسماء المستعارة، مما أجبر أصحاب المدونات الشخصية على الإفصاح علناً عن أسمائهم وعناوينهم الحقيقية[٤٧]. وفي عام ٢٠١٢، اشترطت جمهورية إيران الإسلامية تسجيل جميع عناوين بروتوكولات الإنترنت المستخدمة داخل البلد، واشترطت أيضاً أن يسجل مستخدمو مقاهي الإنترنت أسماءهم الحقيقية قبل استخدام الحاسوب[٤٨]. ويشترط قانون إكوادور على المعلقين على المواقع الشبكية، وأصحاب الهواتف المحمولة، التسجيل بأسمائهم الحقيقية[٤٩].

٥٠- واعتمدت دول معينة قوانين تشترط تسجيل الأسماء الحقيقية في أي نشاط على الإنترنت، وهو نوع من حظر إخفاء الهوية. ففي الاتحاد الروسي، يتعين على كاتبي المدونات الذين يقرأ مدوناتهم أكثر من ٣ ٠٠٠ شخص يومياً التسجيل لدى الجهة المنظمة لوسائط الإعلام وإعلان هويتهم بشكل علني، كما يجب على مستخدمي مقاهي الإنترنت تسجيل هويتهم لكي يمكنهم الاتصال بمرافق الاتصال اللاسلكي العامة[٥٠]. وتشير التقارير إلى أن الصين أعلنت قواعد تنظيمية تشترط على مستخدمي الإنترنت تسجيل أسمائهم الحقيقية عند دخول مواقع شبكية معينة، وعدم نشر محتوى يهدد المصالح الوطنية[٥١]. وتشترط جنوب أفريقيا أيضاً تسجيل الأسماء الحقيقية لمستخدمي الإنترنت والهواتف المحمولة[٥٢].

٥١- وبالمثل، عادة ما تشترط الحكومات تسجيل شريحة الاشتراك في الهواتف المحمولة؛ فقد اشترط، مثلاً، نحو ٥٠ بلداً في أفريقيا، أو هي بصدد اشتراط، تسجيل بيانات الهوية الشخصية

---

(٤٧) Human Rights Watch, "Vietnam: new decree punishes press", 23 February, 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19, Comment on Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam (June 2011).

(٤٨) Islamic Republic of Iran, Bill 106, Communication Regulation Authority.

(٤٩) See Ecuador, Organic Law on Communications (2013).

(٥٠) مشروع القانون رقم ٤٢٨٨٨٤-٦ المعدِّل للقانون الاتحادي بشأن المعلومات وتكنولوجيات المعلومات وحماية المعلومات، ولعدد من القوانين التشريعية للاتحاد الروسي بشأن تبسيط تبادل المعلومات باستخدام شبكات المعلومات والاتصال؛ Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi," 8 August 2014.

(٥١) China Copyright and Media, Internet User Account Name Management Regulations, article 5 (2015).

(٥٢) South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2003; see also Electronic Communications and Transactions Act of 2002 (requiring real name registration for service providers).

عند تفعيل شريحة الاشتراك[٥٣]. وتنفذ كولومبيا، منذ عام ٢٠١١، سياسة للتسجيل الإجباري للهواتف المحمولة، كما ربطت بيرو جميع شرائح الاشتراك برقم هوية وطني منذ عام ٢٠١٠[٥٤]. وتنظر بلدان أخرى في اتخاذ سياسات من هذا القبيل. وتقوض هذه السياسات بشكل مباشر إخفاء الهوية، لا سيما لمن يتصلون بشبكة الإنترنت عن طريق التكنولوجيا المحمولة فقط. ومن شأن التسجيل الإجباري لشرائح الاشتراك أن يمكّن الحكومات من مراقبة الأفراد والصحفيين بما يتجاوز أي مصلحة مشروعة للحكومة.

٥٢- وتسعى الدول أيضاً إلى حظر أدوات إخفاء الهوية، مثل شبكة Tor، وأجهزة الخادوم الوكيل، والشبكات الخاصة الافتراضية، وذلك بمنع الوصول إليها. وقد منعت الصين منذ فترة طويلة الوصول إلى شبكة Tor[٥٥]، وتشير التقارير إلى أن المسؤولين في الحكومة الروسية عرضوا أكثر من ١٠٠ ٠٠٠ دولار لشراء التقنيات التي يمكنها أن تحدد هوية مستخدمي شبكة Tor[٥٦]. وبالإضافة إلى ذلك، سعت إثيوبيا[٥٧] وجمهورية إيران الإسلامية[٥٨] وكازاخستان[٥٩] إلى منع الوصول إلى شبكة Tor. ونظراً إلى أن هذه الأدوات قد تكون هي الآليات الوحيدة التي تتيح للأفراد ممارسات حرية الرأي والتعبير بأمان، فينبغي حماية وتعزيز سبل الوصول إليها.

القيود أثناء الاضطرابات العامة

٥٣- يعدّ الخطاب دون الإفصاح عن الهوية ضرورياً للناشطين والمحتجين، غير أن الدول تحاول بانتظام حظر أو اعتراض الاتصالات المجهولة الهوية في أوقات الاحتجاجات. وتهدف هذه المحاولات الرامية إلى التدخل في حرية التعبير تحقيق هدف غير مشروع، هو تقويض الحق في الاحتجاج السلمي المنصوص عليه في الإعلان العالمي وفي العهد الدولي الخاص بالحقوق المدنية والسياسية.

مسؤولية الوسطاء

٥٤- تتجه بعض الدول والمحاكم الإقليمية نحو إلزام مقدمي خدمات الإنترنت ومنتديات التواصل الاجتماعي بمسؤولية تنظيم التعليقات التي يبديها المستخدمون على الإنترنت دون

---

(٥٣) Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration", 3 February 2014.

(٥٤) انظر Colombia, Decree 1630 of 2011; Perú 21, *Los celulares de prepago en la mira*, 27 May 2010.

(٥٥) MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 April 2012.

(٥٦) العرض الأصلي متاح في الموقع http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008.

(٥٧) Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012); see also Article 19, 12 January 2015.

(٥٨) "Phobos", "Iran partially blocks encrypted network traffic", The Tor Blog (10 February 2012).

(٥٩) "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", The Tor Blog (16 February 2012).

الكشف عن هوياتهم. فمثلاً، تشترط إكوادور، في قانونها الأساسي المتعلق بالاتصالات، أن يضع الوسطاء آليات لتسجيل البيانات الشخصية لكي يمكن معرفة هوية ناشري التعليقات. وفي قضية *دلفي ضد إستونيا* (القضية رقم ٠٩/٦٤٥٦٩)، أيدت المحكمة الأوروبية لحقوق الإنسان قانوناً إستونياً يلقي المسؤولية على أحد منتديات التواصل الاجتماعي لنشره بيانات تشهيرية مجهولة الهوية على موقعه. ومن المرجح أن تؤدي هذه المسؤولية الملقاة على عاتق الوسطاء إما إلى سياسات تلزم بتسجيل الاسم الحقيقي، مما يقوض إخفاء الهوية، أو إلى منع النشر تماماً من جانب المواقع الشبكية التي لا يمكنها تنفيذ إجراءات ترشيح المعلومات، مما يضر بوسائط التواصل الاجتماعي الصغيرة والمستقلة. وتتضمن مبادئ مانيلا المتعلقة بمسؤولية الوسطاء، المعتمدة مؤخراً، والتي صاغها تحالف منظمات المجتمع المدني، مجموعة جيدة من المبادئ التوجيهية للدول وللآليات الدولية والإقليمية تهدف إلى حماية التعبير على الإنترنت.

الاحتفاظ بالبيانات

٥٥- السياسات الإلزامية والواسعة النطاق للاحتفاظ بالبيانات تقيّد قدرة الشخص على إخفاء هويته. ومن المؤكد أن قدرة الدول على مطالبة مقدمي الخدمات والاتصالات على الإنترنت بجمع وحفظ سجلات توثق أنشطة جميع المستخدمين على الإنترنت أسفرت عن حصول الدولة على البصمة الرقمية لجميع المستخدمين. وتؤدي قدرة الدولة على جمع وحفظ السجلات الشخصية إلى توسيع إمكانياتها المتعلقة بالمراقبة وتزيد إمكانية سرقة معلومات الأفراد والكشف عنها.

خامساً- الاستنتاجات والتوصيات

٥٦- يوفر التشفير وإخفاء الهوية ومفاهيم الأمن التي يستندان إليها، الخصوصية والأمن الضروريين لممارسة الحق في حرية الرأي والتعبير في العصر الرقمي. وقد يكون هذا الأمن أساسياً لممارسات حقوق أخرى، مثل الحقوق الاقتصادية، والحق في الخصوصية، والإجراءات القانونية الواجبة، وحرية التجمع السلمي وتكوين الجمعيات، والحق في الحياة والسلامة البدنية. ونظراً إلى أهمية التشفير وإخفاء الهوية في إعمال الحق في حرية الرأي والتعبير، يجب أن تكون القيود المفروضة على التشفير وإخفاء الهوية محدودة للغاية وفقاً لمبادئ الشرعية والضرورة والتناسب ومشروعية الهدف. ولذلك يوصي المقرر الخاص بما يلي.

ألف- الدول

٥٧- ينبغي للدول أن تنقح القوانين واللوائح الوطنية القائمة أو أن تضع، حسب الاقتضاء، قوانين ولوائح وطنية لتعزيز وحماية الحق في الخصوصية وحرية الرأي والتعبير. وفيما يتعلق بالتشفير وإخفاء الهوية، ينبغي للدول أن تعتمد سياسات عدم التقييد

أو الحماية الشاملة، وأن تعتمد فرض القيود على أساس كل حالة على حدة وفقاً لمتطلبات الشرعية والضرورة والتناسب ومشروعية الهدف، وأن تشترط صدور أوامر قضائية لفرض أي قيد محدد، وأن تعزز الأمن والخصوصية على الإنترنت عن طريق تثقيف الجمهور.

٥٨- وقد ركزت المناقشات المتعلقة بالتشفير وإخفاء الهوية، في معظم الأحيان، على مسألة إمكانية استخدامهما لأغراض إجرامية مع تفشي الإرهاب. غير أن حالات الطوارئ لا تعفي الدول من واجب ضمان احترام القانون الدولي لحقوق الإنسان. وينبغي أن تخضع المقترحات التشريعية المتعلقة بمراجعة القيود المفروضة على أمن الأفراد على الإنترنت، أو اعتماد قيود من هذا القبيل، لنقاش عام وأن تُعتمد هذه القيود وفقاً لعملية تشريعية عادية وعامة ومستنيرة وشفافة. ويجب على الدول أن تشجع المشاركة الفعالة من جانب مجموعة متنوعة من الجهات الفاعلة في المجتمع المدني والأقليات في ذلك النقاش وتلك العمليات، وأن تتجنب اعتماد تشريعات بموجب إجراءات تشريعية سريعة. وينبغي أن يسلط النقاش العام الضوء على الحماية التي يوفرها التشفير وإخفاء الهوية، لا سيما للفئات الأشد تعرضاً لخطر التدخلات غير القانونية. ويجب لمثل هذا النقاش أن يأخذ بعين الاعتبار أيضاً ضرورة خضوع القيود لاختبارات صارمة: فإذا كانت هذه القيود تتدخل في الحق في اعتناق الآراء، فلا يجب اعتمادها. أما القيود على الخصوصية والتي تحد من حرية التعبير – وهي، لأغراض هذا التقرير، القيود المفروضة على التشفير وإخفاء الهوية – فيجب أن ينص عليها القانون وأن تكون ضرورية ومتناسبة من أجل تحقيق واحد من الأهداف القليلة المشروعة.

٥٩- وينبغي للدول أن تشجع التشفير وإخفاء الهوية القويين. وينبغي للقوانين الوطنية أن تعترف بحرية الأفراد في حماية خصوصية اتصالاتهم الرقمية، باستخدام التكنولوجيا وأدوات التشفير التي تسمح بإخفاء الهوية على الإنترنت. وينبغي أيضاً أن تتضمن التشريعات والقواعد التنظيمية، التي تحمي المدافعين عن حقوق الإنسان والصحفيين، أحكاماً تتيح الوصول إلى التكنولوجيات التي تؤمّن اتصالاتهم وتدعم استخدام هذه التكنولوجيات.

٦٠- وينبغي للدول أيضاً ألا تقيد التشفير وإخفاء الهوية، اللذين ييسران ويتيحان في كثير من الأحيان إعمال الحق في حرية الرأي والتعبير. أما الحظر الشامل فليس ضرورياً ولا متناسباً. وينبغي للدول أن تتجنب جميع التدابير التي تضعف الأمن الذي قد يتمتع به الأفراد على الإنترنت، مثل تدابير الدخول من الباب الخلفي، ومعايير التشفير الضعيفة، وضمانات مفاتيح التشفير. وبالإضافة إلى ذلك، ينبغي للدول أن تحجم عن اشتراط إعلان هوية المستخدمين قبل الوصول إلى الاتصالات الرقمية وخدمات الإنترنت، وألا تشترط على مستخدمي الهواتف المحمولة تسجيل شريحة الاشتراك. وبالمثل، ينبغي

للشركات الفاعلة أن تنظر في سياساتها التي تقيد التشفير وإخفاء الهوية (بما في ذلك استخدام الأسماء المستعارة). ولا يجوز السماح بفك الشفرة بحكم من المحكمة، بموجب القانون المحلي أو الدولي، إلا إذا استند الحكم إلى قوانين شفافة ومتاحة للجمهور وطُبق فقط على أفراد مستهدفين وعلى أساس كل حالة على حدة (أي لا على مجموعة كبيرة من الأفراد) وبموجب أمر قضائي، وكفل حماية حقوق الأفراد في الإجراءات القانونية الواجبة.

باء- المنظمات الدولية والقطاع الخاص والمجتمع المدني

٦١- ينبغي للدول والمنظمات الدولية والشركات ومنظمات المجتمع المدني أن تعزز الأمن على الإنترنت. وبالنظر إلى أهمية تكنولوجيات الاتصال الجديدة في تعزيز حقوق الإنسان وتحقيق التنمية، ينبغي لجميع الأطراف ذات الصلة أن تعزز بشكل منهجي الوصول إلى التشفير وإخفاء الهوية دون تمييز. ويناشد المقرر الخاص بشكل عاجل كيانات منظومة الأمم المتحدة، لا سيما الكيانات المعنية بحقوق الإنسان والحماية الإنسانية، أن تدعم استخدام الأدوات التي تحقق أمن الاتصالات، وذلك لتوفير الأمن لمن يتعاملون مع هذه الكيانات. ويجب على كيانات الأمم المتحدة أن تراجع ممارساتها وأدواتها المتعلقة بالاتصالات، وأن تستثمر موارد في تحسين أمن وسرية أصحاب المصلحة المتعددين لدى تفاعلهم مع المنظمة عن طريق الاتصالات الرقمية. ويجب على آليات حماية حقوق الإنسان أن تبذل عناية خاصة عند طلبها وإدارتها للمعلومات الواردة من منظمات المجتمع المدني ومن الشهود على انتهاكات حقوق الإنسان وضحاياها.

٦٢- وفي حين لا يخلص هذا التقرير إلى نتائج بشأن مسؤولية الشركات عن أمن الاتصالات، فإن من الواضح أن الشركات الفاعلة ينبغي لها، نظراً إلى التهديدات المحدقة بحرية التعبير على الإنترنت، أن تنظر في مدى ملاءمة ممارساتها فيما يتعلق بمعايير حقوق الإنسان. وينبغي للشركات، على أقل تقدير، أن تلتزم بالقواعد المدرجة في المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان، ومبادئ مبادرة الشبكة العالمية بشأن حرية التعبير والخصوصية، ودليل المفوضية لقطاع تكنولوجيا المعلومات والاتصالات بشأن تنفيذ مبادئ الأمم المتحدة التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان، والمبادئ التوجيهية المتعلقة بحوار قطاع الاتصالات السلكية واللاسلكية. وينبغي للشركات، على غرار الدول، أن تحجم عن منع أو تقييد نقل الاتصالات المشفرة، وأن تسمح بالاتصالات دون كشف الهوية. ويجب إيلاء اهتمام للجهود المبذولة لزيادة إتاحة الروابط المشفرة لمراكز البيانات، ودعم التكنولوجيات الآمنة للمواقع الشبكية، وكفالة التشفير التلقائي على نطاق واسع من بداية السلسلة إلى نهايتها. وينبغي للشركات الفاعلة الموردة للتكنولوجيا التي تقوض التشفير وإخفاء الهوية أن تتحلى بشفافية خاصة فيما يتعلق بمنتجاتها وعملائها.

٦٣- وينبغي تشجيع استخدام أدوات التشفير وإخفاء الهوية وتحسين الثقافة الرقمية. واعترافاً بأن قيمة أدوات التشفير وإخفاء الهوية تقوم على اعتماد استخدامها على نطاق واسع، يشجع المقرر الخاص الدول ومنظمات المجتمع المدني والشركات على المشاركة في حملة تدعو إلى إتاحة التشفير في تصميم الأجهزة وبشكل تلقائي للمستخدمين في جميع أنحاء العالم، وضمان تزويد المستخدمين المعرضين للخطر، عند الضرورة، بالأدوات التي تمكّنهم من ممارسة حقهم في حرية الرأي والتعبير في مناخ آمن.