الأمم المتحدة
A/HRC/41/35
الجمعية العامة
Distr.: General
28 May 2019
Arabic
Original: English

**مجلس حقوق الإنسان**
**الدورة الحادية والأربعون**
٢٤ حزيران/يونيه – ١٢ تموز/يوليه ٢٠١٩
البند ٣ من جدول الأعمال
**تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية**

# المراقبة وحقوق الإنسان

## تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير*

موجز

تبيَّن أن مراقبة الأفراد – ومعظمهم من الصحفيين والنشطاء والشخصيات المعارضة والنقاد وغيرهم ممن يمارسون حقهم في حرية التعبير – تؤدي إلى الاحتجاز التعسفي، وأحياناً للتعذيب وربما الإعدام خارج نطاق القانون. وقد فشت ممارسة هذه المراقبة في ظل ضعف الضوابط التي تخضع لها صادرات التكنولوجيا وعمليات نقلها إلى الحكومات المعروفة بسياساتها القمعية. وفي هذا التقرير، يبدأ المقرر الخاص بتحديد مشكلة المراقبة المحددة الأهداف من منظور الالتزامات التي يفرضها القانون الدولي لحقوق الإنسان على الدول والمسؤوليات ذات الصلة الواقعة على الشركات. ثم يقترح إطاراً قانونياً وسياساتياً لوضع القواعد التنظيمية وتحقيق المساءلة والشفافية داخل قطاع المراقبة الخاص. ويختتم المقرر الخاص تقريره بالدعوة إلى تشديد القواعد الخاصة بتنظيم صادرات معدات المراقبة والقيود المفروضة على استخدامها، فضلاً عن الدعوة إلى وقف فوري لبيع ونقل أدوات المراقبة الخاصة على الصعيد العالمي ريثما توضع ضمانات قوية لحقوق الإنسان تتيح ضبط هذه الممارسات وكفالة استخدام الحكومات والجهات الفاعلة من غير الدول لهذه الأدوات بالطرق الشرعية.

* قُدم هذا التقرير بعد انقضاء الموعد النهائي لتضمينه أحدث المعلومات.

# المحتويات

# أولاً- مقدمة

١- أدانت الجمعية العامة مراقبة الاتصالات واعتراضها على نحو غير قانوني أو تعسفي واعتبرت ذلك "أعمالاً تدخلية بدرجة كبيرة" تمس بحقوق الإنسان الأساسية (انظر قراريْ الجمعية العامة ١٦٧/٦٨ و١٩٩/٧١). ومع ذلك، تستمر ممارسة المراقبة غير القانونية بدون أن تكون هناك قيود واضحة. وتسرد الورقات المقدمة في إطار إعداد هذا التقرير تفاصيل حالة تلو الأخرى لحكومات تستخدم برمجيات مراقبة عملت شركات خاصة على تطويرها وتسويقها وتقديم خدمات الدعم اللازمة. وقد تبيَّن أن مراقبة الأفراد - ومعظمهم من الصحفيين والنشطاء والشخصيات المعارضة والنقاد وغيرهم ممن يمارسون حقهم في حرية التعبير - تؤدي إلى الاحتجاز التعسفي، وأحياناً للتعذيب وربما الإعدام خارج نطاق القانون. وفشت ممارسة هذه المراقبة في ظل ضعف الضوابط التي تخضع لها صادرات التكنولوجيا وعمليات نقلها إلى الحكومات المعروفة بسياساتها القمعية. وتحاط هذه السوق بالسرية؛ ويعود الفضل في علمنا بهذه المشكلة أساساً إلى عمل الأدلة العدلية الرقمية الذي اضطلع به باحثون غير حكوميين وما أعدته منظمات المجتمع المدني من تقارير مُحكَمة وإلى وسائط الإعلام.

٢- وتبلغ هذه المشكلة من الخطورة حداً استدعى من المقرر الخاص اختتام هذا التقرير بالدعوة إلى تشديد القواعد الخاصة بتنظيم صادرات معدات المراقبة والقيود المفروضة على استخدامها، وكذلك إلى وقف فوري لبيع ونقل الأدوات التي ينتجها قطاع المراقبة الخاص على الصعيد العالمي ريثما توضع ضمانات قوية لحقوق الإنسان تتيح ضبط هذه الممارسات وكفالة استخدام الحكومات والجهات الفاعلة من غير الدول لهذه الأدوات بالطرق الشرعية.

٣- ويقترح المقرر الخاص إطاراً قانونياً وسياساتياً لوضع القواعد التنظيمية وتحقيق المساءلة والشفافية داخل قطاع المراقبة الخاص. ويستهل تقريره بتحديد المشكلة، فيركز على المراقبة المحددة الأهداف، ويترك جانباً مسألة الاعتراض الجماعي للاتصالات، وجمع البيانات الخاصة والاحتفاظ بها (يشار إليها غالباً بعبارة "المراقبة الجماعية"). ثم يسلط الضوء على الالتزامات التي يفرضها القانون الدولي لحقوق الإنسان على الدول والمسؤوليات ذات الصلة الواقعة على الشركات. ويقترح في الجزء الرابع، إطاراً لتحسين القوانين والسياسات المعمول بها عن طريق تضمينها حماية الحق في حرية الرأي والحق في حرية التعبير، استناداً إلى القانون الدولي لحقوق الإنسان الساري. ويختتم التقرير بتقديم توصيات للجهات الفاعلة الرئيسية.

٤- واستُفيد في إعداد هذا التقرير من ١١ ورقة مقدمة من الدول و٣٣ ورقة مقدمة من منظمات المجتمع المدني. ونظمت المفوضية السامية لحقوق الإنسان مشاورة لمدة يومين مع الخبراء في بانكوك في كانون الأول/ديسمبر ٢٠١٨. ويرد في إضافة لهذا التقرير، ملخصُ الورقات المقدمة والمشاورة المعقودة[(١)].

(١) أود أن أخص بالشكر آموس توه، وديزيري موراي، وكريستينا بوتوايو، وماثيو ماركولي وكيولي بارك من مركز العدالة الدولية، في جامعة كاليفورنيا، كلية الحقوق في إيرفين، لما قدموه من مساعدة في إعداد هذا التقرير وإضافته.

## ثانياً- الحكومات وقطاع المراقبة الخاص

٥- إننا نعيش زماناً فيه أدوات المراقبة الرقمية متاحة بيسر ويسهل إساءة استخدامها ويصعب كشفها. وقد رأى المكلف السابق بالولاية، السيد فرانك لا رو، في التقرير الرائد الذي قدمه عن المراقبة في عام ٢٠١٣، أن ضعف البيئة التنظيمية وفَّر أرضية خصبة لتعديات طالت الحق في الخصوصية والحق في حرية الرأي والحق في التعبير على نحو تعسفي وغير قانوني (A/HRC/23/40، الفقرة ٣). ورأى المفوض السامية لحقوق الإنسان في التقرير الافتتاحي الذي قدمه في العام التالي بشأن موضوع الخصوصية في العصر الرقمي، أن الممارسات المتبعة في العديد من الدول تنطوي على قصور في التشريعات الوطنية و/أو تدابير الإنفاذ، وضعف الضمانات الإجرائية، وعدم فعالية الرقابة، وكل ذلك أسهم في انعدام المساءلة عن ممارسة المراقبة الرقمية على نحو غير قانوني (A/HRC/27/37، الفقرة ٤٧).

٦- وتلجأ بعض الدول إلى تطوير أدوات المراقبة المحددة الأهداف في إطار الوكالات والإدارات التابعة لها، في حين يوظف البعض الآخر ما لديه من المنتجات ''الجاهزة'' من برمجيات الجريمة، وتشتري دول أخرى أنواعاً تجارية متطورة من برمجيات التجسس الحاسوبي من سوق معدات المراقبة الدولي[٢]. وأكثر ما يهمُّ المقرر الخاص في هذا التقرير هو الفئة الأخيرة من هذه الأدوات. فالمراقبة الرقمية لم تعد حكراً على البلدان التي تملك الموارد اللازمة لممارسة المراقبة الجماعية والمحددة الأهداف بالاعتماد على أدوات داخلية. فقد دخل قطاع المراقبة الخاص هذا المضمار ليعمل بدون إشراف وفي مأمن من العقاب أو يكاد. وتفيد المنظمة الدولية لحماية الخصوصية بأن عدد الشركات التي طورت هذه المنتجات وسوقتها وباعتها لمشترين حكوميين بلغ أكثر من خمسمائة شركة في عام ٢٠١٦[٣].

## أنواع المراقبة التي ينظر فيها هذا التقرير

٧- في هذا التقرير، يولي المقرر الخاص اهتمامه، في المقام الأول، للتكنولوجيات التي تمكن جهة ما من الوصول خلسةً إلى الاتصالات الرقمية، والعمل المنتج، وبيانات التصفح والبحوث وسجل الأماكن ونشاط الأفراد على شبكة الإنترنت وخارجها. وفيما يلي بيان أهم تكنولوجيات وممارسات المراقبة المحددة الأهداف.

### التدخل في نظام الحاسوب

٨- قد تتيح تكنولوجيات المراقبة للمتطفل إمكانية الوصول إلى حاسوب الشخص أو شبكته الخاصة. ويمارس هذا النوع من التدخل على نطاق واسع[٤]. ففي عام ٢٠١٧ على سبيل المثال، نظرت إحدى محاكم الاستئناف في الولايات المتحدة الأمريكية في قضية مراقبة

(٢) Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society* (Toronto, Monk School of Global Affairs, University of Toronto, 2014), Executive Summary, pp. 8–11.

(٣) الورقة المقدَّمة من المنظمة الدولية لحماية الخصوصية، ص.١.

(٤) انظر، على سبيل المثال، Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto, Signal, 2013), pp. 186–190.

أراضي الولايات المتحدة برعاية دولة أجنبية[٥]. وتتعلق القضية بمُواطن من الولايات المتحدة ولد في إثيوبيا ويعيش في ولاية ماريلاند كان يقدم المساعدة التقنية إلى أفراد الجالية الإثيوبية في المهجر. واستُخدمت وثيقة أرسلت في الأصل إلى هذا الناشط من موظفين في الحكومة الإثيوبية لزرع برامجيات خبيثة تطفلية في نظام حاسوبه، وهي عبارة عن برنامج يعرف باسم FinSpy تسوقه شركة ألمانية – بريطانية اسمها مجموعة شركات جاما[٦]. ويزعم أن برنامج FinSpy سجل مكالمات الفيديو التي أجراها هذا الرجل وأسرته عبر الإنترنت، والرسائل الإلكترونية وغير ذلك من الرسائل، بما في ذلك عن طريق تسجيل نقراته على لوحة المفاتيح وإرسال البيانات إلى خواديم يقع مقرها في إثيوبيا[٧].

### الاختراق الحاسوبي للأجهزة المحمولة

٩- تتيح منتجات المراقبة الخاصة أيضاً إمكانية الاختراق الحاسوبي للأجهزة المحمولة على نحو مباشر. ويعد برنامج بيغاسوس للتجسس الحاسوبي، الذي تنتجه مجموعة شركات NSO، مثالاً نموذجياً واستخدامه المزعوم في المكسيك ينبئ عن الكثير. فمنذ عام ٢٠١٥، تلقى العديد من الأشخاص الذين أبلغوا عن الفساد وتجارة المخدرات رسائلَ نصية أو روابط إلكترونية على أجهزتهم المحمولة، وورد بعضها من مصادرَ تبدو قانونيةً مما يدل على وجود معرفة تفصيلية بالأهداف. وتلقى هذه الرسائل صحفيون وسياسيون ومحققون تابعون لمنظمة الأمم المتحدة ومدافعون عن حقوق الإنسان وجهات أخرى. واكتشفت منظمة كندية تعنى بإجراء البحوث والدعوة، تعرف باسم "مختبر المواطن"، أن الروابط الإلكترونية المرسلة زرَعت في الأجهزة برنامج بيغاسوس للتجسس الحاسوبي مما سمح برصد تحركات الأشخاص المستهدفين عن بعد. وكشفت منظمة "مختبر المواطن" عن استخدام برنامج بيغاسوس للتجسس الحاسوبي كأداة مراقبة لاستهداف الأشخاص في ٤٥ بلداً، بما فيها البحرين، المملكة العربية السعودية وتوغو والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية والولايات المتحدة[٨].

### الهندسة الاجتماعية

١٠- يُشفع استخدام العديد من التكنولوجيات التي تقدَّم وصفُها باستراتيجيات لاستدراج هدف من الأهداف إلى تنزيل برامجيات خبيثة على جهازه دون قصد منه. فرسائل البريد الإلكتروني، التي تتضمن روابط إلكترونية خبيثة، مثلاً، تلجأ إما إلى انتحال هوية جهة من جهات الاتصال لدى الهدف أو إلى إيهامه بأنه ينقر على رابط إلكتروني حميد ذي صلة بعمله أو بنشاطه الدعوي أو بشؤونه الشخصية. وعلى سبيل المثال، أُرسلت على تطبيق واتساب رسالةٌ نصية، وصلها باحثون ببرنامج بيغاسوس للتجسس الحاسوبي إلى موظف في منظمة العفو

---

(٥) *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017).

(٦) وللاطلاع على المواد الترويجية لبرنامج FinSpy، انظر منظمة ويكيليكس، Wikileaks, "The spy files: remote monitoring and infection solutions: FINSPY".

(٧) للاطلاع على تفاصيل الادعاءات، انظر الشكوى الأولى المعدلة، قضية *Doe v. Federal Democratic Republic of Ethiopia*، (١٨ تموز/يوليه ٢٠١٤).

(٨) انظر تقرير بيل ماركتزاك وآخرين، "لعبة الغمّيضة: تتبع عمليات برنامج بيغاسوس من شركة NSO في ٤٥ بلدا"، مختبر المواطن، ١٨ أيلول/سبتمبر ٢٠١٨.

الدولية لحثه على تغطية حركة احتجاج، وتضمنت الرسالة رابطاً إلكترونياً زُعم أنه يفضي إلى معلومات إضافية[٩]. وكان من المرجح أن يؤدي النقر على هذا الرابط إلى تنزيل برنامج التجسس الحاسوبي على جهازه.

### مراقبة الشبكات

١١- تعمل بعض التكنولوجيات على شبكة من الشبكات لإتاحة إمكانية المراقبة المحددة الأهداف. فالنظام الروسي لأنشطة التحقيق التنفيذية على سبيل المثال، يقوم على تركيب جهاز في شبكات الاتصالات يتيح إمكانية اعتراض الاتصالات. ويتولى القطاع الخاص تصنيع هذا النظام وتسويقه، وهو يُستخدم على نطاق واسع في الاتحاد الروسي وفي أماكن أبعد في آسيا الوسطى. وتصنع شركة Protei مثلاً، معدات تضمن اشتغال التكنولوجيات التي يستخدمها النظام الروسي، مثل أدوات التنصت واعتراض الإنترنت، في بلدان مثل أوزبكستان وكازاخستان[١٠].

### التعرُّف على الوجوه والعواطف

١٢- تسعى تكنولوجيا التعرُّف على الوجوه إلى التقاط سمات الوجه لدى أي شخص والتعرُّف على هذه السمات، عن طريق تصنيف محتمل للأفراد على أساس الانتماء الإثني أو العرقي أو الأصل القومي، ونوع الجنس وغير ذلك من السمات، وهي غالباً ما تشكل أساساً للتمييز غير القانوني[١١]. أما تكنولوجيا التعرُّف على العواطف، فتسعى إلى استنباط مشاعر الشخص أو انفعالاته أو نواياه من تعابير الوجه، بالاعتماد على نظم تصنيف مريبة إلى حد كبير[١٢]. ولعله ما من بيئة أفضل من الصين لتجسيد التطفل الشمولي الذي تنطوي عليه هذه التكنولوجيات. وتشير تقارير موثوقة إلى أن حكومة الصين تجمع بين استخدام تكنولوجيا التعرف على الوجوه وكاميرات المراقبة في جميع أنحاء البلد "بحثاً عن الويغور دون غيرهم معتمدة في ذلك على سحنتهم وتحتفظ بسجلات تحركاتهم لأغراض الاستقصاء والفحص"[١٣]. ويبدو أن جزءاً كبيراً من التكنولوجيا التي تستخدمها الحكومة قد صنع محلياً على يد الشركات المملوكة للدولة والشركات الخاصة على حد سواء[١٤].

---

(٩) انظر Bill Marczak, John Scott-Railton and Ron Deibert, "NSO Group infrastructure linked to targeting of Amnesty International and Saudi dissident"، مختبر المواطن، ٣١ تموز/يوليه ٢٠١٨.

(١٠) Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York, PublicAffairs, 2015), pp. 190–191.

(١١) انظر، مثلاً، الورقة المقدمة من مركز "مختبر الإنترنت" (Internet Lab)؛ ص. ٦. والورقة المقدمة من "مركز الإنترنت والمجتمع"، ص. ١٢.

(١٢) معهد "الذكاء الاصطناعي الآن" (AI Now)، *تقرير المعهد لعام ٢٠١٨* (نيويورك، جامعة نيويورك، ٢٠١٨)، الصفحتان ١٣-١٤.

(١٣) انظر Paul Mozur, "One month, 500,000 face scans: how China is using A.I. to profile a minority", *New York Times*, 14 April 2019.

(١٤) الورقة المقدمة من منظمة "حقوق الإنسان في الصين"، الصفحتان ٢ و٣. وانظر أيضاً الوثيقة A/HRC/39/29، الفقرة ١٤.

### مصائد رقم التعريف العالمي للمشتركين في اتصالات الهاتف المحمول (ستينغراي)

١٣- تحاكي مصائد رقم التعريف العالمي للمشتركين في اتصالات الهاتف المحمول الأبراجَ الخلوية المجاورة لاعتراض الاتصالات وبيانات الموقع التي تبثها أجهزة الاتصال الشخصية. وتستخدم هذه المصائد على نطاق واسع في جميع أنحاء العالم، وغالباً ما تستخدمها وكالات إنفاذ القانون والاستخبارات. ويُزعم أن شركة خاصة في المملكة المتحدة باعت هذه المصائد وغيرها من برامج التجسس الحاسوبي إلى الفلبين، ويخشى كثيرون من أن تُستخدم هذه الأدوات في تتبع متعاطي المخدرات ورصدهم في إطار حرب الحكومة على المخدرات التي لاقت انتقاداً واسعاً[١٥].

### التفتيش العميق في رزم الرسائل

١٤- تتيح تقنية التفتيش العميق في رزم البيانات إمكانية رصد حركة مرور البيانات عبر شبكات الاتصالات والإنترنت وتحليلها وإعادة توجيهها. ويمكن استخدامها أيضاً لإعادة توجيه المستخدمين إلى مواقع زرعت بها برامجيات خبيثة ومنعهم من الوصول إلى مواقع معينة. وتفيد التقارير بأن هذه الأجهزة رُكِّبت على شبكة شركة الاتصالات التركية "ترك تيليكوم"، واستخدمت في إعادة توجيه المستخدمين في تركيا والجمهورية العربية السورية لتنزيل برمجيات التجسس الحاسوبي لدى محاولتهم تنزيل تطبيقات برامجيات مشروعة[١٦].

## التعاون بين القطاعين العام والخاص

١٥- تتعاون الحكومات تعاوناً وثيقاً مع القطاع الخاص في سوق أدوات المراقبة الرقمية. فالحكومات لديها متطلبات قد لا تملك إداراتها ووكالاتها القدرة على تلبيتها. والشركات الخاصة لديها ما يلزم من حوافز وخبرة وموارد لتلبية تلك الاحتياجات. وهما يلتقيان في المعارض التجارية العالمية والإقليمية التي يقصد من ورائها جمعهما معاً كما هو الحال في خدمات المواعدة[١٧]. ومن تلك اللحظة يقرران ما إذا تحقق الانسجام بينهما. ومن غير المعروف ما إذا كانت الشركات تبذل نوعاً من العناية الواجبة في تقييم سجل المشترين في مجال حقوق الإنسان.

١٦- وقد تكون نوايا البائع مشروعة. فربما تروم الشركات حقاً أن تستخدم السلطات العامة المُخولة منتجاتِها لأغراض "الاعتراض القانوني" ضد أهداف مشروعة بإذن من الجهات القضائية أو من جهات فاعلة أخرى مستقلة. ولكن لا سبيل إلى التأكد من ذلك لأن كل جانب من جوانب هذا التعاون – من بذل العناية الواجبة والمبيعات إلى تقديم خدمات الدعم للمستعمل النهائي – يتسم عادةً بممارسة الرقابة والشفافية في نطاق محدود. وقد جُمعت جميع المعلومات المتاحة للجمهور عن قطاع صناعة المراقبة الخاص بالاعتماد على عمل الأدلة العدلية

(١٥) انظر Sofia Tomacruz, "You think your data, communication devices are safe? Think again", Rappler, 17 March 2018.

(١٦) انظر، بيل مارتشاك وآخرون، "أجهزة ساندفين باكيت لوجيك استُخدمت لنشر برامج التجسس الحكومية في تركيا وإعادة توجيه المستخدمين المصريين إلى الإعلانات التابعة لها"؟ مختبر المواطن، ٩ آذار/مارس ٢٠١٨.

(١٧) انظر على سبيل المثال www.issworldtraining.com؛ وPatrick Howell O'Neill, "ISS World: the traveling spyware roadshow for dictatorships and democracies", Cyberscoop, 20 June 2017.

الذي اضطلعت به منظمات غير حكومية ومؤسسات أكاديمية، مثل "مختبر المواطن" والتقارير الاستقصائية[١٨].

١٧- وتكتنف ضبابية شديدة سير العمل فيما يطلق عليه "سوق نقاط الضعف". ويعرف عن الحكومات والجهات الفاعلة في القطاع الخاص شراؤها نقاط الضعف الأمنية الموجودة في البرمجيات المتاحة عموماً من الباحثين الأمنيين من أجل استخدامها كأداة "استغلال نقاط الضعف دون انتظار" لغرض الاطلاع على اتصالات الأفراد والوصول إلى أجهزتهم[١٩]. وما دامت نقاط الضعف غير معلومة بالنسبة للشركة التي صنعت الجهاز أو البرمجيات، يمكن استخدامها كنقطة دخول للمراقبة. وحين لا تكشف الحكومات والشركات نقاط الضعف هذه، فإنها تعرض أمن المستعملين النهائيين للخطر، بما في ذلك الحكومة وعملاء القطاع الخاص الذين يخزّنون بيانات حساسة تتعلق بالأمور المالية أو الصحية أو العمل أو بإنفاذ القانون في قواعد بيانات تجارية. ولم يُتَّفق حتى الآن، على مسألة مدى وجود مسؤولية على الحكومات والشركات تقتضي منها تقاسم ما لديها من معلومات عن نقاط الضعف، ولا يخضع بيع نقاط الضعف هذه لأي تنظيم. والواقع أن هذا الوضع سهل نشوء سوق ثمينة لنقاط الضعف فضلاً عن أنه جعل العديد من الحكومات والشركات تحرص بشدة على الاحتفاظ بما لديها من معلومات عن نقاط الضعف على أمل استخدامها لأغراض هجومية[٢٠].

١٨- ومن الواضح أيضاً أن التعاون بين القطاعين العام والخاص لا ينتهي عند بيع المنتج وإرساله. فقد أثبتت وثائق مسربة أن شركات المراقبة الخاصة توفر خدمات الدعم بعد البيع. ففي عام ٢٠١٤ مثلاً، قيل إن الشركة المصنعة لمنتجات FinFisher أبرمت "عقداً [عقوداً] سنوياً [سنوية] لتقديم خدمات الدعم" مع عملاء من الحكومات لإدخال تحديثات وتحسينات تقنية على المنتجات وغير ذلك من أشكال دعم العملاء[٢١]. وهي تنظم أيضاً تدريباً على كيفية استخدام برامجياتها الخبيثة بأكفأ صورة للإضرار بالاتصالات الرقمية وأجهزة الكمبيوتر وشبكات الاتصال اللاسلكي التابعة للأهداف المراقَبة[٢٢].

١٩- ومثلما تقيم الشركات روابط وثيقة مع المشترين، تنسج على نفس المنوال روابط مع حكومات البلدان التي تقيم فيها مقرها. ويكون لبعض الشركات صوت مسموع فيما يخص أنظمة مراقبة الصادرات المعتمدة في بلدانها وقد قوضت الجهود الرامية إلى تعزيز هذه الأنظمة. ففي عام ٢٠١٦ على سبيل المثال، أشارت ادعاءات موثوقة إلى أن بعض أشكال تكنولوجيا

(١٨) توضح أخبار المراقبة الخاصة أيضاً تلك الأهمية البالغة التي يكتسيها دور البحوث ووسائط الإعلام الحرة والمستقلة. فهذه التحقيقات جعلت المحققين بدورهم عرضة لخطر المراقبة. انظر على سبيل المثال، Raphael Satter, "Undercover agents target cybersecurity watchdog", Associated Press, 26 January 2019.

(١٩) انظر Privacy International, "Exploiting privacy: surveillance companies pushing zero-day exploits", 7 February 2018.

(٢٠) انظر المناقشة الواردة في الورقة المقدمة من سارة ماكون، الصفحات ٢-٤؛ و Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges* (Brussels, June 2018)؛ و Sven Herpig and Ari Schwartz, "The future of vulnerabilities equities processes around the world", Lawfare, 4 January 2019.

(٢١) انظر Privacy International, "Six things we know from the latest FinFisher documents", 15 August 2014.

(٢٢) المرجع نفسه

المراقبة أزيلت من قائمة الإضافات التي اقتُرح إدراجها في قائمة الاتحاد الأوروبي للسلع والتكنولوجيات ذات الاستخدام المزدوج التي تخضع لمراقبة الصادرات، وذلك بسبب ضغوط مارستها جماعات الضغط التي تمثل مصالح قطاع الصناعة[٢٣]. وخلال المفاوضات التي جرت مؤخراً بشأن نظام مراقبة الصادرات الخاص بالاتحاد الأوروبي، زُعم أن المصالح التجارية كان لها أثرٌ في قرار الحد كثيراً من إدراج ضمانات حقوق الإنسان في التغييرات التنظيمية المقترحة، على الرغم من الاتفاق الواسع على اعتمادها في البرلمان الأوروبي[٢٤].

٢٠- وذكرت التقارير الأخيرة أن العديد من الأشخاص الذين اكتسبوا الخبرة والتجربة في العمل الاستخباري وإنفاذ القانون يتنقلون من وظيفة إلى أخرى في القطاعين الحكومي والخاص. وهذا الباب الدوار يمكن أن يتيح لخبراء حكوميين سابقين تقديم الدعم للجهات الفاعلة في القطاع الخاص التي قد تُستخدم أدواتها في انتهاك حقوق الإنسان[٢٥]. وقد كشفت وكالة رويترز في تقرير صادر في عام ٢٠١٩ عن انتقال عدد من الموظفين السابقين في وكالة الأمن القومي في الولايات المتحدة إلى شركة خاصة لدعم برامج جهاز استخبارات الإشارة في الإمارات العربية المتحدة تحت الاسم الرمزي "مشروع ريفين"[٢٦]. ويُزعم أن الموظفين المعنيين استخدموا خبرتهم في مراقبة المعارضين السياسيين للسلطات في الإمارات العربية المتحدة واستهداف مواطني الولايات المتحدة. ويبدو التنظيم الحكومي لظاهرة "الباب الدوار" في قطاع المراقبة الخاص ضعيفاً في أحسن الأحوال ومنعدماً على الأرجح في العديد من النظم القانونية إن لم يكن أغلبها.

## ثالثاً- الإطار القانوني

### ألف- التزامات الدول

٢١- يتعرض الأشخاص المستهدفون بالمراقبة للتدخل في حقهم في الخصوصية وحقهم في حرية الرأي والتعبير بغض النظر عن نجاح أو إخفاق جهود الرصد[٢٧]. فليس ضرورياً أن يعلم الشخص المستهدف بنجاح محاولة التطفل أو إخفاقها لكي يتمَّ التدخل في حقه في الخصوصية. وتسعى الحكومات عموماً إلى اقتناء الأدوات التي تتيح التطفل على الشخص المستهدف بدون أن يعلم بذلك. ولكن من الأهمية بمكان أن يُنظر إلى هذا التدخل على أنه جزءٌ من مجهود شامل يرمي إلى

(٢٣) نظر Reporters Without Borders, “International regulations: broken or blocked by lobbies”, 14 March 2017.

(٢٤) انظر Daniel Moßbrucker, “Surveillance exports: how EU Member States are compromising new human rights standards”, netzpolitik.org, 29 October 2018.

(٢٥) انظر Privacy International, “Switching hats: why South Africa’s surveillance industry needs scrutiny”, 14 December 2016؛ وتقرير أليكس كين، "كيف أصبحت إسرائيل مركزاً محورياً لتكنولوجيا المراقبة؟" مجلة The Intercept، ١٧ تشرين الأول/أكتوبر ٢٠١٦.

(٢٦) انظر تقرير كريستوفر بينج وجويل شيتمان، "كواليس فريق اختراق إلكتروني من الأمريكيين تجسَّسَ لحساب الإمارات"، رويترز، ٣٠ كانون الثاني/يناير ٢٠١٩؛ و Robert Chesney, “Project Raven: what happens when U.S. personnel serve a foreign intelligence agency”, Lawfare, 11 February 2019؛ والورقة المقدمة من سارة ماكون، الصفحتان ٧ و٨.

(٢٧) الورقة المقدمة من مركز العدالة العالمية، كلية الحقوق في جامعة نيويورك، ص. ٦.

أن تكون له عواقب على الشخص المستهدف. وحين تنفذ محاولة المراقبة – وتنجح العملية – لتحقيق أغراض غير مشروعة، فإنها قد تُستغل في تكميم المعارضين أو معاقبة المنتقدين أو تأديب معدي التقارير المستقلة (والمصادر التي استُند إليها في إعدادها)[٢٨]. وقد لا تفرض الجزاءات على الأشخاص المستهدفين بل على شبكات جهات الاتصال التي لديهم. وفي البيئات التي تتفشى فيها المراقبة غير المشروعة، تكون الجماعات المستهدفة على علم بهذه المحاولات أو تشتبه في وجودها، وهذا يرسم بدوره حدود قدرتها على ممارسة حقوقها في حرية التعبير وتكوين الجمعيات والمعتقد الديني والثقافة وما إلى ذلك، ويحدُّ من هذه القدرة. ومجمل القول إن القصد من التدخل في الخصوصية من خلال المراقبة المحددة الأهداف هو قمع ممارسة الحق في حرية التعبير.

٢٢- ولا ضرورة لتكرار ما ورد في التقارير العديدة المتعلقة بحقوق الإنسان التي قدمت بالفعل من مقررين خاصين سابقين ومكلفين آخرين بولايات ومن المفوضة السامية ومجلس حقوق الإنسان واللجنة المعنية بحقوق الإنسان وغيرها، وهي تقارير سلَّطوا فيها الضوء على السمات الرئيسية للإطار القانوني لحقوق الإنسان الذي يحمي من التعرُّض للمراقبة المحددة الأهداف.

٢٣- ويشار أولاً، إلى أن العهد الدولي الخاص بالحقوق المدنية والسياسية والإعلان العالمي لحقوق الإنسان ينصان على حماية حقوق كل فرد في الخصوصية وحرية الرأي والتعبير. فالمادة ١٩ في كلا الصكين تنصُّ على حماية حق كل شخص في اعتناق الآراء دون مضايقة، وفي التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين بأية وسيلة ودونما اعتبار للحدود. وتكرر المادة ١٧(١) من العهد ما ورد في المادة ١٢ من الإعلان فتنُص على أنه "لا يجوز تعريضُ أي شخص، على نحو تعسفي أو غير قانوني، للتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته".

٢٤- وهناك تشابكٌ بين الخصوصية والتعبير في العصر الرقمي، حيث تعد الخصوصية على شبكة الإنترنت مدخلاً لضمان ممارسة حرية الرأي والتعبير (A/HRC/29/32؛ وCAT/A/HRC/23/40، الفقرة ٢٤). ولا تجيز المادة ١٧ إجراءات التدخل في الحق في الخصوصية إلا إذا كان "يسمح بها القانون المحلي الذي ينبغي أن يكون متاحاً ودقيقاً ويتماشى مع أحكام العهد"، وكان "لها هدف مشروع" و"تستوفي معايير الضرورة والتناسب" (A/69/397، الفقرة ٣٠). وتبين المادة ١٩ معياراً ثلاثياً يقتضي أن تكون القيود منصوصاً عليها في القانون وأن تكون ضرورية لحماية حقوق الآخرين أو سمعتهم، أو حماية الأمن القومي أو النظام العام، أو الصحة العامة أو الآداب العامة[٢٩]. وأكدت اللجنة المعنية بحقوق الإنسان أن المقصود بهذه المبادئ، في الحد الأدنى، هو ما يلي:

(أ) أن تكون القيود محددة بنص القانون/شرعية: يجب أن تصاغ أي قيود بدقة كافية لكي يتسنى للفرد ضبط سلوكه وفقاً لها ويجب إتاحتها لعامة الجمهور. ولا يجوز أن تكون

(٢٨) انظر الورقة المقدمة من مؤسسة حقوق الإنسان.

(٢٩) يرد شرحٌ مفصل للمعيار الثلاثي المنصوص عليه في المادة ١٩ في تعليق لجنة المعنية بحقوق الإنسان العام رقم ٣٤(٢٠١١) بشأن حرية الرأي وحرية التعبير، الفقرات ٥-٩ و٢٢-٣٦؛ والوثيقة A/HRC/38/35.

أي قيود تفرض مبهمة أو واسعة على نحو مفرط إلى حد يمكن أن يمنح الأشخاص المسؤولين عن تنفيذها سلطة تقديرية مطلقة[٣٠]؛

(ب) توخي الضرورة والتناسب: تتحمل الدولة عبء إثبات وجود صلة مباشرة وواضحة بين التعبير والتهديد، وإثبات أن القيود التي تريد فرضها هي أقل الوسائل تطفلاً مقارنة بغيرها من الوسائل التي يمكن أن تحقق نفس الوظيفة الحمائية[٣١]؛

(ج) المشروعية: تضع المادة ١٩(٣) حدوداً معينة للمصالح التي تبرر فرض القيود. ومن الشائع أن تسعى الدول إلى تبرير القيود التي تفرضها، ولا سيما المراقبة المحددة الأهداف، بالاستناد إلى الأمن الوطني، ولكن المقرر الخاص رأى أنه ينبغي أن يقتصر التذرع بهذا الأساس المنطقي على الحالات التي تكون فيها مصالح الأمة بأسرها على المحك، وبذلك تُستبعد القيود التي تخدم حصراً مصلحة حكومة أو نظام أو جماعة نافذة (A/71/373، الفقرة ١٨).

٢٥- وقد طبقت اللجنة المعنية بحقوق الإنسان هذه المبادئ في الملاحظات الختامية التي قدمتها في عام ٢٠١٧ بشأن التقرير الدوري السادس لإيطاليا بموجب العهد الدولي الخاص بالحقوق المدنية والسياسية (CCPR/C/ITA/CO/6، الفقرة ٣٦). وقضت بأن الحق في الخصوصية يتطلب إرساء نظم رقابية محكمة ومستقلة فيما يتعلق بمراقبة الاتصالات واعتراضها وممارسة الاختراق الحاسوبي، وذلك بسبل منها كفالة إشراك السلطة القضائية في ترخيص هذه التدابير، في جميع الحالات، وتوفير سبل انتصاف فعالة للأشخاص المتضررين في حالة حدوث انتهاكات، بما يشمل إخطارهم لاحقاً، حيثما أمكن، بأنهم وضعوا تحت المراقبة أو بأن بياناتهم تعرضت للقرصنة الحاسوبية (المرجع نفسه، الفقرة ٣٧). وقد كررت الجمعية العامة هذه المبادئ في قرارها ١٧٩/٧٣، وأشارت إلى أن مراقبة الاتصالات الرقمية يجب أن تكون متسقة مع الالتزامات الدولية في مجال حقوق الإنسان، وأن تتم بالاستناد إلى إطار قانوني يكون بالضرورة متاحاً للعموم وواضحاً ودقيقاً ومستفيضاً وخالياً من التمييز.

٢٦- وتنطبق هذه المبادئ في جميع حالات المراقبة المحددة الأهداف، غير أنها تكتسي قوة خاصة عندما يتعلق الأمر بالتعبير دفاعاً عن مصلحة عامة. فالمراقبة المحددة الأهداف تدفع إلى ممارسة الرقابة الذاتية وتقوّض فوراً قدرة الصحفيين والمدافعين عن حقوق الإنسان على إجراء التحقيقات وإقامة علاقات مع مصادر المعلومات والحفاظ على هذه العلاقات (A/HRC/38/35/Add.2، الفقرة ٥٣). وقد شدَّدت اللجنة على أنه لا يجوز التذرع مطلقاً بالقيود لتبرير كبح أية دعوة إلى إقامة نظام ديمقراطي متعدد الأحزاب وتحقيق مبادئ الديمقراطية وحقوق الإنسان"[٣٢]. ولا يجوز تبرير الاعتداء على شخص بسبب ممارسة حقه في حرية التعبير بالاستناد إلى المادة ١٩(٣)[٣٣]. وبيَّنت اللجنة كذلك أهمية حماية الصحفيين والأشخاص الذين يشاركون في جمع المعلومات عن حالة حقوق الإنسان وتحليلها، والذين ينشرون التقارير المتصلة بحقوق الإنسان، بمن فيهم القضاة والمحامون[٣٤]. وتشمل هذه الحماية سرية المصادر التي شددت

(٣٠) التعليق العام رقم ٣٤، الفقرة ٢٥.

(٣١) المرجع نفسه، الفقرتان ٣٤-٣٥.

(٣٢) التعليق العام رقم ٣٤، الفقرة ٢٣.

(٣٣) المرجع نفسه

(٣٤) المرجع نفسه

آليات حقوق الإنسان الدولية والإقليمية (في النظم الأفريقية والأوروبية والأمريكية) على ضرورة حمايتها بموجب القانون (A/70/361، الفقرة ٥).

٢٧- وبالإضافة إلى الالتزامات الأساسية التي تقتضي من الدول عدم التدخل في الخصوصية وعدم تقييد حرية التعبير، فإن من واجباتها أيضاً حماية الأفراد من تدخل الغير. وتفرض المادة ٢ من العهد الدولي الخاص بالحقوق المدنية والسياسية، التي تجسد الواجبات الأساسية الواقعة على الدول، واجباً يقضي باحترام الحقوق المعترف بها في العهد، وبكفالة هذه الحقوق لجميع الأفراد الموجودين في إقليمها والداخلين في ولايتها[٣٥]. وتنص المادة ١٧(٢) من العهد على حق كل شخص في أن يحميه القانون من التدخل في حياته الخاصة على نحو غير قانوني. ولكن من غير الواضح ما إذا كانت الدول توفر عموماً الحماية القانونية الإيجابية من المراقبة المحددة الأهداف. ولا شك أن هذا يصدق على المراقبة عبر الحدود الوطنية، حتى عندما يتعرض مواطن دولة من الدول للمراقبة من كيانات أجنبية[٣٦]. وفي حالة تتعلق بورود ادعاءات تشير إلى ممارسة المراقبة المحددة الأهداف في المكسيك، نظم المقرر الخاص المعني بحرية التعبير في لجنة البلدان الأمريكية لحقوق الإنسان والمقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير بعثةً مشتركة إلى البلد وأثارا هناك مسألة استخدام الحكومة برنامج بيغاسوس للتجسس الحاسوبي. وحثا الحكومة على السماح بإجراء تحقيق مستقل في ادعاءات استخدام برنامج التجسس ضد الصحفيين (A/HRC/38/35/Add.2، الفقرات ٥٢-٥٥). وحتى الآن، لم تسفر جهود التحقيق في الادعاءات عن توضيح ملابسات هذا الأمر مع أن المعهد الوطني للشفافية والوصول إلى المعلومات وحماية البيانات الشخصية في المكسيك أوعز للحكومة بكشف طبيعة العقود التي أبرمتها لاقتناء برنامج بيغاسوس[٣٧].

٢٨- ويتضح من المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون "الحماية والاحترام والانتصاف" الذي اعتمده مجلس حقوق الإنسان في عام ٢٠١١، أن واجب الدولة في توفير الحماية يشمل واجب اتخاذ خطوات مناسبة لمنع انتهاك أطرافٍ ثالثة لحقوق الإنسان والتحقيق في هذه الانتهاكات ومعاقبة مرتكبيها وإنصاف الضحايا (A/HRC/17/31). وتحث هذه المبادئ التوجيهية الدول على ممارسة الرقابة الكافية من أجل الوفاء بالتزاماتها الدولية في مجال حقوق الإنسان عندما تتعاقد مع مؤسسات تجارية على تقديم خدمات قد تؤثر على التمتع بحقوق الإنسان، أو عندما تسن تشريعات لهذا الغرض (المرجع نفسه، ص. ١٠).

---

(٣٥) انظر أيضاً اللجنة المعنية بحقوق الإنسان، التعليق العام رقم ٣١(٢٠٠٤) بشأن طبيعة الالتزام القانوني العام المفروض على الدول الأطراف في العهد. وتجدر الإشارة إلى أنه في إطار التعليق العام رقم ٣١، أُدرجت تحديداً، المادة ١٧ المتعلقة بالخصوصية كمثال لمادة تتناول التزامات إيجابية بأن تعالج الدول الأطراف أفعال الخواص من الأفراد أو الكيانات.

(٣٦) انظر Nate Cardozo, "D.C. circuit court issues dangerous decision for cybersecurity: Ethiopia is free to spy on Americans in their own homes", Electronic Frontier Foundation, 14 March 2017.

(٣٧) انظر Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Fiscalía general de la República tiene oportunidad histórica para acabar con la impunidad en caso Pegasus: Salas Suárez", 27 March 2019; and Juan Arvizu, "Ordena Inai a PGR abrir contrato de compra de Pegasus", *El Universal*, 17 April 2018.

## باء- مسؤولية الشركات

٢٩- في ظل غطاء السرية الذي يلف عمل الشركات في قطاع المراقبة الخاص لا يعلم الجمهور شيئاً عما تفعله هذه الشركات لمراعاة تأثير منتجاتها على حقوق الإنسان، هذا إن كانت تفعل شيئاً أصلاً. ومن الصعب أن يتصور المرء أنها تأخذ بالفعل هذا التأثير في حسبانها نظراً لطبيعة هذا القطاع واستخدام منتجاته على نطاق واسع لأغراض تتعارض مع القانون الدولي لحقوق الإنسان. وبعبارة أخرى، لا يمكن أن تكون الشركات جادة في زعمها أنها لا تملك فكرةً عن استخدام أدواتها لأغراض قمعية بالنظر إلى أن القمع الذي يمارسه العديد من عملائها معروف على نطاق واسع بين عامة الناس.

٣٠- وتقدم المبادئ التوجيهية إطاراً لتقييم مدى احترام شركات المراقبة لحقوق المتضررين من منتجاتها والخدمات التي تقدمها. وينصبُّ التركيز بوجه خاص في المبادئ التوجيهية على الالتزامات السياساتية باحترام حقوق الإنسان؛ وعمليات بذل العناية الواجبة لتحديد آثار نشاط الشركات على حقوق الإنسان ومنع هذه الآثار والتخفيف من حدتها وبيان طريقة معالجتها؛ والتشاور مع الفئات المتضررة؛ والتقييم المستمر لمدى فعالية السياسات المتَّبعة في مجال حقوق الإنسان؛ وإتاحة آليات تظلُّم فعالة لأصحاب الحقوق المتضررين (A/HRC/17/31، الفقرات ١٥-٢٥).

٣١- ويبدو أن الشركات تقصُرُ، بكل المعايير، عن الوفاء حتى بهذا الحد الأدنى كخط أساس. فالشركات القليلة التي نشرت سياسة التعامل مع العملاء التي تتبعها، تشير إشارة مبهمة إلى ضرورة احترام حقوق الإنسان. وتفيد شركة Hacking Team مثلاً، بأنها تستعرض "الزبائن المحتملين قبل البيع لتحديد ما إذا كانت هناك أدلة موضوعية أو مخاوف معقولة من أن تُستخدم التكنولوجيا التي تقدمها شركة Hacking Team للزبون في تسهيل انتهاكات حقوق الإنسان"، ولكنها لا تبين ما تفعله بتلك المعلومات، أو حتى تحدد حقوق الإنسان التي قد تمس به تكنولوجياتها[٣٨]. وتزعم مجموعة شركات NSO أنها تعمل وفقاً لتوصيات لجنة معنية بأخلاقيات الأعمال "تضم خبراء خارجيين من مختلف التخصصات، بما في ذلك القانون والعلاقات الخارجية"، وتقول إنه قد يحدث أن تلغي عملاً ما إذا "أسيء استخدام" منتجاتها[٣٩]. وتذكر على موقعها الشبكي أيضاً، أنها سوف "تحقق في أي ادعاء موثوق يشير إلى إساءة استخدام منتجاتها"، ولكن ليس هناك ما يبين ما إذا كان ذلك يشمل انتهاكات حقوق الإنسان[٤٠].

٣٢- وباختصار، لم تفصح الشركات عن حالات اتخذت فيها إجراءات ذات معنى، مثل تنفيذ عمليات بذل العناية الواجبة التي تتيح تحديد الآثار الضارة لأنشطتها الخاصة على حقوق

(٣٨) شركة Hacking Team، سياسة التعامل مع العملاء.

(٣٩) انظر إفادة مجموعة شركات NSO المؤرخ ١٧ أيلول/سبتمبر ٢٠١٨. متاح على الرابط التالي: https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf. وكما نُقل عن "مختبر المواطن" فإن "إفادات مجموعة شركات NSO عن اللجنة المعنية بأخلاقيات الأعمال تُذكِّر بمثال شركة Hacking Team التي تحدثت عن فريق خارجي من الخبراء التقنيين والمستشارين القانونيين ... يستعرض عمليات البيع المحتملة". ويبدو أن المقصود بهذا "الفريق الخارجي" هو مكتب محاماة واحد لم تتبع شركة Hacking Team توصياته دائماً" (بيل ماركتزاك وآخرين، "لعبة الغمّيضة").

(٤٠) انظر www.nsogroup.com/about.

الإنسان، وتجنب التسبب في هذه الآثار أو المساهمة فيها، ومنع الآثار الضارة بحقوق الإنسان التي ترتبط ارتباطاً مباشراً بعملياتها أو منتجاتها أو خدماتها في إطار علاقاتها التجارية (A/HRC/17/31، المرفق، المبدأ ١٣). وليست هناك، على سبيل المثال، معلومات عامة يُستشف منها أن التقييمات المتعلقة بحقوق الإنسان تُجرى بشكل اعتيادي في إطار بذل العناية الواجبة خلال عمليات البيع، وأن الشركات تعطي وزناً راجحاً لهذه التقييمات، وأن إجراء التقييمات يستمر طيلة دورة حياة المنتج ومدة أي عقد يبرم لتوفير خدمات الدعم بعد البيع. والواقع أن تزايد الأدلة على الدور المحوري الذي يؤديه هذا القطاع في تسهيل الانتهاكات الجسيمة لحقوق الإنسان، إلى جانب امتناع هذا القطاع عن توضيح ضماناته، لا يدعا مفراً من استنتاج عقم هذا التنظيم الذاتي.

٣٣- ويبرز التوجيه الصادر عن المفوضية الأوروبية بشأن تنفيذ المبادئ التوجيهية في قطاع تكنولوجيا المعلومات والاتصالات أهمية "مراعاة حقوق الإنسان في عملية التصميم"[(٤١)]. وفي ضوء وجود خطر هائل من أن يساء استخدام المنتجات بالمراقبة، يجدر بالشركات أن تتوقع لبرمجياتها أن تُستخدم استخداماً غير مشروع وتشرع في هندسة الحلول اللازمة لمعالجة الآثار السلبية الحتمية. وقد أقدمت حكومة المملكة المتحدة على خطوة واعدة، بالشراكة مع إحدى جمعيات قطاع صناعة التكنولوجيا، تتمثل في إعداد مجموعة من المبادئ التوجيهية لقطاع الأمن السيبيراني تشدد على أهمية منع المخاطر المرتبطة بحقوق الإنسان والتخفيف من حدتها "عن طريق إدخال التعديلات المناسبة على التصميم" في المراحل الأولى من تطوير المنتج.

## جيم- مراقبة الصادرات على الصعيدين الدولي والمحلي

٣٤- تعد الضوابط على الصادرات عنصراً مهماً في سياق الجهود الرامية إلى تقليص المخاطر التي يسببها قطاع المراقبة الخاص واستعمال أدواته استعمالاً قمعياً. بيد أن فعالية هذه الضوابط محدودة. ويعزى ذلك أولاً إلى أن النظام الدولي لمراقبة الصادرات ذي الصلة - وهو ترتيب فاسنار غير الملزم بشأن ضوابط تصدير الأسلحة التقليدية والسلع والتكنولوجيات المزدوجة الاستخدام، الذي تشارك فيه ٤٢ دولة - مصمّم للحد من التهديدات على الأمن الإقليمي والدولي. وإذا كان هذا الهدف محموداً وضرورياً فإن الإطار المصاحب غير مناسب لمواجهة التهديدات التي تثيرها المراقبة المحدَّدة الهدف على حقوق الإنسان؛ وبالفعل، فهو يفتقر إلى مبادئ توجيهية أو تدابير تعزيزية كفيلة بالتصدي مباشرة لانتهاكات حقوق الإنسان التي تسببها أدوات المراقبة. وتعزى ثانياً إلى أن التركيز على الصادرات خيار قاصر لمعالجة المشكلة المركزية المتمثلة في استخدام هذه التكنولوجيات لاستهداف أشكال التعبير والاختلاف والإبلاغ المشروعة وغيرها من أشكال ممارسة حقوق الإنسان.

٣٥- على أن ترتيب فاسنار يسعى إلى تعزيز أهداف مهمة تنطوي عليها مسألة "الشفافية وزيادة المسؤولية في عمليات نقل أسلحة تقليدية وسلع وتكنولوجيات مزدوجة الاستخدام". والمتوقع من الدول المشاركة في هذا الترتيب أن تطبّق ضوابط التصدير على جميع المواد الواردة في

(٤١) انظر المفوضية الأوروبية، *دليل قطاع تكنولوجيا المعلومات والاتصالات لتنفيذ مبادئ الأمم المتحدة التوجيهية بشأن الأعمال التجارية وحقوق الإنسان* (لكسمبرغ، ٢٠١٣).

قائمة السلع والتكنولوجيات المزدوجة الاستخدام[٤٢]. وبهذه الصفة، يكون ترتيب فاسنار (أو ينبغي أن يكون) قد أُدرج في القوانين والسياسات المحلية من قبل الدول المشاركة والدول غير المشاركة في الترتيب؛ لكن لا توجد للأسف أي آلية تنفيذية تكفل تجسيد هذا الترتيب في القوانين المحلية أو تنفيذه من قبل الوكالات المحلية المعنية.

٣٦- وفي عام ٢٠١٣، أضافت الدول المشاركة عناصر متعلقة بـ "البرامجيات التطفلية" وبنُظم مراقبة الاتصالات على أساس شبكة بروتوكولات الإنترنت إلى قائمة التكنولوجيات مزدوجة الاستخدام. ووفقاً لهذه القائمة، فإن البرنامج الحاسوبي التطفلي هو "'برنامج حاسوبي' مصمم أو معدّل خصيصاً لتفادي انكشاف الأمر 'بأدوات الرصد'، أو لإبطال 'التدابير المضادة للحماية'"، وهو إما يَستخرج بيانات من حاسوب أو جهاز شبكي وإما يغيّر "مسار التنفيذ المعتاد" لبرنامج ما للسماح "بتنفيذ تعليمات مقدمة من الخارج"[٤٣].

٣٧- وتبيّن التقارير المفصّلة عن التجاوزات المتصلة بالمراقبة أن نظام الرقابة على الصادرات القائم على أساس ترتيب فاسنار لم يؤد حقاً إلى الحد من انتشار تكنولوجيات المراقبة واستخدامها للأغراض القمعية. وتعثُّر جهود البرلمانيين الأوروبيين لتعزيز أشكال حماية حقوق الإنسان في القوانين والسياسات الأوروبية المتعلقة بالتصدير إنما يكشف مدى التحديات التي يواجهها مسعى الإصلاح. وكانت جهودهم تسعى صراحة إلى توسيع قائمة المواد مزدوجة الاستعمال وضوابط الرقابة الشاملة، وإلى أخذ مسألة "احترام حقوق الإنسان في بلد المقصد النهائي" لتكنولوجيات المراقبة بعين الاعتبار[٤٤]. وفي كانون الثاني/يناير ٢٠١٨، عُرض هذا الاقتراح للقراءة الأولى في البرلمان الأوروبي، وكان في الأصل يحظى بالتأييد لإعمال ضوابط أشد على الصادرات ذات الاستعمال المزدوج[٤٥]. على أن الاقتراح تعرض فيما بعد لانتقادات من تسع دول أعضاء على الأقل، مطالبة بأن تكون أشكال الحماية لحقوق الإنسان أضعف[٤٦]. وقد بات مستقبل هذا التشريع الآن غير واضح[٤٧].

٣٨- وعلى الصعيد المحلي، يتفاوت إعمال الضوابط على الصادرات حتى بين الدول المشاركة في ترتيب فاسنار. فعلى سبيل المثال، لم تعتمد الولايات المتحدة بعد إضافات عام ٢٠١٣ من العناصر المتعلقة بالبرامجيات المتطفّلة ونُظم مراقبة الاتصالات على أساس شبكة بروتوكولات

(٤٢) انظر ترتيب فاسنار، "قائمة السلع والتكنولوجيات المزدوجة الاستخدام وقائمة الذخائر".

(٤٣) المرجع نفسه، الصفحة ٢٢١.

(٤٤) انظر المفوضية الأوروبية، "Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)"، ٢٨ أيلول/سبتمبر ٢٠١٦؛ و Lucie Krahulcova, "The European Parliament is fighting to strengthen the rules for surveillance trade", Access Now, 8 December 2017.

(٤٥) لأخذ فكرة عامة عن التاريخ التشريعي للائحة المقترحة المذكورة أعلاه، انظر EUR-Lex, Doc. 52016PC0616.

(٤٦) وفود إستونيا وإيرلندا وإيطاليا وبولندا وتشيكيا والسويد وفنلندا وقبرص والمملكة المتحدة، "لاعتماد لائحة الاتحاد الأوروبي المحسَّنة ٢٠٠٩/٤٢٨ بشأن مراقبة الصادرات ولإعمال ضوابط متعلقة بالمراقبة الالكترونية بما يعزز حقوق الإنسان والقانون الإنساني الدولي عموماً"، INIT 5755/2018 WK (١٥ أيار/مايو ٢٠١٨)؛ وانظر الآن، "الاتحاد الأوروبي: دول تدفع من أجل تخفيف القواعد المتعلقة بتصدير تكنولوجيا المراقبة لمنتهكي حقوق الإنسان"، ١١ حزيران/يونيه ٢٠١٨.

(٤٧) انظر Catherine Stupp, "Nine countries united against EU export controls on surveillance software", Euractiv, 11 June 2018; and Moßbrucker, "Surveillance exports".

الإنترنت[٤٨]. على أن وزارة التجارة في الولايات المتحدة تعكف على إجراء استعراض واسع للإطار الحالي وكُلّفت بوضع عملية مشتركة بين الوكالات لتحديد ضوابط جديدة تخص التكنولوجيات "الناشئة" و"الأساسية" على السواء في إطار قانون عام ٢٠١٨ بشأن إصلاح الضوابط على الصادرات[٤٩]. واعتمدت إسرائيل، وهي دولة غير مشاركة، ضوابط على تصدير مواد مزدوجة الاستخدام مشمولة بترتيب فاسنار، لكن إعمالها هذه الضوابط محاط بالكتمان[٥٠].

## دال- عدم وجود سبل انتصاف بخصوص الرقابة المحددة الهدف

٣٩- في إطار واجب الدولة احترام حقوق الإنسان وكفالة التمتع بها، تفرض المادة ٢(٣)(أ) من العهد الدولي الخاص بالحقوق المدنية والسياسية التزاماً بتمكين ضحايا الانتهاكات من التماس سبيل انتصاف فعال. وبيّنت المادة ٢(٣)(أ) أن الادعاءات بالتعرض لهذه الانتهاكات يجب أن تبت فيها سلطات قضائية أو إدارية أو تشريعية مختصة، أو أي سلطة مختصة أخرى نص عليها النظام القانوني للدولة. وشددت اللجنة المعنية بحقوق الإنسان على أنه ينبغي لسلطات إنفاذ القانون والنيابة أن تحقق في الادعاءات بوقوع انتهاكات بصورة سريعة وشاملة وفعالة عن طريق هيئات مستقلة ونزيهة[٥١]. ثم إن واجب توفير سبل انتصاف فعالة يقتضي أيضاً الالتزام بحماية الأفراد من أعمال تقوم بها كيانات من القطاع الخاص تتسبب في انتهاك الحرمات، وذلك بممارسة الحرص الواجب لمنع وقوع الضرر بسبب أعمال تصدر عن أشخاص أو كيانات من القطاع الخاص والمعاقبة عليها والتحقيق فيها وجبر من لحقهم هذا الضرر[٥٢].

٤٠- ولم يحالف ضحايا المراقبة محددة الهدف الكثير من التوفيق في جهودهم للحصول على الإقرار بالضرر الذي لحقهم، ناهيك عن تمكينهم من سبل الانتصاف جراء ما لحقهم من ضرر. والأمر كذلك رغم أنه، كما بيّنت المحكمة الأوروبية لحقوق الإنسان والمفوضية السامية لحقوق الإنسان، مجرد التهديد بالمراقبة، حتى عندما يكون سرياً، مقترناً بعدم وجود سبيل للانتصاف، يمكن أن يشكل تدخلاً في الحق في الخصوصية[٥٣].

٤١- والمقاضاة باعتبارها إجراء لالتماس الانتصاف من شركات المراقبة الخاصة التي تصنّع وتبيع هذه الأدوات والحكومات التي تستعملها غير مؤكدة. والافتقار إلى حق إقامة الدعوى وإلى سبل الانتصاف يثير مخاوف حقيقية إزاء مدى إمكانية تحميل الشركات المسؤولية على انتهاكات حقوق الإنسان. وقد باشر ضحايا مزعومون إجراءات التقاضي أو شكاوى رسمية ضد شركات للمراقبة الخاصة أو حكومات في ثمانية بلدان على الأقل[٥٤]. غير أن العراقيل أمام

---

(٤٨) الورقة المقدمة من المنظمة الدولية لحماية الخصوصية Privacy International، الصفحة ٥.

(٤٩) John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No 115–232 (2018).

(٥٠) انظر "Israel-U.S. export controls", export.gov, 20 July 2018". وانظر أيضاً الفقرة ٤٣ أدناه.

(٥١) التعليق العام رقم ٣١، الصفحة ١٥.

(٥٢) المرجع نفسه، الصفحة ٨.

(٥٣) المحكمة الأوروبية لحقوق الإنسان، *Roman Zakharov v. Russia* (application No. 47143/06), judgment of 4 December 2015, para. 171؛ وA/HRC/27/37، الفقرة ٢٠.

(٥٤) انظر Siena Anstis, "Litigation and other formal complaints concerning targeted digital surveillance and the digital surveillance industry", Citizen Lab, 12 December 2018.

بلوغ إجراءات التقاضي والشكاوى الرسمية هذه مداها كبيرة للغاية، ومن ذلك الافتقار إلى الإشراف القضائي وسبل الانتصاف وحق إقامة الدعوى والإنفاذ والاحتفاظ بالبيانات.

٤٢- وفي بعض الحالات، طلبت منظمات المجتمع المدني بأن تحقق الحكومات في عمليات المراقبة غير القانونية، لكن غالباً ما تُرفَض هذه الطلبات. ففي المملكة المتحدة، قدمت المنظمة الدولية لحماية الخصوصية شكوى جنائية ضد شركة Gamma Group الدولية إلى الوكالة الوطنية المعنية بالجريمة، قائلةً إن الشركة انتهكت قوانين محلية متعددة حين باع فرعها، FinFisher، تكنولوجيا متعلقة بالمراقبة وقدّم المساعدة إلى حكومة البحرين[٥٥]. وقدّم المركز الأوروبي للحقوق الدستورية والإنسانية والمنظمة الدولية لحماية الخصوصية أيضاً شكوى جنائية في ميونيخ، بألمانيا، دعيا فيها إلى التحقيق مع هذه الشركة، لكن سلطات النيابة العامة رفضت الطلب[٥٦]. وحتى في الحالات التي فتحت فيها الدول تحقيقات لمعرفة ما إذا كانت عمليات المراقبة الحكومية تنتهك معايير حقوق الإنسان أو قوانين دول، فإن هذه التحقيقات يمكن أن تكون تعسفية أو مختلّة النظام.

٤٣- ويبدو أن بدائل اللجوء إلى القضاء، التي تتيح سبل انتصاف متسقة مع القانون الدولي لحقوق الإنسان، غير متاحة. ومن ذلك على سبيل المثال أن منظمة العفو الدولية، وعلى إثر استهداف أحد موظفيها برسالة WhatsApp مشبوهة يدّعى أنها ذات صلة ببرنامج Pegasus، وجّهت رسالة إلى وزارة الدفاع الإسرائيلية تطلب منها إلغاء رخصة التصدير الممنوحة لشركة NSO Group[٥٧]. وردّت وكالة مراقبة الصادرات الدفاعية في هذا البلد برسالة ذكرت فيها أنها لا تقدم معلومات عن سياساتها المتعلقة بمنح تراخيص التصدير أو أي معلومات عن التراخيص الحالية ذاتها[٥٨]. ولم تؤكّد الوكالة ولم تنف وجود الترخيص بالتصدير، لكنها لاحظت أن "تراخيص التصدير التي منحتها [وزارة الدفاع] لشركة NSO Group فيما يتعلق بزبائنها من الحكومات منسجمة مع الالتزامات الدولية"[٥٩]. ويتبين أن ثمة عوائق كبيرة تتمثل في عدم ممارسة الضغوط على الصعيدين الإقليمي والدولي وانتهاج سياسات محاطة بالسرية بدعوى الأمن القومي.

٤٤- وقدمت المنظمة الدولية لحماية الخصوصية أيضاً شكاوى إلى جهة الاتصال الوطني في كل من ألمانيا والمملكة المتحدة في إطار منظمة التعاون والتنمية في الميدان الاقتصادي ضد شركتي Gamma وTrovicor على دورهما المزعوم في أعمال المراقبة التي قامت بها حكومة البحرين

(٥٥) انظر المنظمة الدولية لحماية الخصوصية، "Criminal complaint to national cyber crime unit on behalf of Bahraini activists", 13 October 2014. دعاوى قضائية مرفوعة ضد مجموعة NSO في إسرائيل وقبرص: see David D. Kirkpatrick and Azam Ahmed, "Hacking a prince, an emir and a journalist to impress a client", New York Times, 31 August 2018.

(٥٦) انظر المركز الأوروبي للحقوق الدستورية والإنسانية، "FinFisher: no investigation into German-British software company", 12 December 2014.

(٥٧) ورقة مقدمة من منظمة العفو الدولية، الصفحة ٨.

(٥٨) المرجع نفسه.

(٥٩) المرجع نفسه.

واستهدفت معارضين سياسيين[٦٠]. وطلبت الشكوى ضد Trovicor من جهة الاتصال الوطنية في ألمانيا "التأكّد إن كانت الشركة انتهكت المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي المتعلقة بالمؤسسات المتعددة الجنسيات بتصديرها منتجات متعلقة بالمراقبة إلى البحرين، حيث تستعمل السلطات هذه المنتجات مرتكبة انتهاكات لحقوق الإنسان، بما في ذلك القبض على معارضين ومنشقين سياسيين واحتجازهم وتعذيبهم"[٦١]. لكن جهة الاتصال الوطنية رفضت الشكوى بدعوى أن الدليل بوجود شركة Trovicor في البحرين غير كاف. وفي شكوى مماثلة تقريباً قُدّمت إلى جهة الاتصال الوطنية بالمملكة المتحدة ضد شركة Gamma، ادعت عدة منظمات من المجتمع المدني ارتكاب انتهاكات مماثلة[٦٢]. وقبلت جهة الاتصال الوطنية الشكوى وأصدرت تقييماً أولياً في حزيران/يونيه ٢٠١٣ ذكرت فيه أنه: "صحيح أن كلا الطرفين لم يقدم دليلاً مباشراً بشأن تزويد شركة Gamma البحرين بمعدات، إلا أن الأدلة المقدمة تشير إلى أن منتجات تابعة للشركة قد تكون استُعملت ضد نشطاء بحرينيين. واعتبرت [جهة الاتصال الوطنية] أن ذلك يثبت المسائل المتعلقة بالتزامات الشركة باتخاذ ما يجب من الاحتياطات المناسبة وتدارك الآثار المترتبة"[٦٣].

٤٥- ورغم أن التقرير النهائي الصادر عن جهة الاتصال الوطنية قدّم عدّة توصيات تستند إلى معايير حقوق الإنسان، لا يوجد دليل على أن شركة Gamma نفذتها، ولا هي أكّدت إحاطتها علماً بالتقرير[٦٤].

## رابعاً- الإطار لحماية الحقوق الأساسية من المراقبة المحددة الهدف

٤٦- لا يكفي القول بوجود نظام شامل ومُختَلٍ لمراقبة واستعمال تكنولوجيات المراقبة المحددة الهدف. فهو لا يكاد يكون موجوداً. وإذا كان قانون حقوق الإنسان يضع قيوداً محددة على استعمال أدوات المراقبة، فإن الدول تقدِم على أعمال غير مشروعة في مجال المراقبة دون الخوف من التبعات القانونية. فإطار قانون حقوق الإنسان موجود، لكن الإطار لإنفاذ القيود غير موجود. ومن الضروري، والملح أيضاً، أن تحصر الدول استخدامات هذه التكنولوجيات على الاستخدامات المشروعة فقط، وإخضاعها لأكثر أشكال الإشراف والترخيص صرامةً، وأن تجعل

(٦٠) ذكرت المنظمة على موقعها الشبكي أن الدور الرئيسي لجهة الاتصال الوطنية "هو زيادة فعالية المبادئ التوجيهية بالقيام بأنشطة دعائية وتناول التحريات والمساهمة في تسوية المسائل التي قد تنشأ من عدم التقيّد المزعوم بالمبادئ التوجيهية في حالات بعينها".

(٦١) انظر المنظمة الدولية لحماية الخصوصية، "OECD complaint: Trovicor exporting surveillance technology to Bahrain", 1 February 2013.

(٦٢) انظر المنظمة الدولية لحماية الخصوصية، "German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain", 20 December 2013.

(٦٣) المملكة المتحدة، مديرية الابتكارات والمهارات في مجال الأعمال، "German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain", 20 December 2013 (لندن، ٢٠١٣)، الفقرة ٢٥.

(٦٤) انظر Amitpal Singh, "OECD finds actions of Gamma International to be in violation of human rights", Citizen Lab, 3 March 2015; and "UK National Contact Point for the OECD Guidelines for Multinational Enterprises – Privacy International and Gamma International UK Ltd: final statement after examination of complaint", December 2014.

الدول مشاركة القطاع الخاص في سوق أدوات المراقبة – بدءاً من البحث والتطوير إلى تسويق هذه الأدوات وبيعها ونقلها وصيانتها – مشروطاً بالتزام الحرص الواجب إزاء حقوق الإنسان والتمتع بسجل يثبت امتثال معايير حقوق الإنسان.

٤٧- وقد شدّد المكلّف السابق بالولاية على ضرورة اتخاذ الدول تدابير لمنع الاتجار بتكنولوجيات المراقبة، مع إيلاء اهتمام خاص لمسألة جعل هذه التكنولوجيات مادة للبحث والتطوير والتجارة والتصدير والاستخدام، مراعيةً قدرتها على تسهيل ارتكاب انتهاكات منهجية لحقوق الإنسان (A/HRC/23/40، الفقرة ٩٦). وهذا النداء يظل يكتسي أهمية في الوقت الحاضر. وفي هذا الجزء من التقرير، يستعرض المقرر الخاص العناصر الرئيسية لإطار حماية الأفراد من استخدامات تكنولوجيا المراقبة التي تعوق تمتعهم بحقوق الإنسان. والخطوات المقترحة في هذا التقرير تتطلب اتخاذ وتنفيذ إجراءات: من قِبل الدول، بوصفها المستخدم لهذه التكنولوجيات وبوصفها البلدان المصدرة لها؛ ومن قِبل الشركات، عملاً بالمبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان؛ ومن قِبل الدول والشركات في عملها سوياً مع المجتمع المدني؛ ومن قِبل مجلس حقوق الإنسان.

## ألف- التزام وقف اختياري لتصدير واستخدام تكنولوجيات المراقبة المحددة الهدف

٤٨- تقوم الشركات الخاصة باستحداث ونقل وصيانة تكنولوجيات المراقبة – فيما تقوم الدول بشرائها واستخدامها – بطرق مثيرة للقلق. وقد بيّنت ادعاءات ذات مصداقية أن الشركات تبيع أدواتها للحكومات التي تستخدمها لاستهداف صحفيين ونشطاء وشخصيات معارضة وغيرهم ممن يضطلع بأدوار حيوية في مجتمع ديمقراطي. وبعض هذه الشركات يعترض على هذه الادعاءات، قائلة بأنها لا تسمح باستخدام منتجاتها للأغراض غير المشروعة، وأنها تملك آليات لتقييم المبيعات لمستخدمين نهائيين "تثار بشأنهم مشاكل"، وأنها تتقيّد بالقوانين الوطنية بشأن مراقبة الصادرات. ومن الممكن أن تكون الشركات بصدد بذل محاولات حقيقية لمعالجة التهم بالتواطؤ في أعمال القمع والتجاوزات المستندة إلى أعمال المراقبة. بيد أنه لا يوجد سبب معين يحملنا على تصديق ما تقوله الشركات الخاصة دون إخضاعها لعمليات كشف المعلومات على الملأ والمساءلة. فخطورة الادعاءات يتطلب التزام الشفافية في علاقات الشركات وعملياتها، فضلاً عن طائفة من الخطوات الأخرى التي يرد شرحها أدناه.

٤٩- وسيستغرق تنفيذ الخطوات التي ترد في هذا التقرير بعض الوقت. وفي الأثناء، يظل عشرات الصحافيين والنشطاء والمدافعين عن حقوق الإنسان ومنتقدي الحكومات تحت رحمة الحكومات التي يشجعها على ذلك وجود تشكيلة متنوعة من أدوات المراقبة شديدة التطفّل في متناولها. وعليه، فمن الضروري أن تتوقف الشركات على الفور عن بيع ونقل ودعم هذه التكنولوجيات إلى حين تقديمها أدلة مقنعة على اعتمادها تدابير كافية (على النحو المبيّن أدناه) فيما يتعلق بالتزام الحرص الواجب والشفافية والمساءلة لمنع أو تخفيف استخدام هذه التكنولوجيات لارتكاب انتهاكات حقوق الإنسان. وينبغي للحكومات أيضاً أن تفرض وقفاً اختيارياً على منح التراخيص لتصدير تكنولوجيات المراقبة، إلى أن توجد أدلة مقنعة على إمكانية حصر استخدام هذه التكنولوجيات من الناحية التقنية على الأغراض المشروعة المنسجمة مع معايير حقوق الإنسان، أو أن يكون تصديرها مقتصراً على البلدان التي يخضع استعمالها فيها

لترخيص تمنحه هيئة قضائية مستقلة ونزيهة وفقاً للإجراءات المرعية ولمعايير التزام القانون والضرورة والمشروعية. لكن في الوقت الحاضر، ثمة أدلة متراكمة على أن أدوات المراقبة المطوّرة من القطاع الخاص يجري استخدامها لأغراض غير مشروعة على نحو صارخ، الأمر الذي تتيح حجة قوية لإقرار وقف اختياري على هذه التكنولوجيا.

## باء- واجبات الحكومات بوصفها الجهات المستخدمة لتكنولوجيات المراقبة

### ١- تعزيز القوانين الوطنية بما يقصر الرقابة على ما يتوافق مع التزاماتها بموجب القانون الدولي لحقوق الإنسان

٥٠- تكمن الخطوة الأولى بالنسبة للدول التي تنشر أدوات المراقبة في وجوب ضمان انسجام عملها ذلك مع الإطار القانوني المحلي الذي يستوفي المعايير التي يقتضيها القانون الدولي لحقوق الإنسان. وينبغي أن تكون المراقبة مرخّصة بالقانون فقط للجرائم الأكثر خطورة. ولامتثال هذه المعايير، يجب على القوانين الوطنية:

(أ) أن تشدد على تمتع كل فرد بالحق في عدم التعرض للتدخل غير المشروع أو التعسفي في شأنه الخاص والحق في اعتناق آراء دون تدخل وفي التماس المعلومات والأفكار وتلقّيها ونقلها إلى الآخرين دون أي اعتبار للحدود عن طريق أي واسطة إعلامية؛

(ب) أن تشترط جعل أي تشريع يحكم مسألة الرقابة متضمناً في قوانين محددة ومتاحاً للجمهور وألا يُطبَّق إلى عند الضرورة وبما يتناسب مع تحقيق أحد الأهداف المشروعة المقررة في المادة ١٩(٣) من العهد الدولي الخاص بالحقوق المدنية والسياسية؛

(ج) أن تكفل حصول أي عملية مراقبة على الموافقة لاستخدامها ضد شخص بعينه فقط بما ينسجم مع القانون الدولي لحقوق الإنسان وأن تحدد، عند منح الموافقة من قِبل هيئة قضائية مخوّلة ومستقلة ونزيهة، جميع القيود المتعلقة بمدة المراقبة ومكانها ونطاقها؛

(د) أن تشترط خضوع المستخدِمين المرخَّص لهم، بالنظر إلى المخاطر الشديدة بوقوع تجاوزات مرتبطة بتكنولوجيات المراقبة المحددة الهدف، لمتطلبات إمساك سجلات مفصلة بشأنهم. وينبغي ألا يُسمح بالمراقبة إلا إذا كانت متوافقة مع العمليات القانونية النظامية والموثّقة وبعد صدور التراخيص اللازمة بهذا الاستعمال. وينبغي إخطار الجهات المستهدَفة بالمراقبة بقرار السماح بمراقبتهم ما دام هذا الإخطار لا يقوّض الغرض من المراقبة تقويضاً بالغاً[٦٥].

٥١- ومن الشائع أن يكون سقف الاشتراطات الذي تفرضه الدول عالياً في حال التحقيقات الجنائية الساعية إلى الوصول إلى عمل الصحافيين (A/70/361، الفقرة ٢٤). وكثيراً ما تستعمل تكنولوجيات المراقبة لاستهداف الذين يضطلعون بأدوار كبيرة في النهوض بالقيم الديمقراطية. ويسلّم المقرر الخاص بأن بعض الدول قد تعتقد أن ثمة حالات مثلاً حيث يستخدم صحافيون وظيفتهم غطاءً للانخراط في جرائم خطيرة. ويرى المقرر الخاص، من واقع خبرته، أن هذه الادعاءات تكاد تكون خاطئة أو مبالغاً فيها دائماً. وفي أغلب الأحيان، تستخدم الحكومات هذا النوع من الادعاءات لتقويض آراء الصحافيين والمخالفين أو لاستهداف

(٦٥) انظر "Necessary and proportionate: International Principles on the Application of Human Rights to Communications Surveillance" (May 2014).

الصحافيين بالمراقبة حتى عندما لا يكونون هدفاً لتحقيق جنائي مشروع، وهو ما يؤدي إلى التأثير على الصحافة الحرة تأثيراً مفرطاً. وفي هذا السياق، ينبغي أن يكون الموقف التلقائي للقانون هو حظر استخدام أدوات المراقبة الرقمية ضد الأفراد في وسائط الإعلام. وبطبيعة الحال، لا يَمنح ذلك للصحافيين حصانة من أشكال أخرى من الإجراءات القانونية المشروعة، بما في ذلك المراقبة غير الرقمية. والأمر ببساطة هو أن حدوث تجاوزات أو "التسرّب" من التحقيق الجنائي المشروع إلى مجالات تشمل أعمالاً صحفية أخرى، في سياق تكنولوجيات المراقبة الرقمية المتطفلة، إمكانية حقيقية ومن الصعب، إن لم يكن من المستحيل، احتواؤها. وإمكانية حدوث ذلك من شأنه على الأرجح أن يعمل على ردع الصحافيين عن تناول أكثر المواضيع حساسية، فضلاً عن إحجام المصادر والمبلّغين عن المخالفات عن تقديم معلومات.

### ٢- إنشاء آليات عمومية للموافقة والإشراف على تكنولوجيات الرقابة

٥٢- الترخيص القضائي لاستخدام الحكومات تكنولوجيات المراقبة ضروري لكنه غير كاف. فاقتناء هذه التكنولوجيات ينبغي أيضاً أن يكون خاضعاً لعمليات الإشراف والتشاور والرقابة العامة المجدية. وفي السنوات الأخيرة، حيث تزايد استخدام تكنولوجيات المراقبة من قِبل هيئات إنفاذ القوانين في الولايات المتحدة، عمَدت عدة سلطات محلية إلى إنشاء مجالس مدنية للرقابة بغية تنظيم استخدام واقتناء هذه التكنولوجيات. ومن ذلك أن مدينة أوكلاند في كاليفورنيا على سبيل المثال اعتمدت مرسوماً ينص على عدة عناصر متعلقة بشراء تكنولوجيا المراقبة يمكن أن تأخذ بها ولايات أخرى(٦٦). وتشمل هذه العناصر ما يلي:

(أ) عملية لمنح الموافقة، تتولاها الإدارات المعنية، تأخذ في الحسبان التزامات الدولة في مجال حقوق الإنسان؛

(ب) الإبلاغ العام بالمشتريات في هذا المجال من خلال عمليات منتظمة ومشاورات عامة تتناول مسائل مثل انعكاسات هذه المشتريات على صعيد حقوق الإنسان ومعرفة ما إذا كانت التكنولوجيات موضوع الحديث ستحقق غرضها المنشود بفعالية؛

(ج) الإبلاغ العام المنتظم بعمليات الموافقة والمشتريات والاستخدامات.

٥٣- وينبغي، بالأخص في الدول التي تتيح للأجهزة الوطنية على المستوى المحلي قدراً من الاستقلالية في شراء الأدوات المستعملة في مجال إنفاذ القانون، التشجيع على الرقابة المجتمعية على هذه المشتريات وإنفاذ هذا الأمر. وبالنظر إلى الاهتمام العام الواضح بالحفاظ على خصوصية مجموعة كبيرة من البرمجيات التجارية وأمنها، ينبغي أيضاً أن تكون آليات الإشراف العام مخوّلة بوضع سياسات بشأن تراكم أوجه الضعف وتطوير البرمجيات ذات الصلة.

### ٣- تمكين الضحايا من أدوات الجبر القانونية على الصعيد المحلي

٥٤- بالنظر إلى الأسباب المبيّنة أعلاه، من الصعب على من يُستهدَفون بالمراقبة غير القانونية أو التعسفية تقديم شكاوى على الحكومات. وبعض العراقيل في هذا الصدد هيكلي، مثل عدم وجود إمكانية رفع شكوى على الجهات الفاعلة الحكومية في العديد من النُظم

(٦٦) انظر American Civil Liberties Union of Northern California, "Oakland becomes latest municipality to reclaim local control over surveillance technologies used by local law enforcement", 2 May 2018.

القانونية. وقد يكون المشرّعون والمحاكم على حد سواء أيضاً سبباً في إعاقة هذه الشكاوى عندما يمنحون أفضلية مفرطة للمصالح المتصوّرة من حيث الأمن القومي وإنفاذ القانون. وقد يكون من الصعب المضي قدماً في بعض الشكاوى بسبب صعوبات وتكاليف إثبات وجود المراقبة أو نسبتها إلى جهات فاعلة حكومية – أو حتى لوكالات حكومية محددة يمكن أن تُستهدَف بدعوى قضائية. والأفراد المستهدفون بالمراقبة لا علم لهم في الغالب بعملية المراقبة التي يجري تنفيذها ضدهم – أو، إن كانوا على علم بها، قد تتجاوز حدود تعطيل قانون التقادم(٦٧). وبعبارة أخرى، من النادر جداً أن يتمكن صاحب شكوى من كسب دعواه في سياق الدعاوى القانونية المحلية الناشئة عن المراقبة غير المشروعة المزعومة.

٥٥- وينبغي للدول التي تأخذ الانتهاك الذي تتسبب فيه تكنولوجيات المراقبة على محمل الجد أن تتخذ خطوات لتمكين الأفراد من تقديم شكاوى على الجهات الفاعلة الحكومية وغير الحكومية. وسيستلزم ذلك بالضرورة، بالنسبة للعديد من الدول، التأكد من أن القواعد المتعلقة بالاختصاص القضائي والإثبات وسرعة الأداء وغير ذلك من الاشتراطات الأساسية موافقة للغرض في هذا العصر الرقمي. فينبغي لها على سبيل المثال التأكد من تمكُّن المحاكم من قبول تحليل الطب الشرعي الذي يقوم به خبراء فنيون وتقييمه باعتباره دليلاً من الأدلة. وينبغي أن ينشئ التشريع الوطني أيضاً حق إقامة الدعوى ضد الهيئات الخاصة الذي يراعي التغيرات الحاصلة في ملكية الشركات (المعروف باسم "الانتقالات" أو "التحوّلات")، التي كثيراً ما تعقّد جهود الضحايا الرامية إلى تحقيق المساءلة والجبر(٦٨). وينبغي أيضاً مراعاة أشكال الجبر البديلة، مثل لجان إقرار الحقيقة التي تمكّن ضحايا انتهاكات حقوق الإنسان الجسيمة التي سهّلت المراقبة الرقمية وقوعها من الإدلاء بالشهادة والتي تدقق في مدى تواطؤ الشركات في هذه الانتهاكات.

٥٦- وفي الوقت نفسه، ليست المراقبة محددة الهدف محصورة إقليمياً دائماً. فعندما تتجاوز الدول حدودها لتنفيذ عمليات مراقبة محددة الهدف، قد يكون من الصعب على الأفراد المستهدفين بهذه المراقبة تقديم شكاوى على الدولة المخالِفة. وقد تنطوي هذه الحالات كذلك على بعض الأعباء من حيث الإثبات وغيرها من الأعباء نفسها التي تنطوي عليها شكاوى محلية. وفضلاً عن ذلك، قد لا تكون المحاكم، كما في قضية *Doe* المشار إليها أعلاه، مستعدة لقبول النظر في دعاوى قضائية ضد جهات خارجية ذات سيادة. وإذا كانت القواعد إزاء هذه الدعاوى متفاوتة، فينبغي للدول أن تفسّر معايير حصانة الجهات ذات السيادة بما يكفل لمحاكمها إمكانية قبول النظر في الدعاوى المرفوعة على حكومات خارجية.

## جيم- واجبات الحكومات التي ترخّص تصدير تكنولوجيا المراقبة

٥٧- ترتيب فاسنار ليس هو القول الفصل في مجال مراقبة صادرات تكنولوجيات المراقبة؛ وإعمال قوائم المراقبة يتوقف على مدى التنفيذ الوطني. ثم إن الترتيب لا يقضي بمشاركة جميع كبرى البلدان المصدّرة: فإسرائيل، وهي لاعب كبير في سوق تكنولوجيا المراقبة، تدّعي أنها

(٦٧) انظر قضية *رومان زخاروف ضد روسيا*.

(٦٨) ورقة المقدمة من Access Now، الصفحة ٨.

"ممتثلة بالكامل" لترتيب فاسنار، وإن كانت لم تصبح بعد دولة مشاركة[٦٩]. وهو أيضاً عبارة عن إطار محدود إذ لا ينطوي، رغم أهمية أهدافه المتعلقة بالسلم والأمن الإقليميين والدوليين، على توجّه مراعٍ لحقوق الإنسان. ومع ذلك، ينبغي للدول المشاركة، بالنظر إلى أن هذا الترتيب ينشئ معايير تحمل على توقع وقوع تنفيذ وامتثال واسعين، استغلال هذا الإطار الثمين لفرض قيود حقوقية على نقل تكنولوجيات المراقبة.

٥٨- وبغية تحسين دور هذا الترتيب في تطوير معايير عالمية في مجال التصدير، من شأن الدول المشاركة أن تستفيد من إنشاء فريق عامل لحقوق الإنسان يمكنه اقتراح وبحث معايير متعلقة بالصادرات تأخذ في الاعتبار الشواغل إزاء حقوق الإنسان التي تثيرها عمليات نقل التكنولوجيا. لكن يتعين عليها، سواء اعتمدت مثل هذا الفريق العامل أو أي آلية أخرى، إيجاد إطار يكون فيه الترخيص لأي تكنولوجيا مشروطاً باستعراض حالة حقوق الإنسان على الصعيد الوطني وامتثال الشركات المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان، على النحو المبيّن أدناه. ومثلما عبرت عنه المنظمة الدولية لحماية الخصوصية، ينبغي للدول المشاركة، وكذلك الحكومات الأخرى المصدِّرة، رفض الترخيص "إذا تبيّن أن ثمة احتمالاً كبيراً لأن تستخدم هذه الصادرات لانتهاك حقوق الإنسان، أو إذا لم يوجد في بلد الوِجهة إطار قانوني ينظم استخدام مواد المراقبة، أو إذا كان الإطار القانوني المتعلق باستخدامها قاصراً عن الوفاء بالقانون الدولي لحقوق الإنسان أو المعايير ذات الصلة"[٧٠]. ولضمان الامتثال في حالات رفض تراخيص التصدير على هذا الأساس، ينبغي إدراج تكنولوجيات المراقبة المشمولة بهذا الرفض في نُظُم العقوبات المعمول بها[٧١].

٥٩- وإذا كانت هذه المعايير ستمثل إضافة قيّمة لترتيب فاسنار، فإن قدرة الجمهور العام أو منظمات محددة في المجتمع المدني على رصد تنفيذها سيتوقف على فرض التزامات أكثر صرامة في مجال الشفافية على الصعيدين الوطني والدولي. وينبغي لهذا الترتيب ذاته أن يشجع على الشفافية وذلك بتحديد مبادئ توجيهية واضحة وقابلة للإنفاذ لتبادل المعلومات على الصعيد الحكومي الدولي وكشف المعلومات للجمهور العام بشأن معايير الترخيص، وقرارات منح الموافقة أو تعديل أو رفض الترخيص، والحوادث أو نمط إساءة استعمال تكنولوجيات المراقبة، وانتهاكات حقوق الإنسان ذات الصلة، والتعامل مع أوجه القصور الرقمية. وينبغي أن تتيح قوانين التصدير الوطنية تخصيص ما يكفي من الموارد لحفظ وإتاحة السجلات العامة فيما يتعلق بقرارات ترخيص التصدير، وتكليف الوكالات الحكومية المعنية بدعوة الجمهور العام إلى تقديم ملاحظات وإجراء مشاورات بإشراك جهات متعددة ذات مصلحة عند قيامها بمعالجة طلبات ترخيص الصادرات. وفي الأخير، ينبغي للدول أيضاً استحداث إعفاءات للبحوث في المجال الأمني وإعفاء مواد التشفير من قيود مراقبة الصادرات[٧٢].

(٦٩) انظر Wassenaar Arrangement, "IL – Israel cybersecurity export control policy" (PowerPoint presentation), June 2016.

(٧٠) ورقة من المنظمة الدولية لحماية الخصوصية، الصفحة ٨.

(٧١) المرجع نفسه، الصفحتان ٣ و٤.

(٧٢) المرجع نفسه، الصفحة ٥.

## دال- تنفيذ المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان من قِبل الشركات

٦٠- بالنظر إلى الاحتمال الكبير القائم بتسبب تكنولوجيات المراقبة في انتهاكات، ينبغي أن يكون منح تراخيص التصدير محظوراً بموجب القانون المحلي إلا إذا أثبتت الشركة بانتظام أنها أوفت بدقة بالتزاماتها بموجب المبادئ التوجيهية فيما يخص تصميم هذه التكنولوجيات وبيعها ونقلها ودعمها. ومن شأن ذلك بالفعل أن يجعل من هذه المبادئ التوجيهية شروطاً مسبقة يتعين على الشركات الوفاء بها للمشاركة في سوق تكنولوجيا المراقبة. وقد بيّن المقرر الخاص، في تقارير سابقة، الكيفية التي ينبغي أن يفي بها قطاع تكنولوجيا المعلومات والاتصالات بمسؤولياته بإزاء حقوق الإنسان (A/HRC/35/22، الفقرات ٤٥-٧٥). ولكي يتسنى لشركات المراقبة الخاصة الوفاء بهذه المسؤوليات، يجب عليها استحداث ما يلي:[٧٣]

(أ) سياسات خدمة الزبائن التي تؤكد بصورة لا لبس فيها مسؤولية الشركات عن احترام حرية التعبير والخصوصية وحقوق الإنسان ذات الصلة في جميع عملياتها، وأن امتثال الزبائن القانون الدولي لحقوق الإنسان شرط لإقرار وإتمام البيع أو نقل البضاعة أو عقد الدعم؛

(ب) عمليات توخي المراعاة الواجبة بإزاء حقوق الإنسان (مثل عمليات تقييم الأثر من حيث حقوق الإنسان) التي يُلجأ إليها عند انخراط الشركات في أنشطة ذات أثر على حرية التعبير والخصوصية، مثل تصميم منتجات وخدمات المراقبة وبيعها ونقلها وخدمتها؛

(ج) سياسات داخلية وأحكام تعاقدية معيارية ينشأ عنها أشكال واضحة ومحددة من حظر عمليات التكييف أو الاستهداف أو الخدمة أو المساعدة فيما يتعلق بمنتجات تنتهك القانون الدولي لحقوق الإنسان؛

(د) عمليات داخلية تكفل تصميم وبلورة خيارات تدمج ضمانات حقوق الإنسان، مثل نُظم الإشعار التي تكشف عن حالات سوء استخدام ومفاتيح الإيقاف التي تشغَّل في حال سوء الاستخدام؛

(هـ) برامج منتظمة للمراجعة وعمليات تدقيق بشأن حقوق الإنسان للتأكد من امتثال استخدام هذه المنتجات والخدمات القانون الدولي لحقوق الإنسان، بما في ذلك الالتزام بالإعلان على الملأ عن الاستنتاجات الرئيسية لهذه المراجعات وعمليات التدقيق؛

(و) عمليات إشعار للإبلاغ على الفور عن حالات سوء الاستخدام لأدواتها موجهة لهيئات الإشراف الحكومية المعنية (مثل المؤسسات الوطنية لحقوق الإنسان) أو الهيئات الحكومية الدولية (مثل آليات الشكوى في إطار الإجراءات الخاصة)؛

(ز) تقارير الشفافية التي تكشف عن الاستخدامات والقدرات الممكنة لمنتجاتها وأصناف الدعم المقدم بعد البيع، وحوادث سوء الاستعمال والبيانات المتعلقة بأعداد وأنواع المبيعات لوكالات إنفاذ القانون والاستخبارات وغيرها من الوكالات الحكومية أو وكلائها؛

(٧٣) العديد من هذه المعايير مستمدة من المساهمات المقدمة من المجتمع المدني والتي يمكن العثور عليها في الملحق بهذا التقرير وفي الموقع الشبكي للمقرر الخاص.

(ح) عمليات تشاور منتظمة مع أصحاب الحقوق المتضررين ومجموعات المجتمع المدني ومنظمات الحقوق في السياق الرقمي تتناول الآثار الواقعة أو الممكنة لمنتجاتها وخدماتها وضمانات حقوق الإنسان المطلوبة لمنع هذه الآثار أو التخفيف منها، مع التركيز بوجه خاص على إشراك المعرَّضين للتمييز أو القمع استناداً إلى عمليات المراقبة، كالأقليات العرقية والإثنية والمجموعات المهمّشة تاريخياً؛

(ط) آليات التظلّم التي تمكّن الأفراد من تقديم شكاوى متعلقة بانتهاكات حقوق الإنسان الناجمة عن منتجات وخدمات الشركات، وتتيح تقييم هذه الشكاوى تقييماً مستقلاً ومتابعتها متابعة مجدية؛

(ي) آليات الانتصاف التي تتيح لأصحاب الشكاوى التماس التعويض والاعتذار وغير ذلك من أشكال الجبر، بحسب مقتضى الحال، في حالات التدقيق في الشكاوى بصورة مستقلة.

## هاء- المبادرات التنظيمية على أساس المشاركة

٦١- قد تكون النُّهُج التي تتبعها الدول والشركات، كما هو مبين في هذا التقرير، غير كافية للتصدي للمشكلة العالمية المتمثلة في المراقبة المحددة الهدف. وهي تفتقر أيضاً إلى إسهامات مهمة من جهات متعددة - إسهامات الأطراف الفاعلة في المجتمع المدني، سواء كانوا نشطاء أو تقنيين في المجال التكنولوجي أو أكاديميين أو ضحايا أو من ينتمون إلى أكثر من واحدة من هذه الفئات. فالإدارة التنظيمية على أساس المشاركة التي تتحقق فيها مشاركة مجدية من جانب الأطراف الفاعلة من الدول ومؤسسات الأعمال والمجتمع المدني قد تتيح توجيهات للعمل لإحقاق المساءلة إزاء حقوق الإنسان في قطاع المراقبة الخاصة. ولعل من المفيد النظر على وجه الخصوص في المبادرات التنظيمية على أساس المشاركة التي وضعت في القطاع الأمني الخاص للحث على المساءلة والإشراف في الشركات. وعلى غرار شركات المراقبة الخاصة، ترتبط المخاطر التي تتحملها الشركات الأمنية الخاصة بانخراطها المتأصّل في وظائف الدول، لا سيما في مجال الأمن القومي. لذا فإن التنظيم التشاركي للشركات الأمنية الخاصة يتطلب بذل جهود لتثقيف الشركات بشأن الشواغل إزاء حقوق الإنسان ويولّد حوافز لمشاركة جهات متعددة ذات مصلحة (شهادة إقرار استناداً إلى عمليات المراجعة والرصد الشاملة للمجتمع المدني)، وهو ما يمكن أن ينتقل بصورة جيدة إلى قطاع المراقبة الخاصة.

٦٢- وثمة جانبان من البيئة التنظيمية للشركات الأمنية الخاصة جديرين بالنظر فيهما في سياق شركات المراقبة الخاصة. فوثيقة مونترو بشأن الالتزامات القانونية الدولية والممارسات السليمة للدول ذات الصلة بعمليات الشركات العسكرية والأمنية الخاصة أثناء النزاع المسلح تورد توصيات للممارسات الجيدة للدول في مثل هذه الأوضاع[٧٤]. وبالرغم من عدم إلزامية هذه الوثيقة، فهي تتضمن التزامات قانونية دولية للشركات الأمنية الخاصة، وكذلك توصيات في شكل ممارسات جيدة للدول المتعاقدة ودول الإقليم ودول المنشأ. والمبادئ الواردة في هذه الوثيقة

(٧٤) انظر وزارة الشؤون الخارجية السويسرية واللجنة الدولية للصليب الأحمر، "The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict" (برن، ٢٠٠٨).

بشأن الكشف العلني والتزام الحرص الواجب ترجع إلى وقت سابق وتعكس المسؤوليات الموجودة في المبادئ التوجيهية.

٦٣- وقد تكون مدونة قواعد السلوك الدولية لشركات الخدمات الأمنية الخاصة أيضاً نموذجاً مناسباً. فهذه المدونة التي وضعت بدعم من المجتمع المدني والقطاع الخاص وحكومة سويسرا، تعد أحد النُّهُج القليلة التي تنطوي على مشاركة الشركات الأمنية الخاصة. والرابطة المعنية بمدونة قواعد السلوك الدولية لشركات الخدمات الأمنية الخاصة عبارة عن مبادرة متعددة الجهات ذات المصلحة تضم ممثلين عن الدول والشركات الأمنية الخاصة ومنظمات المجتمع المدني. وتهدف هذه المدوّنة غير الملزمة إلى استكمال الرصد والإشراف، وبيان التزامات القانون الدولي الواقعة على الشركات، واستحداث الهيكلة لإطار المساءلة أمام الرابطة. وتتألف الرابطة من جمعية عام، تمثَّل فيها المجموعات ذات المصلحة، ومجلس إدارة، يضم ١٢ عضواً منتخباً يمثلون المجموعات ذات المصلحة الثلاث. وعلى وجه الخصوص، يستلزم قبول الشركة امتثال المدونة، بما في ذلك شهادة الإقرار التي تصدرها الرابطة وعمليات المراجعة والتدقيق.

٦٤- ومثلما ذُكر في النظام الأساسي، تتمثل الفكرة الرئيسية للمدوّنة في التشجيع على الاستخدام المسؤول للخدمات الأمنية الخاصة، فضلاً عن احترام القانون الدولي لحقوق الإنسان. وتبيّن المدوّنة ذاتها الالتزامات العامة للدول والشركات الأمنية الخاصة وغيرها من مقدمي الخدمات الأمنية الخواص، وكذلك مبادئ محددة للسلوك في مجالات تشمل: استعمال القوة، والاعتقال، والقبض على الأشخاص، والتعذيب وغيره من أصناف العقاب، والعنف الجنساني، والاتجار بالبشر، والرِّق والعمل الشاق، والتمييز، وتحديد وتسجيل موظفي الأمن الخاص(٧٥).

## واو- الاتجاهات في قيود الدول

٦٥- لقد أنشأ مجلس حقوق الإنسان، لمصلحة حقيقية، عدّة فرق عمل مكلفة بولايات لتناول مواضيع رئيسية متعلقة بتنفيذ المعايير الدولية لحقوق الإنسان. وقد ينظر المجلس أو إجراءاته الخاصة في استحداث آلية جديدة تولي ما يلزم من العناية لحالات بعينها قد لا يستطيع فرادى المكلفين بولايات تناولها وتقييمها. فيمكن لفريق عامل جديد أو فرقة عمل شاملة لعدة ولايات أو خطة عمل يصدر بها تفويض أن تولي اهتماماً خاصاً للادعاءات بأن الممارسات الوطنية في مجال المراقبة - التي تمس بالعيديد من مجالات قانون حقوق الإنسان ومن ثم بالعديد من الولايات في إطار الإجراءات الخاصة - تشكل إخلالاً بحقوق الإنسان الأساسية.

## خامساً- التوصيات

٦٦- **توصيات موجهة إلى الدول:**

(أ) **ينبغي للدول إقرار وقف اختياري فوراً بخصوص تصدير وبيع ونقل واستعمال وخدمة أدوات المراقبة التي تطورها شركات خاصة إلى حين وضع نظام ضمانات يمتثل حقوق الإنسان موضع التنفيذ؛**

(٧٥) انظر أيضاً المعلومات الواردة من سارة ماكّون، الصفحة ١٠.

(ب) ينبغي للدول التي تقتني أو تستعمل تكنولوجيات المراقبة ("الدول المقتنية") ضمان عدم إجازة القوانين المحلية استعمال هذه التكنولوجيات إلا إذا كان متوافقاً مع معايير حقوق الإنسان المتمثلة في موافقة الأهداف للقانون وكونها ضرورية ومشروعة، وإقامة آليات قانونية للجبر منسجمة مع التزاماتها بإتاحة سبيل انتصاف فعال لضحايا الانتهاكات المتصلة بعمليات المراقبة؛

(ج) ينبغي للدول المقتنية أيضاً استحداث آليات تكفل الموافقة والإشراف والرقابة العامة أو المجتمعية على شراء تكنولوجيات المراقبة؛

(د) ينبغي للدول التي تصدِّر أو تسمح بتصدير تكنولوجيات المراقبة ("الدول المصدِّرة") التأكد من طلب الوكالات الحكومية المعنية مساهمات عامة وإجرائها مشاورات متعددة الجهات ذات المصلحة عند معالجتها طلبات ترخيص التصدير. وينبغي تخزين جميع المعلومات المتعلقة بترخيص التصدير وجعلها متاحة على أوسع نطاق ممكن. وينبغي لها أيضاً إقرار إعفاءات للبحوث في المجال الأمني وإعفاء مواد التشفير من قيود مراقبة الصادرات؛

(هـ) ينبغي للدول المصدِّرة الانضمام إلى ترتيب فاسنار والتقيّد بقواعده ومعاييره مادامت منسجمة مع القانون الدولي لحقوق الإنسان؛

(و) ينبغي للدول المشارِكة في ترتيب فاسنار استحداث إطار يكون فيه الترخيص لأي تكنولوجيا مشروطاً باستعراض حالة حقوق الإنسان على الصعيد الوطني وامتثال الشركات المبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان. ويمكن استحداث مثل هذا الإطار من خلال فريق عامل لحقوق الإنسان يُقام خصيصاً لهذا الغرض. وفضلاً عن ذلك، ينبغي لها تحديد توجيهات واضحة وقابلة للإنفاذ بشأن الشفافية والمساءلة بإزاء قرارات الترخيص، وانتهاكات حقوق الإنسان المرتبطة بعمليات المراقبة، والتعامل مع مواطن القصور الرقمية؛

٦٧- توصيات موجّهة للشركات:

(أ) ينبغي لشركات المراقبة الخاصة أن تؤكّد علانيةً مسؤوليتها عن احترام حرية التعبير والخصوصية وحقوق الإنسان ذات الصلة، والأخذ بمتطلبات التزام الحرص الواجب في سياق حقوق الإنسان من أولى مراحل تطوير الإنتاج إلى باقي عملياتها. وينبغي أن يكون تصميم هذه العمليات مصحوباً بإدماجها حقوق الإنسان، وإجراء مشاورات منتظمة مع المجتمع المدني (لا سيما المجموعات المعرّضة للمراقبة)، والإبلاغ الحقيقي في إطار الشفافية عن أنشطة مؤسسات الأعمال التي تؤثر في حقوق الإنسان؛

(ب) ينبغي للشركات أيضاً أن تضع ضمانات قوية موضع التنفيذ لضمان امتثال أي استخدام لمنتجاتها أو خدماتها معايير حقوق الإنسان. وتشمل هذه الضمانات الأحكام التعاقدية التي تحظر عمليات التكييف أو الاستهداف أو الخدمة أو أي استخدام آخر ينتهك القانون الدولي لحقوق الإنسان، وخصائص التصميم التقني لإبراز حالات سوء الاستخدام أو منعها أو التخفيف منها، وعمليات المراجعة والتدقيق بإزاء حقوق الإنسان؛

(ج) ينبغي للشركات، عند كشفها حالات سوء استخدام منتجاتها أو خدماتها لارتكاب انتهاكات لحقوق الإنسان، الإبلاغ عنها فوراً لهيئات الإشراف المحلية أو الإقليمية

**أو الدولية المعنية. وينبغي لها أيضاً استحداث آليات فعالة للتظلّم والانتصاف تكفل لضحايا انتهاكات حقوق الإنسان المرتبطة بعمليات المراقبة تقديم شكاوى والتماس الجبر.**

**٦٨- توصية موجّهة للأمم المتحدة: ينبغي للمنظمة، وبالأخص مجلس حقوق الإنسان، إنشاء فريق عامل أو فرقة عاملة شاملة لعدة ولايات لرصد وتقديم توصيات عن الحالات الفردية لانتهاكات حقوق الإنسان التي أدت عمليات المراقبة الرقمية إلى تسهيل وقوعها وعن الاتجاهات في مثل هذه الانتهاكات.**

**٦٩- توصية موجّهة لجميع الجهات ذات المصلحة: ينبغي للدول والقطاع الخاص والمجتمع المدني وسائر الجهات ذات المصلحة إيجاد مبادرات تنظيمية قائم على أساس المشاركة كفيلة بتطوير معايير سلوك حقوقية موجهة لقطاع المراقبة الخاصة وإنفاذ هذه المعايير عن طريق عمليات مراجعة مستقلة ومبادرات تعليمية وأخرى في مجال السياسات العامة.**