الأمم المتحدة

A/HRC/31/64

الجمعية العامة

Distr.: General
24 November 2016
Arabic
Original: English

مجلس حقوق الإنسان

الدورة الحادية الثلاثون

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 بالحق في الخصوصية* **

مذكرة من الأمانة

يصف المقرر الخاص المعني بالحق في الخصوصية، في تقريره المقدم إلى مجلس حقوق الإنسان عملاً بقرار المجلس ١٦/٢٨، رؤيته الخاصة بولايته وأساليب عمله وخطة عمله الثلاثية. ويتضمن التقرير كذلك عرضاً عاماً عن حالة الخصوصية في مطلع عام ٢٠١٦.

* تأخر تقديم هذا التقرير عن الموعد المحدد لتضمينه آخر ما استجد من تطورات.

** تُعمم مرفقات هذا التقرير باللغة التي قُدم بها فقط.

GE.16-20847(A)

1620847

تقرير المقرر الخاص المعني بالحق في الخصوصية

المحتويات

أولاً- مقدمة

١- أنشأ مجلس حقوق الإنسان ولاية المقرر الخاص المعني بالخصوصية، في قراره ١٦/٢٨ بشأن الحق في الخصوصية في العصر الرقمي، الذي شدد فيه المجلس على وجوب امتثال الدول على أكمل وجه لالتزاماتها بموجب القانون الدولي لحقوق الإنسان. ولا يخلو ذلك من تحديات خاصة على صعيد الحق في الخصوصية، لما يطرأ على تكنولوجيا المعلومات من تطورات سريعة تنشئ فرصاً جديدة للتفاعل الاجتماعي، لكنها في الآن ذاته تثير شواغل حول السبل الكفيلة بزيادة بلورة هذا الحق لمواجهة هذه التحديات.

٢- وعملاً بالقرار المذكور أعلاه، سيقدم المقرر الخاص تقريراً سنوياً إلى المجلس وإلى الجمعية العامة معاً. ويصف المقرر الخاص، في هذا التقرير، أساليب عمله (الفرع ثانياً) وحالة الخصوصية في عام ٢٠١٦ (الفرع ثالثاً) والأنشطة التي اضطلع بها حتى الآن (الفرع رابعاً) وخطة عمل من عشر نقاط لاستكشاف الحق في الخصوصية وزيادة بلورته في القرن الحادي والعشرين (الفرع خامساً). وفي الفرع سادساً، يعرض المقرر الخاص استنتاجاته.

٣- وينبغي النظر إلى هذا التقرير باعتباره ذا طابع بسيط وبدائي، لأنه أُعدّ في غضون ستة أشهر فحسب من تعيين المقرر الخاص في ١ آب/أغسطس ٢٠١٥. وبالتالي، لم يتوفر للمقرر الخاص ما يكفي من الوقت للتشاور مع الطيف الكامل من أصحاب المصلحة، رغم ما بذله من جهود حثيثة في هذا السبيل. ولذلك فإن الهدف الرئيسي لهذا التقرير هو تسليط الضوء على عدد من المسائل الهامة، دون ترتيب أولويتها بالضرورة. ومن المتوقع أن يتسنى للمقرر الخاص، بعد أن تتوفر له فرصة الاستماع لشواغل عدد أكبر بكثير من أصحاب المصلحة من مختلف أنحاء العالم، أن يرتب في غضون الأشهر الاثني عشر المقبلة (بحلول كانون الثاني/يناير ٢٠١٧ تحديداً) أولوية الإجراءات التي يتعين اتخاذها. وترِد في المرفق الأول للتقرير رؤية المقرر الخاص بشأن ولايته والتحديات التي يتوقعها في هذا الصدد.

ثانياً- أساليب عمل المقرر الخاص

ألف- الرصد القطري

٤- يجري العمل على تطوير قاعدة بيانات للسياسات والتشريعات والإجراءات والممارسات القائمة حالياً فيما يتصل بالحق في الخصوصية، وتضم مجموعة متنوعة من التقارير والتشريعات ذات الصلة. وستتيح قاعدة البيانات المذكورة للمقرر الخاص تحديد الشواغل وأفضل الممارسات ومن ثم تقاسمها.

باء- الدراسات المواضيعية: التحليل والتقييم

٥- في عالم يستفيد على نطاق واسع من شبكة إنترنت لا حدود لها، تؤشر مشاورات المقرر الخاص إلى وجود دعم قوي لمبدئين عامين هما: ضمانات بلا حدود وسبل انتصاف عبر الحدود.

٦- وبالتالي فإن هاجس ضمانات حماية الخصوصية والانتصاف من انتهاكاتها يشكل عماد الدراسات المواضيعية التالية التي سيجريها المقرر الخاص في عدد من القطاعات التي يبدو أنها تنطوي على أكبر قدرٍ من المخاطر المتعلقة بالخصوصية. ومن المتوقع أن تفضي كل دراسة من هذه الدراسات إلى تقرير مخصص يعكس المشاورات والتفاعلات الجارية وما ينبثق عنها من ملاحظات.

١- الخصوصية والشخصية عبر الثقافات

٧- تلبي هذه الدراسة الحاجة إلى تحقيق فهم أفضل لما تعنيه الخصوصية، أو ما ينبغي أن تعنيه، عبر الثقافات في عام ٢٠١٦، على نحو وثيق الصلة بالعصر الرقمي الذي تتغلغل فيه شبكة الإنترنت بلا حدود. وعندما يطرح المقرر الخاص سؤال "لماذا الخصوصية؟" ويضع مسألة الخصوصية في إطار الحق الذي يشكل وسيلة لا غاية في ذاته، فإنه يتطلع إلى تحليل الحق في الخصوصية كوسيلةً لبلوغ الحق الجوهري الراسخ في تنمية شخصية الفرد بحرية ودون عائق. ويجري المقرر الخاص هذا التحليل في إطار من التعاون الوثيق مع العديد من المنظمات غير الحكومية، ومن المتوقع أن يكون هذا الموضوع محوراً لمؤتمر دولي هام يُزمع تنظيمه في عام ٢٠١٦. ويتموضع هذا التحليل أيضاً ضمن سياق أوسع يرمي إلى دراسة علاقة الحق في الخصوصية بالحقوق الأخرى الأساسية، حيث يُتوقع أن تُدرس علاقته مثلاً بحرية التعبير وحرية الوصول إلى المعلومات العامة من خلال عمل مشترك مع المقررين الخاصين الآخرين للأمم المتحدة. وهناك مناقشات جارية بالفعل مع المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، بهدف استكشاف فرص العمل المشترك بشأن هذا الموضوع خلال عامي ٢٠١٦ و٢٠١٧.

٢- نماذج الأعمال التجارية لشركات الإنترنت واستخدام البيانات الشخصية

٨- تمخضت الشبكة العالمية، على مدى ٢٥ عاماً من وجودها، عن نمو عضوي للشركات الخاصة يفتقر بشكل كبير إلى التنظيم، حيث تكاثرت هذه الشركات في بعض الأحيان لتتفرع إلى كيانات متعددة الجنسيات تنشط عبر الحدود وتجتذب عملاء من مختلف أنحاء العالم. وتمثلت إحدى العلامات الفارقة لهذا النمو في جمع البيانات الشخصية واستخدامها، حيث تترك كل عملية بحث أو قراءة لمادة منشورة، وكل تبادل لرسالة إلكترونية أو غير ذلك من وسائل تبادل الرسائل، وكل عملية شراء لمنتج أو خدمة على الإنترنت، مئات الآلاف من البصمات الإلكترونية التي يمكن تجميعها لتشكيل صورة دقيقة عن المستخدم، ما يميل إليه وما ينفر منه، ومزاجه، وقدراته المالية، وميوله الجنسية وحالته الصحية وأنماط تسوقه، فضلاً عن اهتماماته وآرائه الثقافية والسياسية والدينية والفلسفية. وهناك مسألة تُثار عموماً حول ما إذا كان لمقدمي خدمات معينة على الإنترنت الحق في تتبع السلوك الفردي لضمان الحصول على تعويض منصف. وهذه الخريطة التي تزداد بياناتها تفصيلاً عن سلوك المستهلك أدّت إلى تحويل البيانات الشخصية إلى سلعة أساسية. وأصبح الوصول إلى هذه البيانات واستغلالها أحد أهم القطاعات التجارية العالمية التي تدرّ إيرادات تُحصى بمئات مليارات الدولارات، معظمها يتخذ شكل إعلانات دعائية موجهة. ويبدو في كثير من الأحيان أن المستهلكين قد يكونون على وعي بالمحتوى الذي ينشرونه هم بأنفسهم على الإنترنت، غير أنهم أقل وعياً بكثير فيما يتصل بحجم ونوعية واستخدامات البيانات الكلية التي تتولد عن

استخدامهم للإنترنت، سواء من خلال التصفح أو الدردشة أو التسوق أو أي شكل آخر من أشكال التفاعل عبر الشبكة. فالبيانات المتاحة لتصنيف الأفراد اليوم تفوق أضعافاً مضاعفة ما كانت عليه قبل ٢٥ عاماً، فيما لا يتوفر فهم حقيقي كامل لنطاق مخاطر الخصوصية المرتبطة باستخدام هذه البيانات أو إساءة استخدامها. وهناك بعض الأدلة على أن تسليع البيانات الشخصية، وبخاصة في القطاعات التي تعتبر حساسة تقليدياً، كالبيانات الطبية، قد بلغ حدوداً تخفى على المستخدمين الذين إما لا علم لهم ببيع هذه البيانات أو إعادة بيعها، أو لا يوافقون على ذلك. ومن جهة أخرى، لا توجد أدلة كافية تسمح بإجراء تقييم سليم للمخاطر التي تحفّ بالبيانات التي يُزعم أنها مخفية الهوية، حيث يمكن هندسة هذه البيانات بشكل عكسي لربطها بشخص محدد. وهذه الانتهاكات لخصوصية الأفراد يمكن أن تعرضهم، بل وتعرّض المجتمعات المعنية، لمخاطر متعددة، لا سيما في حالة وصول جهات معينة لهذه البيانات بشكل غير مرخص، من قبيل سلطات الدولة العازمة على استخدام هذه البيانات لنيل السلطة أو الحفاظ عليها، وعصابات الإجرام المنظم أو الشركات التجارية التي تتصرف بصورة غير مشروعة. وكان أحد الشواغل الرئيسية في الأيام الأولى للحواسيب الرقمية، هو استخدام الدول للبيانات الشخصية وقدرتها على ربط البيانات المشتقة من مصادر متنوعة لتشكيل صورة مفصلة عن أنشطة فردٍ ما وأصوله. أما في عام ٢٠١٦، فيبدو أن البيانات الشخصية في حوزة الشركات قد فاقت بكثير ما تحوزه الدول. ولا شك أن الإيرادات الضخمة المنبثقة عن تسليع البيانات الشخصية تُضعف الحافز لتغيير نموذج هذه الأعمال التجارية مراعاةً للشواغل المتعلقة بالخصوصية. فبعض الشركات التي اتجهت لاتباع نهج أكثر صرامةً واحتراماً للخصوصية لم تفعل ذلك إلا عندما تعرضت إمكانات الربح التي يولدها هذا النموذج للتهديد مؤخراً لاعتبارات ترتبط بالخصوصية. وقد آن الأوان على ما يبدو لإجراء مناقشة عالمية، تستند إلى جمع الأدلة المعتبرة، من أجل تحديد الشكل الأنسب من سياسة المعلومات لتحقيق أقصى قدر من الحماية لخصوصية الأفراد والحد من المخاطر المرتبطة بالبيانات التي تجمعها عنهم الشركات. وستقوم هذه المناقشة على المفاهيم والتوقعات المتعلقة بالخصوصية التي يعرب عنها المواطنون. ومن المتوقع أن تُشرك المشاورات التي بدأت بالفعل في عام ٢٠١٥ الشركات القائمة على شبكة الإنترنت في عام ٢٠١٦، فيما يُخطط لتنظيم مشاورة عامة كبرى بشأن هذا الموضوع في عام ٢٠١٧.

٣- الأمن والمراقبة والتناسب والسلم في الفضاء الإلكتروني

٩- لم يزل هاجس الأمن الدولي مهيمناً على مستجدات عامي ٢٠١٥ و٢٠١٦. وقد كشفت عملية الرصد القُطري المشار إليها أعلاه أمثلة عديدة على تشريعات تُمرر على عجل عبر البرلمانات الوطنية في مسعى لشرعنة استخدام بعض التدابير التي تقتحم الخصوصية على يد أجهزة الأمن والمخابرات ووكالات إنفاذ القانون في هذه الدول. وقد أدّى استحداث هذه التدابير التشريعية في العديد من هذه البلدان، ولكن ليس في جميعها للأسف، إلى إثارة نقاش عام حول المسائل التالية:

(أ) مدى ملاءمة آليات الرقابة؛

(ب) الفرق بين المراقبة الموجهة والمراقبة الجماعية (أو المراقبة بالجملة كما تُدعى لتخفيف وقعها في بعض البلدان)؛

(ج) مدى تناسب هذه التدابير في مجتمع ديمقراطي؛

(د) تكلفة هذه التدابير من حيث فعاليتها ومدى كفاءتها إجمالاً.

١٠- وتتمثل الأهداف المعلنة لهذه التشريعات في مكافحة الإرهاب والجريمة المنظمة، فضلاً عن الجرائم الأخرى الحساسة اجتماعياً، كالميل الجنسي إلى الأطفال. وقد طُرحت في هذه النقاشات أدلة متضاربة تشير عادةً إلى أن التدابير التي تقتحم الخصوصية، وبخاصة المراقبة الجماعية، لن تفضي إلى تعزيز الأمن، وأن إخفاقات المعلومات الاستخباراتية ينبغي أن تُعالج بوسائل أخرى. وقد انتهج المقرر الخاص برنامج عمل مستمر مع وكالات إنفاذ القانون وأجهزة الأمن والمخابرات في مختلف أنحاء العالم، سعياً للتوصل إلى فهم أفضل للشواغل المشروعة لهذه الوكالات والأجهزة، وإبراز أفضل الممارسات التي يمكن تقاسمها لفائدة الجميع، وتحديد السياسات والممارسات والتشريعات المشكوك في جدواها أو التي تثير مخاطر غير مقبولة فيما يتعلق بالخصوصية، على الصعيدين الوطني والعالمي على السواء. وفي بعض الحالات، يرتبط هذا التحليل ارتباطاً لا ينفصم بمسألتي أمن الفضاء الإلكتروني والتجسس الإلكتروني. وهناك عدد قليل، ولكن متزايد، من الدول تتعامل مع الفضاء الإلكتروني كما لو كان مسرحاً لعمليات وكالات الأمن والاستخبارات، ويبدو أنها ليست على استعداد للتعاون مع بعضها البعض، وأحياناً حتى مع المقرر الخاص، بشأن هذه المسائل التي لا يُستغرب أن لها أثراً مباشراً كذلك على خصوصية المواطنين، بصرف النظر عن جنسياتهم. ومع أن المواطن العادي قد لا يكون بالضرورة الهدف الرئيسي لتدابير الأمن والتجسس في الفضاء الإلكتروني، فإنه قد يجد نفسه وسط هذا التراشق في نهاية المطاف وقد تتعرض بياناته الشخصية وأنشطته على الإنترنت للمراقبة باسم الأمن القومي، على نحو غير مبرر أو غير متناسب أو مفرط. ويعتبر المقرر الخاص نفسه محظوظاً لأنه، بمنأى عن العمل التحقيقي المخصص الذي يضطلع به في أداء ولايته، يجد في متناوله مصادر زاخرة بالأدلة من الأبحاث المستقلة الحالية والسابقة التي تُجرى في إطار من التعاون في ميدان الأمن، ولا سيما الأبحاث الممولة من الاتحاد الأوروبي[أ]. ويواصل المقرر الخاص دراسته هذه على أربع جبهات رئيسية هي التالية: (أ) قدرات الدول في مجال المراقبة المتناسبة في نطاقها والمقيدة بضمانات تشريعية وإجرائية وتقنية كافية، بما يشمل آليات رقابة محكمة؛ (ب) التركيز على المراقبة الموجهة، مقارنةً بالمراقبة الجماعية؛ (ج) وصول وكالات إنفاذ القانون وأجهزة الأمن والمخابرات إلى البيانات الشخصية في حوزة الشركات الخاصة والكيانات الأخرى غير الحكومية؛ (د) تحديد التركيز على السلم في الفضاء الإلكتروني. ويؤمن المقرر الخاص بشدة بأن المراقبة الإلكترونية والحرب المستعرة في الفضاء الإلكتروني يهددان بتدمير هذا الفضاء، وأن على الحكومات والجهات الأخرى صاحبة المصلحة

(أ) تشمل مشاريع من قبيل: CONSENT, SMART, RESPECT, SiiP, INGRESS, E-CRIME, EVIDENCE, MAPPING, CITYCoP وCARISMAND.

أن تعمل معاً لإرساء السلم في الفضاء الإلكتروني. وبهذا المعنى على الأقل، تكون حماية الخصوصية جزءاً من الحركة الأشمل نحو تحقيق السلم في الفضاء الإلكتروني. ويمكن للفضاء الإلكتروني بذلك أن يصبح حقيقةً ساحة رقمية يمكن للفرد أن يتوقع فيها احترام خصوصيته وأمنه، ورحبة مسالمة لا تهددها على الدوام أنشطة دول معينة، ناهيك عن تهديدات الإرهاب والإجرام المنظم.

٤- تحليل البيانات المفتوحة والبيانات الضخمة، وما لذلك من أثر على الخصوصية

١١- تتصدى إحدى أهم المسائل المتعلقة بسياسة المعلومات وإدارتها في العقد الثاني من القرن الحادي والعشرين لمسألة تحديد التوازن المناسب بين استخدام البيانات لفائدة المجتمع وفقاً لمبادئ البيانات المفتوحة من جهة، والمبادئ التي وُضعت حتى الآن بهدف حماية الحقوق الأساسية، كالخصوصية والاستقلال وتنمية الفرد شخصيته بحرية، من جهة أخرى. ويرِد في المرفق الثاني سرد أكثر تفصيلاً لشواغل المقرر الخاص على هذا الصعيد.

٥- علم الوراثة والخصوصية

١٢- يلاحظ المقرر الخاص أن ربع الدول الأعضاء تقريباً لديها قواعد بيانات وطنية جنائية للحمض النووي. ويمكن لقواعد البيانات هذه أن تضطلع بدور هام في حل ملابسات جرائم كثيرة، غير أنها تثير أيضاً شواغل تتعلق بحقوق الإنسان، بما في ذلك إمكانية إساءة استخدامها لأغراض المراقبة الحكومية (تحديد الأقارب وإثبات النسب مثلاً) ومخاطر إنكار العدالة. علاوة على ذلك، يبدو أن هناك اتجاهاً متزايداً نحو استخدام قاعدة بيانات الحمض النووي لأغراض إدارية، كإصدار بطاقات الهوية أو إجراءات الهجرة. ومن المرجح أن تُتخذ خلال الأعوام القليلة المقبلة خطوات نحو إنشاء قاعدة بيانات للحمض النووي تشمل المواطنين كافة. وقد تجددت الشواغل التي أثيرت في التسعينات حول استخدام البيانات الجينية في قطاع التأمين، حيث يُتوقع أن يؤدي الاتجاه نحو شخصنة الطب إلى تقديم العديد من الأشخاص بياناتهم الجينية كاملةً بمحض إراداتهم إلى قطاع الرعاية الصحية. وفي ظل هذه المخاوف وغيرها، هناك حاجة مستمرة إلى نقاش عام وسياساتي موسع مع تزايد استخدام قواعد بيانات الحمض النووي حول العالم. ويعتزم المقرر الخاص مواصلة الانخراط في مشاريع تهدف إلى وضع معايير دولية لقواعد بيانات الحمض النووي من منظور حقوق الإنسان، عن طريق بلورة ممارسات فضلى في هذا المجال وإشراك الخبراء ومقرري السياسات وعامة الجمهور في نقاش مفتوح بهذا الصدد. ومن المنتظر أن يسهم هذا التفاعل في صوغ مبادئ توجيهية بشأن أفضل الممارسات اللازم تحديدها بمُدخلات ومساهمات من الجهات الفاعلة في المجتمع المدني.

٦- الخصوصية والكرامة والسمعة

١٣- قد تكون الشواغل المتعلقة بالأمن والمراقبة مسؤولة عن حرف الانتباه عن الشواغل الأخرى التي تتقاسمها شريحة واسعة من المواطنين بشأن الأشكال التي تتعرض بها خصوصيتهم وكرامتهم وسمعتهم للمخاطر على الإنترنت. فالعصر الرقمي هو ثمرة التطورات والتغيرات التي شهدتها وسائط الإعلام على مدى العقدين الماضيين، لا سيما الطريقة التي مكّنت بها الإنترنت

المواطنين العاديين الذين لم يتلقوا تدريباً رسمياً في الميدان الصحافي، من نشر المواد المكتوبة والمسموعة والمرئية كيفما ارتأوا وفي أي وقت شاؤوا. لقد أكسبت هذه التطورات المواطنين قدرات كبيرة، لا سيما في الحالات التي يتمكنون فيها من تفادي الرقابة أو العوائق الأخرى، أو في الحالات التي تيسّر فيها التكنولوجيا حرية التعبير على نحو يعزز الديمقراطية في المجتمع. غير أن ظاهرة المواطنين – الصحافيين والمدونين في ساحة إعلامية سريعة التغير، مقترنةً بالانتشار الكاسح لوسائط الإعلام الاجتماعي، أثارت في المقابل هاجساً عاماً بشأن إساءة استعمال الحق في حرية التعبير على نحو يؤثر سلباً على حقوق الإنسان الأساسية الأخرى، كالحق في الخصوصية وفي الكرامة. وقد سلّطت الأبحاث التي أجريت خلال الأعوام الخمسة الماضية الضوء على المخاوف المتزايدة للمواطنين إزاء سهولة تعرّض أسمائهم وسمعتهم للهجوم والتخريب على الإنترنت، فضلاً عن الشعور المتنامي بقلة الحيلة لدى العديد من مواطني الإنترنت في سعيهم للحصول على ضمانات وسبل انتصاف في حالات التشهير و/أو انتهاك الخصوصية. ويودّ المقرر الخاص أن يتعاون مع المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، والمجتمع المدني، ووكالات الأمم المتحدة الأخرى مثل منظمة الأمم المتحدة للتربية والعلم والثقافة، من أجل استكشاف مجموعة من الضمانات الملموسة لحماية خصوصية الفرد وكرامته وسمعته على الإنترنت، مشفوعةً بسبل الانتصاف في حال انتهاك هذه الضمانات. وتظل العلاقة بين الخصوصية وإدارة الإنترنت، شأنها شأن الدراسات المواضيعية الأخرى المبينة أعلاه، واحدة من المسائل الأساسية المتكررة التي تتصل أيضاً بالخصوصية والكرامة والسمعة.

٧- علم الأحياء القياسي والخصوصية

١٤- تشير دراسة استقصائية للأبحاث الحالية في هذا المجال إلى حدوث طفرة كبيرة في الاهتمام باستخدام علم الأحياء القياسي لأغراض متنوعة تتراوح من إنفاذ القانون إلى الاستفادة الشخصية من الأجهزة النقالة. وليس التعرف الصوتي، ومسح الشبكية، والتعرف على الهيئة وملامح الوجه، وتكنولوجيا بصمات الأصابع السطحية وتحت الجلدية، سوى أمثلة على التكنولوجيات الرقمية العديدة التي يجري تطويرها ونشرها لخدمة أغراض متنوعة في العقد الثاني من القرن الحادي والعشرين. ويعتزم المقرر الخاص مواصلة التعاون مع مجتمع الأبحاث البيومترية ووكالات إنفاذ القانون وأجهزة الأمن والمخابرات والمجتمع المدني، في سعيه للمضي في بلورة الضمانات وسبل الانتصاف المناسبة فيما يتصل باستخدام الأدوات البيومترية.

جيم- الشكاوى الفردية

١٥- تلقى المقرر الخاص، وسيظل يتلقى على الأرجح خصوصاً عندما تُعمم ولايته على نطاق أوسع، شكاوى من أفراد وجهات فاعلة في المجتمع المدني بخصوص انتهاكات مزعومة للحق في الخصوصية. وتجري متابعة هذه الشكاوى من خلال التراسل مع أصحابها والسلطات الحكومية المعنية على السواء. وتُجرى اتصالات المتابعة وفقاً للمنهجية التي يستخدمها المكلفون بولايات الإجراءات الخاصة، والتي تهدف إلى استيضاح الادعاءات المقدمة وتقصي الحقائق وتقديم توصيات بشأن الإجراءات التصحيحية المنشودة، عند الاقتضاء. وقد تنطوي هذه

الاتصالات أيضاً على مقابلات إلكترونية أو شخصية حسبما يلزم. وإذا استدعت الأدلة الواردة اهتماماً خاصاً أو عاجلاً، ولم تلق أشكال الاتصال العادية رداً مناسباً، فقد ينظر المقرر الخاص في إصدار بيان عام للإعراب عن قلقه.

دال- الإجراءات المشتركة

١٦- يتلقى المقرر الخاص طلبات منتظمة من المقررين الخاصين الآخرين لاتخاذ إجراءات مشتركة، وأحياناً يباشر بنفسه هذه الطلبات. وتُنشر تفاصيل هذه الإجراءات المشتركة على حدة في التقارير المتعلقة بالبلاغات في إطار الإجراءات الخاصة.

١٧- وإلى حين ٥ آذار/مارس ٢٠١٦، لم يتسن الوقت لجمع أدلة كافية في أي فئة من الفئات المذكورة أعلاه سوى المشاركة في إجراءين من الإجراءات المشتركة. غير أنه يُنتظر تجميع البيانات المحصلة في كل فئة لإرساء الأسس الاستدلالية المطلوبة لمواصلة الحوار والتعاون بين المقرر الخاص والدول المعنية، بوسائل تشمل الاتصالات والزيارات القطرية وغير ذلك من سبل التعاون.

هاء- بناء الجسور وسياسة الانخراط

١٨- استخدم المقرر الخاص ولايته لمواصلة وتوسيع العمل الجاري سابقاً لبناء الجسور مع أصحاب المصلحة وفيما بينهم. وتمخض هذا العمل عن سياسة مستمرة تقوم على الانخراط مع جميع أصحاب المصلحة، بما يشمل، على سبيل المثال لا الحصر، العمل مع المسؤولين الحكوميين والوزراء في العواصم أو في الاجتماعات الثنائية في المحافل العالمية؛ والاجتماعات مع العديد من مفوضي الخصوصية وحماية البيانات، ولا سيما رئيس فريق العمل المعني بالمادة ٢٩ للاتحاد الأوروبي، ورئيس اللجنة الاستشارية لمجلس أوروبا بشأن اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، والمناقشات مع هيئات المعايير التقنية، كالاتحاد الدولي للاتصالات ومعهد المهندسين الكهربائيين والإلكترونيين؛ واجتماعات معمقة، فردية وجماعية، مع الجهات الفاعلة في المجتمع المدني؛ واجتماعات مع أخصائيي حقوق الإنسان أو المسؤولين الآخرين من البعثات الدائمة في جنيف. وترِد دعوات شبه يومية لإلقاء خطابات أو المشاركة في مناقشات خبراء ومؤتمرات واللقاء مع ممثلي المجتمع المدني. وفي حين يُقبل العديد من هذه الدعوات، لا سيما التي تتعلق منها مباشرة بالدراسات المواضيعية السبع المذكورة أعلاه، فقد اضطر المقرر الخاص إلى رفض العديد منها، وبخاصة عندما تتعذر المشاركة لأسباب تتعلق بضيق الوقت و/أو قيود الميزانية. وقد تمخضت سياسة الانخراط هذه عن نتائج عديدة، منها اعتماد قرار يضفي طابعاً رسمياً على التعاون مع السلطات المعنية بالخصوصية وحماية البيانات[ب]، اعتمده المؤتمر الدولي لمفوضي الخصوصية وحماية البيانات.

(ب) اعتُمد في المؤتمر الدولي لمفوضي الخصوصية وحماية البيانات، المعقود في ٢٧ تشرين الأول/أكتوبر ٢٠١٥ في أمستردام. متاح على الرابط: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

ثالثاً- الخصوصية في مطلع عام ٢٠١٦

ألف- التعريف والفهم

١٩- مع أن مفهوم الخصوصية لم يغب قط عن أي من المجتمعات والثقافات في أي مرحلة من مراحل التاريخ البشري، فليس هناك تعريف ملزم ومقبول عالمياً لهذا المفهوم[ج]. ولتحقيق فهم أشمل للحق في الخصوصية لا بد من تناوله من منظورين مختلفين. فأولاً، ينبغي النظر فيما يشمله المحور الإيجابي لهذا الحق. وثانياً، ينبغي تناول السؤال المطروح حول كيف يمكن حصر هذا الحق من منطلق التعريف السلبي. ولم تُنجز بعد أي من هاتين المهمتين.

٢٠- وقد أكّد مجلس حقوق الإنسان مجدداً في قراره ١٦/٢٨ أن المادة ١٢ من الإعلان العالمي لحقوق الإنسان والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية تشكلان ركيزة الحق في الخصوصية في القانون الدولي لحقوق الإنسان. وعندما تُقرن هاتان المادتان مع عدد من الصكوك القانونية الدولية والوطنية، بما فيها الدساتير والتشريعات ذات الصلة، فإن ذلك يعني أن ثمة إطاراً قانونياً عالمياً قد يكون مجدياً لحماية الخصوصية وتعزيزها. غير أن ما يحدّ من جدواه بشدة هو غياب تعريف للخصوصية يكون مقبولاً ومتفقاً عليه عالمياً. وحتى لو وقّعت ١٩٣ دولة على مبدأ حماية الخصوصية، فلن يكون لذلك جدوى تُذكر ما لم يكن هناك فهم واضح لما وافقت هذه الدول على حمايته.

٢١- وليس غياب هذا التعريف المقبول والمتفق عليه عالمياً هو التحدي الوحيد الرئيسي الذي يواجه المقرر الخاص. فحتى لو تضمنت جميع الصكوك القانونية ذات الصلة تعريفاً متفقاً عليه عالمياً للخصوصية، فستظل هناك أبعاد أخرى يتعين تناولها تتعلق بالزمان والمكان والاقتصاد والتكنولوجيا. فمرور الزمن وتأثير التكنولوجيا، مقترنين بتفاوت مستويات التنمية الاقتصادية وتغلغل التكنولوجيا في مختلف المناطق الجغرافية، يعني أن المبادئ القانونية التي أرسيت قبل ٥٠ عاماً (أي حين اعتُمد العهد الدولي الخاص بالحقوق المدنية والسياسية) أو حتى قبل ٣٥ عاماً (حين اعتُمدت مثلاً اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية)، ناهيك عن قبل ٧٠ عاماً (الإعلان العالمي لحقوق الإنسان)، باتت بحاجة إلى إعادة النظر فيها وزيادة تطويرها، بل ربما توطيدها واستكمالها لتصبح أكثر تواؤماً مع وقائع اليوم.

٢٢- ونظراً لغياب تعريف للخصوصية متفق عليه عالمياً ولاعتبارات الزمان والمكان والاقتصاد والتكنولوجيا، فمن الواضح أن ثمة حاجة إلى تأسيس فهم لما تعنيه الخصوصية لأناس مختلفين في أماكن مختلفة وظروف متباينة في مختلف أنحاء المعمورة. ومن البديهي أن هذا المسعى لا يبدو مهمة فائقة الأهمية فحسب، بل أولوية عليا بالنسبة للمقرر الخاص.

(ج) للاطلاع على تصور مفصل لتقييم المقرر الخاص بشأن البُعد الزماني والمكاني والتاريخي للخصوصية عبر الألفية، انظر Joseph A. Cannataci, ed., *The Individual and Privacy*. *Volume I* (Oxford, Ashgate, 2015).

٢٣- وفي بعض الثقافات يتطرق النقاش بشأن الخصوصية إلى مسألة الإجهاض. ودون الخوض في حيثيات هذا النهج، ولتفادي أي لبس بهذا الشأن، ينبغي الإشارة بوضوح، في هذه المرحلة المبكرة من الولاية، إلى أن تركيز المقرر الخاص سيكون على الخصوصية المعلوماتية. ومن هذا المنطلق، سيركز نهجه على وظيفة ودور الخصوصية في تحديد تدفقات المعلومات في المجتمع وما يترتب عليها من أثر على تنمية شخصية الفرد. وسيتضمن النهج أيضاً المسائل ذات الصلة، كتوزيع النفوذ والثروة داخل المجتمع. غير أن ما سيتضح في هذا المسعى، هو أن الخصوصية ليست المسألة الوحيدة المؤثرة على تدفق المعلومات في مجتمع ما، وإنما هناك حقوق أخرى مؤثرة أيضاً، كحرية التعبير وحرية الوصول إلى المعلومات العامة. فجميع هذه الحقوق هامة والالتزام بأحدها لا ينفي أهمية حق آخر أو يتعارض مع حمايته. والنظر إلى الحقوق من منظور الاقتران كلما أمكن أجدى وأنجع من النظر إليها من منظور التعارض. وبعبارة أصح، لا يجدر الحديث عن "الخصوصية مقابل الأمن" وإنما الأصح الحديث عن "الخصوصية والأمن"، إذ لا يغني أحدهما عن الآخر، وكلاهما وسيلة حقوقية لا غاية في ذاته. فالحق في الأمن وسيلة لإعمال الحق الأنبل في الحياة، كما أن الحق في الخصوصية وسيلة لإعمال الحق في الشبكة المعقدة لتدفقات المعلومات في المجتمع، بما لها من أهمية جوهرية في تحقيق استقلالية الفرد وقدرته على تحديد خياراته على نحو مستنير في إطار سعيه إلى تنمية شخصيته في سيرورة حياته.

٢٤- وعندما يُطرح النقاش حول ماهية الخصوصية وما ينبغي أن تكونه، يودّ المقرر الخاص التركيز على الأساسيات وتفادي حرف النقاش إلى الفوارق المحلية أو الثقافية، المتصورة أو الحقيقية، لما تعنيه الخصوصية، بدلاً من التركيز على الجوهر الراسخ لقيم الخصوصية التي قد يتبين لاحقاً أنها تحظى بتوافق عالمي. وللمساعدة على إجراء حوار منهجي ومتجدد حول الأساسيات، يعتزم المقرر الخاص، على نحو لا يخلو من بعض الاستفزاز المقصود، أن يطرح الخصوصية بوصفها حقاً يشكل وسيلة لا غاية في ذاته. فقد أرست بلدان عديدة حول العالم حقاً أساسياً للفرد في الكرامة وفي تنمية شخصيته بحرية ودون عائق. ودونت بلدان متباعدة جغرافياً، كالبرازيل وألمانيا، هذا الحق في دساتيرها. ومن هذا المنطلق، يحتج المقرر الخاص بما يلي: (أ) أن الحق في الكرامة وفي تنمية شخصية الفرد بحرية ودون وعائق ينبغي أن يعتبر حقاً منطبقاً عالمياً؛ (ب) أن الحقوق المعترف بها أصلاً، كالحق في الخصوصية وفي حرية التعبير وفي الوصول إلى المعلومات، تشكل ثلاثياً من الحقوق التي تعدّ أفضل وسيلة لتمكين أي إنسان من تنمية شخصيته بحرية. فطرح الخصوصية، بل طرح سؤال "لماذا الخصوصية؟"، في سياق نقاش أوسع بشأن الحق الأساسي في الكرامة وفي تنمية شخصية الفرد بحرية ودون عوائق، يعكس وقائع الحياة في هذا العصر الرقمي. واعتماد نهجٍ من هذا النوع من شأنه أن يساعد جميع المشاركين في النقاش، بصرف النظر عن بلدهم أو ثقافتهم، على التركيز على أساسيات تنمية شخصية الفرد ونوع الحياة التي يُطمح أن تساعد الخصوصية في حمايتها، بدلاً من هدر الكثير من الوقت في مناقشة أي التقاليد المتعلقة بالخصوصية في ثقافة معينة ينبغي التركيز عليها أو الدفاع عنها أو الترويج لها.

٢٥- وسيُلاحظ أن النقاش حول الخصوصية لا ينفك، في كثير من الحالات، عن النقاش بشأن قيمة الاستقلالية أو تقرير المصير. وقد أُشبع المصطلح الأخير نقاشاً وتمخض، فيما يتعلق بالحق في الخصوصية وفي تنمية الشخصية، عن تبني الحق الدستوري في "تقرير المصير المعلوماتي" في ألمانيا في عام ١٩٨٣. وهناك حاجة إلى زيادة تقييم صحة هذا المفهوم وجاذبيته في سياق نقاش عالمي بشأن كيف يمكن فهم الحق في الخصوصية بشكل أفضل في عام ٢٠١٦، ربما في سياق نقاش حول حماية وتعزيز الحق في الكرامة وفي تنمية شخصية الفرد بحرية ودون عائق.

٢٦- ولا يخفى أن وجود الحقوق الثلاثة السابقة الذكر - أي الخصوصية وحرية التعبير وحرية الوصول إلى المعلومات - سابق لظهور التكنولوجيات الرقمية، شأنها شأن الحق في الكرامة وفي تنمية شخصية الفرد بحرية ودون عائق. غير أن للتكنولوجيا الرقمية تأثيراً هائلاً على هذه الحقوق، سواء خارج الإنترنت (عن طريق بطاقات الائتمان وأجهزة التعرف الراديوي وغير ذلك من النُظم الإلكترونية مثلاً) أو عبر شبكة الإنترنت، حيث يولدّ مواطنو الإنترنت عشرات الآلاف من حزم البيانات عن أنفسهم قياساً بما كان معلوماً عنهم قبل عقدين من الزمان، أي قبل أن يصبحوا مواطنين في هذه الشبكة. وقد تمخضت الأجهزة النقالة والتكنولوجيات المتقاربة، كالهواتف الذكية المحمولة - حيث تتلاقى وظائف الاتصال الهاتفي والإنترنت والتصوير الفوتوغرافي - عن أنماط حياة جديدة وأشكال رفاهية جديدة وتوقعات جديدة على صعيدي الراحة الشخصية والخصوصية معاً.

٢٧- ويعني تأثير التكنولوجيات الجديدة أيضاً أن الفرق بين الخصوصية الفردية والجماعية قد يحتاج إلى إعادة النظر فيه، شأنه شأن توقعات الخصوصية في المجالين العام والخاص، في سياق الحق في الكرامة وفي تنمية شخصية الفرد بحرية ودون عائق.

باء- ملاحظات أولية في عامي ٢٠١٥ و٢٠١٦

٢٨- يصعب تحديد أهم الأحداث التي وقعت فيما يتعلق بالخصوصية منذ تسلم المقرر الخاص ولايته، لا سيما لعدم توفر الموارد اللازمة للتحقيق بدقة في هذه الأحداث. ولا يريد المقرر الخاص الانتقاص من الدور الذي يؤديه المجتمع المدني، كالمنظمة الدولية لحماية الخصوصية ومنتسبيها، التي دأبت على تنظيم حفل جوائزها السنوي[د] طوال عشرين عاماً، مسلطةً الضوء على أحسن الممارسات وأسوئها في مجال الخصوصية. ومن جهة أخرى، يود المقرر الخاص أن يشيد بالممارسات الجيدة والقوانين وقرارات المحاكم وحتى الأفكار التي تشجع وتعزز حماية الخصوصية. ومن هذا المنطلق، يود المقرر الخاص أن يعرض التطورات الهامة التالية على مجلس حقوق الإنسان، دون أن يزعم أنها قائمة حصرية ودون ترتيب معين لبنودها.

(د) www.bigbrotherawards.org.

١- إحجام حصيف - لا لاتصالات الأبواب الخلفية في هولندا والولايات المتحدة الأمريكية

٢٩- تجدر الإشادة بحكومتي هولندا والولايات المتحدة الأمريكية لما أبدتاه من وازع في عدم السماح باستخدام القانون لهندسة أبواب اتصالات خلفية. ففي ٤ كانون الثاني/يناير ٢٠١٦، أُعلن رفض حكومة هولندا رسمياً استحداث أبواب خلفية في منتجات التشفير. وفي ورقة رسمية تعبر عن موقف الحكومة(هـ)، نشرتها وزارة الأمن والقضاء ووقعها وزيرا الأمن والأعمال التجارية، قالت الحكومة إن الوقت ليس مناسباً لاعتماد تدابير قانونية تقيد تطوير برمجيات التشفير وتوفيرها واستخدامها في هولندا. وجاءت هذه النتيجة خلاصة لورقة من خمس صفحات تضمنت الحجج المؤيدة لتعزيز التشفير والمناوئة لتمكين السلطات من الوصول إلى المعلومات المشفرة. فتضمين منتجات التشفير منفذاً يسمح للسلطات بالوصول إلى الملفات المشفرة يجعل هذه المعلومات أكثر عرضة لوصول المجرمين والإرهابيين وأجهزة المخابرات الأجنبية كذلك. وسيؤثر ذلك سلباً على أمن المعلومات المخزنة والمتبادلة وسلامة نُظم تكنولوجيا المعلومات والاتصالات، التي أصبحت لها أهمية متزايدة في سير المجتمع.

٣٠- ويبدو موقف الحكومة الهولندية أكثر حزماً من موقف حكومة الولايات المتحدة الذي سبق موقفها بنحو ثلاثة أشهر. ففي مطلع تشرين الأول/أكتوبر ٢٠١٥، قال مدير مكتب التحقيقات الاتحادي، جميس كومي الابن، في شهادته أمام الكونغرس الأمريكي إن الإدارة ليست اليوم في وارد المطالبة بتشريع يرغم الشركات على كشف البيانات المشفرة للعملاء. ولعل ما يثير القلق أكثر هو أن إدارة الولايات المتحدة، مثلما انكشف في القضية التي رُفعت مؤخراً ضد شركة أبل، ستواصل سعيها لإقناع الشركات التي تشفر بيانات عملائها بإتاحة منفذ للحكومات للاطلاع على بيانات الأشخاص عندما تستدعي ذلك التحقيقات الجنائية أو المتعلقة بالإرهاب. ويعكس بيان مفوض الأمم المتحدة السامي لحقوق الإنسان الذي أدلى به في ٤ آذار/مارس ٢٠١٦ بشأن هذه القضية(و)، إلى حد كبير موقف المقرر الخاص بصفته المستقلة. وتعدّ آخر تعليقات أدلى بها وزير الدفاع الأمريكي، أشتون كارتر، وقال فيها إن التشفير المحكم ضروري لحفظ أمن الوطن، تصريحات مشجعة في هذا الصدد. فقد قال في حديثه أمام جمهور يتألف من أخصائيين في قطاع التكنولوجيا يوم ٢ آذار/مارس ٢٠١٦، إنه لا يؤمن بالأبواب الخلفية أو ببرامج التشفير التي تترك ثغرات يطّلع منها المتطفلون على ملفات مشفرة. ويتسق قوله هذا مع التصريحات التي أدلى بها في تشرين الأول/أكتوبر ٢٠١٥(ز) ويعبر عن موقف جدير بالتشجيع والدعم.

(هـ) متاحة على الرابط: www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015 (اطُلع على الرابط في ٢٣ آب/أغسطس ٢٠١٦).

(و) انظر الرابط: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E.

(ز) انظر الرابط: http://europe.newsweek.com/us-defense-secretary-ashton-carter-doesnt-believe-encryption-backdoors-432811?rm=eu.

٢- بداية النهاية القضائية للمراقبة الجماعية – المسألة الموضوعية

٣١- في ٦ تشرين الأول/أكتوبر ٢٠١٥، أصدرت محكمة العدل التابعة للاتحاد الأوروبي حكماً في قضية *مكسيمليان شريمس ضد مفوض حماية البيانات*، أعلنت فيه عن بطلان القرار الصادر عن المفوضية الأوروبية الذي أنشئ بموجبه ما يُدعى إطار "الملاذ الآمن" والمستند إلى الأمر التوجيهي 95/46/EC. ويود المقرر الخاص التشديد على ما يمكن اعتبارها من أهم فقرات هذا الحكم من منظور (إنشاء) وتأكيد نهج يشكل سابقة في هذا المجال:

> ٩٤- وبشكل خاص، يجب أن يُنظر إلى التشريعات التي تسمح للسلطات العامة بالوصول على أساس معمم إلى محتوى الاتصالات الإلكترونية على أنه يفرط بجوهر الحق الأساسي في احترام الحياة الخاصة، على النحو الذي تكفله المادة ٧ من الميثاق ....

٣٢- ولا شك أن جدلاً ما سيدور حول المعنى الدقيق لعبارة "الوصول على أساس معمم" في هذا الحكم، ومن الواضح أن المحكمة تشير إلى محتوى الاتصالات في قبالة البيانات الكلية، غير أنه سيكون من الصعب على أي قانون أوروبي يرمي إلى شرعنة المراقبة الجماعية أن يتجاوز مقتضيات هذا المعيار إذا صممت المحكمة على التمسك بتطبيقه بحذافيره. ويتبدد الغموض مع ذلك جزئياً على الأقل، عندما يُقرأ الحكم المتعلق بقضية *شريمس* بالاقتران مع الحكم الصادر في قضية *زاخاروف* المذكورة أدناه، والذي يشكل قانوناً للاتحاد الأوروبي بقدر ما يشكل قانوناً في الدول الأعضاء في مجلس أوروبا.

٣- أهمية الحصول على سبيل انتصاف – الإنفاذ والمسائل الإجرائية

٣٣- بالإشارة مجدداً إلى قضية *شريمس*، يرحب المقرر الخاص بحقيقة أن محكمة العدل أصبحت منبراً لأشخاص مثل صاحب الشكوى، الذي بدأ القضية كفرد معني بتبعات تطور تكنولوجيا المعلومات العصرية على كرامته كإنسان في مجتمع ديمقراطي. وتشكل الفرصة المتاحة للأفراد كي يعرضوا قضيتهم ويدافعوا عن حقوقهم أمام مؤسسة عامة فوق وطنية، متحدين بذلك تجاذبات القوى القائمة، عنصراً أساسياً في توليد المعرفة اللازمة لتعزيز رفاه المجتمع على نحو يتسق مع تطور القانون الدولي لحقوق الإنسان. ووجود مثل هذه الآليات هو أمر فائق الضرورة لحماية حقوق الإنسان واستعادة الثقة في استخدام التكنولوجيا سواء من جانب الدول أو الجهات الفاعلة الأخرى.

٣٤- وتبشر هذه القضية أيضاً بتطور جديد في المجتمع، إذ تسلط الضوء على أهمية احترام الحقوق وإعمالها في كل مكان وليس في المكان الذي توجد فيه خوادم البيانات فقط.

٣٥- ويدلّ الحكم الصادر عن محكمة العدل أيضاً على القيمة المضافة لنُهُج السياسات الإقليمية التي قد تُستخدم في المستقبل للترويج لصكوك قانونية قائمة على المشاركة تنطلق من القاعدة إلى القمة وتحقق انتشاراً عالمياً أوسع.

٤- مجرد وجود تدابير مراقبة سرية يشكل انتهاكاً للحق في احترام الحياة الخاصة

٣٦- خلصت الدائرة الكبرى للمحكمة الأوروبية لحقوق الإنسان، في حكمها الصادر في ٤ كانون الأول/ديسمبر ٢٠١٥ في قضية *رومان زاخاروف ضد روسيا*[ح]، إلى قرار يُجمع على أن النظام الروسي للتجسس على اتصالات الهواتف النقالة يشكل انتهاكاً للمادة ٨ من اتفاقية حماية حقوق الإنسان والحريات الأساسية (الاتفاقية الأوروبية لحقوق الإنسان). ومما يثير الاهتمام إضافة إلى ذلك أن المحكمة قبلت بأن بمقدور صاحب الطلب، إذا توفرت شروط معينة، أن يدّعي وقوعه ضحية انتهاك المادة ٨ من الاتفاقية لمجرد وجود تدابير مراقبة سرية. ولعل التطور الأهم هو إعلان المحكمة عدم قانونية نُظم المراقبة الجماعية على نحو جازم أكثر مما أبدته محكمة العدل في قضية *شريمس*:

> ٢٧٠- إن المحكمة ترى أن الأسلوب الذي يعمل به نظام المراقبة السرية في روسيا يتيح لأجهزة الأمن والشرطة وسيلة تقنية للالتفاف على إجراء طلب الترخيص واعتراض أي اتصالات دون الحصول على إذن قضائي مسبق. ومع أن إمكانية صدور فعل غير سوي من مسؤول يتصف بعدم النزاهة أو الإهمال أو الحماس المفرط هي إمكانية لا يمكن نفيها بالكامل أياً كان هذا النظام (انظر قضية *كلاس وآخرين*، المشار إليها أعلاه، الفقرة ٥٩) فإن المحكمة ترى أن نظام مراقبةٍ كالنظام الروسي، يمكّن الأجهزة السرية والشرطة من اعتراض اتصالات كل مواطن مباشرة ودون تقديم ترخيص بالمراقبة لمقدم خدمة الاتصالات أو لأي شخص آخر، هو نظام معرّض لإساءة الاستعمال بشكل خاص. وتبدو الحاجة من ثم كبيرة تحديداً إلى ضمانات تحمي من العشوائية وإساءة الاستعمال.

٣٧- ويؤسس هذا القرار معلماً فائق الأهمية يسلط الضوء على متطلبات الشك المعقول والإذن القضائي السابق فضلاً عن إبرازه الطابع غير المقبول "لنظام ... يمكّن الأجهزة السرية والشرطة من اعتراض اتصالات كل مواطن مباشرة ودون تقديم إذن بالمراقبة". ويشكل ذلك بالتالي المحك الذي ينبغي أن تُعرض عليه جميع التشريعات القائمة والمقترحة بشأن المراقبة في أي بلد أوروبي. ويلاحظ المقرر الخاص بقلق بالغ أيضاً التقارير المتعددة بشأن قرار مجلس الدوما (البرلمان) الروسي الذي يسمح بإبطال قرارات المحكمة الأوروبية لحقوق الإنسان[ط]. وإذا ثبتت صحة هذه التقارير، فإن ذلك قد يؤدي في واقع الممارسة إلى حرمان مواطني البلدان التي صدّقت على الاتفاقية الأوروبية لحقوق الإنسان من سبيل هام للغاية من سبل الانتصاف المتاحة إليهم، بما في ذلك في حالات انتهاك الحق في احترام الحياة الخاصة. ويدعو المقرر الخاص حكومة الاتحاد الروسي إلى مساعدته في تحري صحة هذه التقارير وبحث القانون المعني بمزيد من العناية وإقناع

(ح) *Roman Zakharov v. Russia* [GC], 4 December 2015, no. 47143/06, Reports of Judgments and Decisions.

(ط) انظر الرابط: www.bbc.com/news/world-europe-35007059.

مجلس الدوما، إذا ثبتت دقة التقارير المذكورة، بإلغاء قانون ٤ كانون الأول/ديسمبر ٢٠١٥ وبالتالي استعادة فعالية سبل الانتصاف المتاحة للمواطنين الروس بموجب الاتفاقية الأوروبية لحقوق الإنسان، بما فيها سبل الانتصاف من الدولة في حالة تعرض حقهم في الخصوصية للانتهاك.

٥- مشروع قانون السلطات التحقيقية للمملكة المتحدة لبريطانيا العظمى وآيرلندا الشمالية

٣٨- يجدر التنويه بلجان برلمانية ثلاث للمملكة المتحدة، هي لجنة العلم والتكنولوجيا (١ شباط/فبراير ٢٠١٦)، واللجنة البرلمانية للمخابرات والأمن (٩ شباط/فبراير ٢٠١٦)، وأهمها اللجنة المشتركة بشأن مشروع قانون السلطات التحقيقية نفسها (١١ شباط/فبراير ٢٠١٦)، لما وجهته من انتقادات متسقة وصارمة، وإن كانت مفرطة التهذيب في بعض الأحيان، لمشروع قانون السلطات التحقيقية المعروض حالياً على البرلمان. فقد أدرجت اللجنة المشتركة بشأن مشروع قانون السلطات التحقيقية في تقريرها ٨٦ توصية لإدخال تغييرات على مشروع القانون، مركزةً على مسائل الوضوح والرقابة القضائية وتبرير مختلف السلطات. ويجدر التنويه كذلك بحكومة المملكة المتحدة، التي استمعت إلى مشورة مختلف الأوساط وتستخدم مشروع القانون حالياً لتعزيز آليات الرقابة اللازمة بشدة. وقد يظل هناك متسع للتحسين في هذا المجال، غير أن الخطوات المتخذة تسير في المسار الصحيح. ومع ذلك، فإن ثمة شواغل جسيمة لدى المقرر الخاص، في وقت تقديم هذا التقرير، بشأن جدوى بعض التنقيحات التي أُدخلت مؤخراً على النسخة الأخيرة من مشروع القانون والتي نُشرت في ١ آذار/مارس ٢٠١٦. وحتى وقت كتابة هذا التقرير، يبدو أن بعض مقترحات الحكومات تسير ليس فقط عكس منطق واستنتاجات المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، في تقريره لعام ٢٠١٤ الذي يركز في جملة أمور على مسألة المراقبة الجماعية(ي)، لكنها تتخلف بوضوح أيضاً عن المعايير التي أرستها محكمة العدل في قضية *شريمس* والمحكمة الأوروبية لحقوق الإنسان في قضية *زاخاروف*. ويشجع المقرر الخاص بشدة اللجان الثلاث التي أشاد أعلاه بجهودها، على مواصلة ممارسة نفوذها بعزم وهمة متجددين، لرفض التدابير غير المتناسبة والاقتحامية، كالمراقبة بالجملة والاختراق الحاسوبي بالجملة على النحو الذي يتوخاه مشروع القانون، بدلاً من شرعنتها. وإذا أُخذ في الحسبان ما لتشريعات المملكة المتحدة من نفوذ كاسح في قوانين ربع الدول الأعضاء في الأمم المتحدة التي لا تزال تشكل جزءاً من رابطة الكومنولث، فضلاً عن تاريخها كديمقراطية من الديمقراطيات العريقة التي أسست هيئات إقليمية رائدة لحقوق الإنسان، مثل مجلس أوروبا، فإن المقرر الخاص يشجع حكومة المملكة المتحدة على اغتنام هذه الفرصة الذهبية للاضطلاع بدور القدوة والتراجع عن التدابير غير المتناسبة التي قد تكون لها تداعيات سلبية تتجاوز بكثير شواطئ المملكة المتحدة. ويدعو المقرر الخاص الحكومة، تحديداً، إلى إبداء التزام أقوى بحماية الحق الأساسي في الخصوصية لمواطنيها ومواطني البلدان الأخرى، وللكف عن تقديم نموذج سيء للدول الأخرى بمواصلتها اقتراح تدابير، تحديداً من قبيل المراقبة

(ي) A/69/397.

بالجملة والاختراق بالجملة، تنافي ظاهراً معايير العديد من اللجان البرلمانية للملكة المتحدة وتتعارض مع آخر الأحكام الصادرة عن محكمة العدل والمحكمة الأوروبية لحقوق الإنسان، وتقوض الحق في الخصوصية قلباً وقالباً. وأخيراً، يدعو المقرر الخاص الحكومة إلى العمل معه عن كثب، لا سيما في سياق دراسته المواضيعية بشأن المراقبة، سعياً لتحديد التدابير المتناسبة التي تعزز الأمن دون أن تفرط في اقتحام الخصوصية.

٦- الخطوات الصغيرة الأولى نحو السلم في الفضاء الإلكتروني؟

٣٩- اتخذت الصين والولايات المتحدة الأمريكية زمام الريادة في البدء بإثارة فتيل النزاع في الفضاء الإلكتروني، وهو أمر جدير بالثناء.

٤٠- وقد تكون هناك ثلاثة أبعاد رئيسية ممكنة للسلم في الفضاء الإلكتروني، جميعها مهددة جراء أعمال التجسس على الإنترنت:

(أ) التخريب والأعمال العدائية؛

(ب) حقوق الملكية الفكرية والتجسس الاقتصادي؛

(ج) الحقوق المدنية والمراقبة.

٤١- وفي حين ترتبط الخصوصية بالبعد الثالث بشكل رئيسي، فإنها كثيراً ما تُطرح أيضاً في النقاشات التي تدور بشأن البعدين الآخرين. ففي أيلول/سبتمبر ٢٠١٥، أُعلن أن الولايات المتحدة والصين "اتفقتا على أن أياً من حكومتيهما لن تدعم أو تمارس سرقة للملكية الفكرية بواسطة الفضاء الإلكتروني" وأن "البلدين ملتزمان كلاهما بالتوصل إلى معايير مناسبة لسلوك الدول في الفضاء الإلكتروني ضمن إطار المجتمع الدولي. واتفق البلدان كذلك على إنشاء فريق خبراء أعلى للمضي في مناقشة الشؤون ذات الصلة"[ك]. ولم تكتف الولايات المتحدة والصين بإتباع هذه الخطوة الهامة بمحادثات بشأن الفضاء الإلكتروني في كانون الأول/ديسمبر ٢٠١٥، وإنما بدا أنهما يضربان للبلدان الأخرى مثالاً يُحتذى في هذا المجال، حيث "تلا إعلانَ الولايات المتحدة إعلان مماثل بين المملكة المتحدة والصين، ونبأ عن اعتزام برلين توقيع صفقة "امتناع عن السرقة الإلكترونية" مع بيجين في عام ٢٠١٦. وفي تشرين الثاني/نوفمبر ٢٠١٥، اتفقت الصين والبرازيل وروسيا والولايات المتحدة وأعضاء آخرين من مجموعة العشرين، على القاعدة التي تقضي بعدم ممارسة أو دعم سرقة الملكية الفكرية بواسطة الفضاء الإلكتروني"[ل]. وقد لا تشبه هذه الخطوات إنجاز اتفاقات كاملة بشأن حرب الفضاء الإلكتروني أو المراقبة على الإنترنت وتأثير التجسس على خصوصية المواطنين، لكنها تشكل بداية على الأقل ولا يسع المقرر الخاص إلا أن يسعى لإقناع جميع الأطراف المعنية بضرورة توسيع المناقشات لتتضمن تدابير ملموسة لاحترام الخصوصية على شبكة الإنترنت أيضاً.

(ك) انظر الرابط: www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

(ل) انظر الرابط: http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement.

رابعاً- الأنشطة الرئيسية للمقرر الخاص

ألف- توفير الموارد اللازمة لأداء ولاية المقرر الخاص

٤٢- بما أن ولاية المقرر الخاص هي ولاية جديدة لم تُقرّ لها ميزانية رسمية حتى كانون الثاني/يناير ٢٠١٦، وبما أنها دخلت حيز التنفيذ في ١ آب/أغسطس ٢٠١٥، أي في موسم العطل في معظم أنحاء أوروبا، فقد استغرق الأمر عدة أسابيع من المقرر الخاص للحصول على أي شكل من أشكال الدعم من مفوضية الأمم المتحدة السامية لحقوق الإنسان. ويُقدم الدعم الإداري حالياً على أساس مؤقت في انتظار تعيين موظفين متفرغين، وهو أمر يتوقع إنجازه في حزيران/يونيه ٢٠١٦. وعندما أجرى المقرر الخاص تقييماً لحالة الموارد المتاحة إليه، فإنه سارع إلى اتخاذ خطوات فورية للحصول على تمويل من خارج الأمم المتحدة. وقد عُيّن باحث في مرحلة الدراسات العليا ما بعد الدكتوراة (حائز على شهادة دكتوراة في الخصوصية وحق النسيان) ابتداء من تشرين الأول/أكتوبر ٢٠١٥ على أساس غير متفرغ، ثم على أساس متفرغ ابتداء من كانون الثاني/يناير ٢٠١٦، لتقديم المساعدة في المسائل المواضيعية. وسيستمر تقديم الدعم الخارجي إلى حين تسوية الوضع المتعلق بالموارد البشرية. وتفضل أخصائيون وموظفون آخرون من المؤسسات التي يعمل معها المقرر الخاص، وتحديداً قسم سياسات المعلومات وإدارتها في كلية الإعلام والعلوم المعرفية بجامعة مالطة، ومجموعة أبحاث الأمن والتكنولوجيا والخصوصية الرقمية في كلية القانون بجامعة غرونينغن بهولندا، بتقديم المساعدة الطوعية إلى المقرر الخاص. وتتيح هذه المساعدة، الجديرة بالتنويه والامتنان شأنها شأن الخدمات التي يقدمها موظفو مكتب الأمم المتحدة في جنيف، أداء مهام المقرر الخاص إلى حين تتسنى زيادة القدرات المتاحة له على النحو المناسب وتهيئة هيكل دائم للدعم يفي بالغرض المنشود منه.

باء- خريطة طريق لولاية المقرر الخاص – بلورة خطة النقاط العشر

٤٣- بالإضافة إلى الأنشطة اليومية المبينة في الفرع ثانياً، استثمر المقرر الخاص الكثير من وقته في بلورة خطة النقاط الشعر المعروضة في الفرع "خامساً" أدناه وفي المشاورات مع العديد من أصحاب المصلحة.

جيم- المشاركة في مناسبات متعددة

٤٤- قبل المقرر الخاص دعوات للمشاركة في اجتماعات ومؤتمرات ومناقشات خبراء ومشاورات فردية، لا سيما تلك التي تساعد في إدامة سياسة العمل المشترك بشأن الدراسات المواضيعية السبع المبينة أعلاه. وفيما يلي قائمة غير حصرية بالأحداث التي شارك فيها المقرر الخاص:

(أ) مناقشة الخبراء بشأن "الارتباط الوثيق بين حرية التعبير والخصوصية في إدارة الإنترنت"، الجمعية العامة الأولى لمشروع "MAPPING"، هانوفر، ألمانيا، ٢٢ أيلول/سبتمبر ٢٠١٥؛

(ب) اللقاء بمدير الشؤون العالمية لمنظمة هيومن رايتس ووتش، ٣٠ أيلول/سبتمبر ٢٠١٥؛

(ج) المشاركة في الحلقة الدراسية بشأن حماية البيانات والخصوصية في الإحصاءات، المعقودة يومي ١٣ و١٤ تشرين الأول/أكتوبر ٢٠١٥ في جنيف، وإلقاء عرض فيها؛

(د) عقد اجتماع مع نائب أمين عام الاتحاد الدولي للاتصالات، جنيف، ١٤ تشرين الأول/أكتوبر ٢٠١٥؛

(هـ) تنظيم ورئاسة مناقشة خبراء بشأن الخصوصية والمراقبة في المؤتمر المتعلق بالاستخبارات في مجتمع المعرفة لعام ٢٠١٥، بوخارست، ١٦ تشرين الأول/أكتوبر ٢٠١٥؛

(و) إلقاء خطاب رئيسي بشأن الخصوصية في العصر الرقمي في المؤتمر الدولي لمفوضي الخصوصية وحماية البيانات، جلسة مغلقة، أمستردام، ٢٧ تشرين الأول/أكتوبر ٢٠١٥؛

(ز) المشاركة في مناقشة المائدة المستديرة "جولة حول العالم" في المؤتمر الدولي لمفوضي الخصوصية وحماية البيانات، أمستردام، ٢٩ تشرين الأول/أكتوبر ٢٠١٥؛

(ح) المشاركة في جلسات متعددة، عامة وثنائية، في منتدى إدارة الإنترنت، جواو بيسوا، البرازيل، ٩-١٣ تشرين الثاني/نوفمبر ٢٠١٥[م]؛

(ط) إلقاء خطاب رئيسي أثناء اجتماع مغلق في حلقة العمل الدولية للبيانات الضخمة في بلدان الجنوب، ريو دي جانيرو، البرازيل، ١٦-١٧ تشرين الثاني/نوفمبر ٢٠١٥[ن]؛

(ي) عقد اجتماعات مع مسؤولي وزارة العدل في البرازيل أثناء تحليل معمق لمشروع قانون برازيلي جديد بشأن الخصوصية، برازيليا، ١٨ تشرين الثاني/نوفمبر ٢٠١٥؛

(ك) عقد اجتماع مشترك مع مسؤولي وزارات الاتصالات والعدل والداخلية في البرازيل، بخصوص مشروع القانون البرازيلي الجديد بشأن الخصوصية، برازيليا، ١٨ تشرين الثاني/نوفمبر ٢٠١٥؛

(ل) عقد اجتماع مع مكتب المدعي العام في برازيليا، ١٨ تشرين الثاني/نوفمبر ٢٠١٥؛

(م) عقد اجتماع مع مدير حقوق الإنسان بوزارة الشؤون الخارجية في البرازيل، برازيليا، ١٩ تشرين الثاني/نوفمبر ٢٠١٥؛

(م) انظر الرابط: www.intgovforum.org/cms/igf-2015-schedule.

(ن) انظر الرابط: http://itsrio.org/en/2015/11/05/encontro-fechado-workshop-internacional-big-data-no-sul-global.

(ن) إلقاء خطاب (عن طريقة وصلة فيديو) في المؤتمر العالمي للمنظمة الدولية للمستهلكين، برازيليا، ١٩ تشرين الثاني/نوفمبر ٢٠١٥[س]؛

(س) عقد اجتماعات ومشاورات معمقة مع مؤسس ومدير رابطة حقوق الخصوصية للمرضى، مالطة، ٢٥ تشرين الثاني/نوفمبر ٢٠١٥؛

(ع) إلقاء خطاب أثناء الجلسة التمهيدية للمؤتمر الرفيع المستوى بشأن حماية الخصوصية على شبكة الإنترنت عن طريق تعزيز أمن تكنولوجيا المعلومات واستقلال تكنولوجيا المعلومات في الاتحاد الأوروبي، الذي نظمته اللجنة المعنية بالحريات المدنية والعدالة والشؤون الداخلية بالمشاركة مع فريق تقييم الخيارات العلمية والتكنولوجية للبرلمان الأوروبي، بروكسل، ٨ كانون الأول/ديسمبر ٢٠١٥[ع]؛

(ف) إلقاء كلمة رئيسية في مؤتمر بشأن الأمن والخصوصية في سياق النسخة الثانية من إطار الملاذ الآمن، روما، ٩ كانون الأول/ديسمبر ٢٠١٥[ف]؛

(ص) إلقاء كلمة رئيسية عن الخصوصية والهوية والأمن والحرية في المؤتمر السنوي لمنظمة الخصوصية والهوية، أوتريخت، هولندا، ١١ كانون الأول/ديسمبر ٢٠١٥[ص]؛

(ق) المشاركة في جلسة إرشادية للمقررين الخاصين، جنيف، ١٤-١٦ كانون الأول/ديسمبر ٢٠١٥؛

(ر) اللقاء بوفد للمملكة المتحدة، جنيف، ١٧ كانون الأول/ديسمبر ٢٠١٥؛

(ش) اللقاء بوفد للصين، جنيف، ١٧ كانون الأول/ديسمبر ٢٠١٥؛

(ت) اللقاء بوفد للاتحاد الروسي، ١٧ كانون الأول/ديسمبر ٢٠١٥؛

(ث) المشاركة بواسطة وصلة فيديو في الاجتماع الخاص للجنة مكافحة الإرهاب بشأن منع الإرهابيين من استغلال الإنترنت ووسائط الإعلام الاجتماعي لتجنيد الإرهابيين والتحريض على تنفيذ أعمال إرهابية، مع الحرص في الآن ذاته على احترام حقوق الإنسان والحريات الأساسية، نيويورك، ١٧ كانون الأول/ديسمبر ٢٠١٥؛

(خ) تقديم عرض في اجتماع حلقة مستديرة للمنظمات غير الحكومية، ضمّ ممثلين للمنظمة الدولية لحماية الخصوصية ومنظمة العفو الدولية ومنظمة مراسلين بلا حدود ومجتمع الإنترنت وهيومن رايتس ووتش والاتحاد الأمريكي للحريات المدنية، وإدارة مناقشات الاجتماع، جنيف، ١٨ كانون الأول/ديسمبر ٢٠١٥؛

(س) انظر الرابط: http://congressprogramme.consumersinternational.org/speakers.html.

(ع) انظر الرابط: www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/privacy.

(ف) انظر الرابط: www.dimt.it/tag/cannataci.

(ص) انظر الرابط: www.pilab.nl/index.php/2015/12/14/the-privacy-identity-lab-four-years-later-published.

(ذ) اللقاء مع نائب مدير مكتب توحيد معايير الاتصالات لدى الاتحاد الدولي للاتصالات (ومعه ممثل الوحدة القانونية للاتحاد)، جنيف، ١٨ كانون الأول/ديسمبر ٢٠١٥؛

(ض) تقديم مداخلات وعرض، عن طريق وصلة فيديو، عن الخصوصية ونوعية الحياة والمدن الذكية: توسيع نطاق "المراقبة"، في مؤتمر الاتحاد الدولي للاتصالات عن المدن الذكية، سنغافورة، ١٨ كانون الثاني/يناير ٢٠١٦؛

(ظ) عقد اجتماعات مع هيلين والاس وأندرو جاكسون من منظمة " GeneWatch UK"، مالطة، ٣ شباط/فبراير ٢٠١٦؛

(غ) إلقاء خطاب رئيسي (عن طريق وصلة فيديو) في حلقة العمل الخامسة بشأن حماية البيانات في المنظمات الدولية، جنيف، ٥ شباط/فبراير ٢٠١٦[ق]؛

(أأ) إلقاء خطاب رئيسي والمشاركة في اجتماع عام لأصحاب المصلحة في وزارة الشؤون الخارجية الهولندية، لاهاي، هولندا، ٣ آذار/مارس ٢٠١٦.

خامساً- خطة عمل النقاط العشر

٤٥- توخياً للمضي في بلورة أبعاد الحق في الخصوصية وعلاقته بحقوق الإنسان الأخرى، أعدّ المقرر الخاص خطة عمل من عشر نقاط. وينبغي التشديد على أن النقاط المدرجة في الخطة ليست مرتبة وفق ترتيب معين ولا توحي بأولوية معينة لعناصر برنامج العمل. ويرى المقرر الخاص دوره بمثابة رائد، أي أنه يسعى لشق الطريق إلى الأمام بينما يعمل في الآن ذاته على تحديد المسائل الملحّة التي يتعين التصدي لها والتفاعل مع احتياجات الأفراد أو البلدان التي تقتضي إجراءات مسؤولة عاجلة. وتشكل خطة عمل النقاط العشر أدناه قائمة مهام لا قائمة أمنيات. وقد باشر المقرر الخاص بالفعل بالعمل على كل نقطة منها، غير أن إحراز التقدم مرهون بوفرة الوقت والموارد.

١- معنى "الحق في الخصوصية"

٤٦- لا بد لتجاوز الإطار القانوني القائم وتحقيق فهم أعمق لما تعهدت الأطراف بحمايته، من العمل على بلورة فهم أفضل وأكثر تفصيلاً وعالميةً لما يعنيه "الحق في الخصوصية". ما الذي يعنيه وما الذي ينبغي أن يعنيه في القرن الحادي والعشرين؟ وكيف يمكن تحسين حمايته في العصر الرقمي؟ وستُنفذ في هذا الصدد أنشطة وتُدعم أبحاث من أجل استطلاع الأجوبة الممكنة لهذه الأسئلة الجوهرية، وهو ما سيساعد في إرساء الأسس الضرورية لتناول العناصر الأخرى من خطة عمل المقرر الخاص.

(ق) انظر الرابط: www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations.

٢- إذكاء الوعي

٤٧- تتمثل مسألة أخرى هامة في إذكاء وعي المواطنين من أجل مساعدتهم على فهم معنى الخصوصية. فمن المهم إجراء حوار عام عما ينطوي عليه حق المواطنين في الخصوصية وكيف قد يتعرض هذا الحق للانتهاك، لا سيما في ظل التكنولوجيات الجديدة وسلوكهم في الفضاء الإلكتروني. وهم بحاجة إلى معرفة كيف يجري تداول بياناتهم الشخصية كسلعة وما هي الضمانات القائمة وسبل الانتصاف المتاحة لحماية حقهم في الخصوصية. وما الذي ينبغي القيام به للحد من خطر انتهاك حقهم في الخصوصية، وكيف يمكنهم التفاعل مع المشرعين وقطاع الشركات من أجل النهوض بحماية خصوصيتهم؟ فإذكاء الوعي مهمة جسيمة، ويعتزم المقرر الخاص أن يساهم في أداء هذه المهمة من خلال ولايته، بالعمل الدائب مع جميع أصحاب المصلحة، لا سيما المجتمع المدني.

٣- تهيئة حوار منهجي متواصل عن الخصوصية

٤٨- لا بد من خوض حوار أكثر منهجيةً وانفتاحاً وشمولاً وفعالية، والأهم من ذلك كله أن يكون حواراً دائماً بين مختلف أصحاب المصلحة. فحماية الخصوصية تقتضي بناء الجسور. ويعتزم المقرر الخاص التركيز بشدة على هذا النشاط مستفيداً من المحافل القائمة، فضلاً عن إنشاء محافل جديدة لهذا الغرض. ومما يتسم بأهمية بالغة في هذا الصدد تيسير الحوار المنهجي بين المنظمات غير الحكومية ومفوضي الخصوصية وحماية البيانات ووكالات إنفاذ القانون وأجهزة الأمن والمخابرات. ومن الضروري العمل مع جميع فئات أصحاب المصلحة من أجل تحسين الإجراءات الداخلية وتعزيز الخصوصية عن طريق تبني تدابير لحمايتها في تصميم التكنولوجيات التي تُنشر والإجراءات التي تُتبع. ومن الأهمية كذلك تعزيز الشفافية والمساءلة إلى أقصى حد ممكن وتدعيم الرقابة النزيهة والفعالة لتبلغ مستوى رفيعاً من الفعالية والمصداقية.

٤- نهج شامل للضمانات وسبل الانتصاف القانونية والإجرائية والعملية

٤٩- لطالما كانت الضمانات المناسبة وسبل الانتصاف الفعالة جزءاً من علة وجود قوانين حماية البيانات منذ وضعها. وتهدف هذه القوانين إلى توفير المشورة والحماية على المستوى المناسب في عالم ما فتئ يزداد تعقيداً في ظل التغيرات التكنولوجية المطردة. وينبغي توفير حماية أكثر وضوحاً وفعالية للمواطنين من أجل منع انتهاكات الحق في الخصوصية. ويتعين كذلك إتاحة سبل انتصاف حقيقية لجميع المعنيين في حالات حدوث مثل هذه الانتهاكات بالفعل. والسعي إلى توفير الضمانات وسبل الانتصاف هو سعي شامل يصب في جميع الدراسات المواضيعية للمقرر الخاص المبينة في الفرع ثانياً أعلاه.

٥- تجديد التركيز على الضمانات التقنية

٥٠- لا يمكن أن تقتصر الضمانات وسبل الانتصاف المتاحة للمواطنين على بُعد قانوني أو تنفيذي صرف. فالقانون وحده لا يكفي. وسيواصل المقرر الخاص العمل مع المجتمع التقني سعياً لتعزيز وضع ضمانات تقنية فعالة، بما في ذلك التشفير وبرمجيات التمويه وشتى الحلول التقنية الأخرى التي تحمي الخصوصية عملياً بحكم تصميمها.

٦- إجراء حوار شديد التركيز مع عالم الشركات

٥١- هناك عدد متزايد اليوم من الشركات التي تجمع كماً من البيانات الشخصية يفوق ما تستطيع الحكومات أو تريد جمعه. والسؤال المطروح هنا هو: ما هي البدائل المقبولة أو التغييرات الرئيسية التي ينبغي أن يتوقعها المجتمع من نماذج الأعمال التجارية الراهنة التي تحول البيانات الشخصية إلى سلعة نقدية؟ وما هي الضمانات المنطبقة في الحالات التي تطلب منها سلطات دولة ما الحصول على البيانات التي تحتفظ بها شركات خاصة؟ يقتضي هذا البعد من الولاية الكثير من الوقت والاهتمام. وقد بدأ المقرر الخاص بالفعل اتصالات مباشرة مع ممثلين لعالم الشركات وسيسعى لإدامة حوار يركز على الخصوصية بشأن هذه المسائل مع طائفة من الجهات الفاعلة في هذا القطاع، بنية الاطلاع على المستجدات في قطاع الشركات واطلاعها كذلك على المعلومات المتعلقة بالجوانب الأخرى لولايته.

٧- تعزيز التطورات الوطنية والإقليمية في آليات حماية الخصوصية

٥٢- ينبغي أن تكون التطورات الوطنية والإقليمية في آليات حماية الخصوصية موضع تقدير على الصعيد العالمي. وللمقرر الخاص دور تكميلي هام عندما يعمل في إطار من التعاون الوثيق مع مفوضي الخصوصية وحماية البيانات من مختلف أنحاء العالم. فمن خلال التعاون والحوار، يمكن النهوض بمعايير حماية الخصوصية إلى حد كبير. وقد باشر المقرر الخاص سلسلة من الأنشطة العالمية التي خططها ونفذها بالتعاون مع سلطات حماية البيانات. وتتضمن هذه الأنشطة أحداث من المقرر تنظيمها في أستراليا والمغرب ونيوزيلندا وتونس وآيرلندا الشمالية في عام ٢٠١٦، بالإضافة إلى أنشطة أخرى كثيرة يجري العمل على تنفيذها في الأعوام القادمة.

٨- تسخير طاقة المجتمع المدني ونفوذه

٥٣- بعد أن التقى المقرر الخاص بممثلي ٤٠ منظمة غير حكومية أثناء الأشهر الستة الأولى من ولايته، فإنه يعتزم مواصلة تكريس الوقت للاستماع إلى ممثلي المجتمع المدني الذين يبذلون جهوداً كبيرة للنهوض بحماية الخصوصية في جميع أنحاء العالم، وللعمل معهم في سبيل تحقيق هذه الغاية.

٩- الفضاء الإلكتروني، والخصوصية والتجسس والحرب والسلم في هذا الفضاء

٥٤- ينبغي أن يتخذ المجتمع العالمي موقفاً متحرياً وصريحاً ومفتوحاً تجاه ما يجري حقيقةً في الفضاء الإلكتروني، بما في ذلك حقائق المراقبة الجماعية والتجسس والحرب في هذا الفضاء. وسيجري تناول هذه الحقائق انطلاقاً من نتائج نقاط العمل الأخرى المذكورة أعلاه، فضلاً عن نتائج الدراسات المواضيعية المحددة في الفرع ثانياً أعلاه. ويتوقع المقرر الخاص أن تظل هذه المسائل سمة ثابتة في عدد من تقاريره وفي العديد من زياراته القطرية. وهو يأمل، من خلال الحوار الشفاف مع أصحاب المصلحة بشأن هذه المسائل، في القيام بدور بناء في تحسين حماية الخصوصية في العصر الرقمي.

١٠- مواصلة الاستثمار في القانون الدولي

٥٥- مع أن القانون وحده لا يكفي، فإن ذلك لا ينفي ما له من أهمية بالغة. وينبغي لذلك استكشاف إمكانية تطوير القانون الدولي المتعلق بالخصوصية، بجميع أشكالها. والمقرر الخاص مستعد لتقييم أي صك قانوني بصرف النظر عما إذا كان يعتبر من القوانين اللينة أو المتشددة. ويبدو في هذا الصدد أن نقطة انطلاق جيدة قد تتمثل في التصدي لمسألة ذات أولوية، مثل تحديث الصكوك القانونية القائمة عن طريق إدراج فهم أوسع لما يعنيه الحق في الخصوصية. ويبدو أن ثمة توافقاً بين العديد من أصحاب المصلحة على أن أحد هذه الصكوك القانونية يمكن أن يتخذ شكل بروتوكول إضافي للمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية[ر]، التي شُجع المقرر الخاص بشأنها على "تعزيز البدء في مفاوضات بشأن وضع بروتوكول من هذا النوع خلال فترة ولايته الأولى"[ش]. غير أن التوقيت المحدد لهذه المسألة قد يرتهن بالمدة التي ستستغرقها المناقشات المعمقة والموسعة المقرر إجراؤها في إطار النقطة ١ أعلاه وما ستفضي إليه من نتائج، وهي النقطة التي تتعلق بتحقيق فهم عالمي أفضل لما تنطوي عليه الخصوصية، أو ما قد تنطوي عليه، من قيم جوهرية. وهناك مسائل أخرى تتعلق بالخصوصية، تشمل على وجه الخصوص المسائل المتعلقة بالاختصاص القضائي أو مبدأ الإقليمية في الفضاء الإلكتروني، لا يمكن التصدي لها بصورة مرضية ما لم يكن هناك اتفاق دولي واضح بهذا الشأن، وهو ما يتخذ عادةً شكل معاهدة متعددة الأطراف بشأن موضوع محدد أو مجموعة من المسائل على الأرجح. ولتفادي أي لبس في هذا الصدد، ينبغي إيضاح أن ما نصبو إلى تحقيقه ليس اتفاقية دولية عالمية وشاملة جديدة، تغطي جميع المسائل المتعلقة بالخصوصية أو إدارة الإنترنت. إذ من العقلانية أكثر توقع إمكانية تعزيز حماية الخصوصية من خلال نمو تصاعدي للقانون الدولي، وبالتالي من خلال توضيح الصكوك القانونية القائمة، ومن ثم توسيع نطاقها. وقد يتضمن ذلك، في الأمدين المتوسط والبعيد، وضع صكوك قانونية جديدة تماماً. وسيعمل المقرر الخاص أيضاً على رصد المناقشات الجارية بشأن القانون الدولي والصكوك القانونية الجديدة في مجال إدارة الإنترنت، من أجل تحديد الوقت المناسب لاتخاذ إجراءات في هيئات الأمم المتحدة، فضلاً عن نوع ونطاق الصك القانوني الذي قد يودّ المقرر الخاص أن يوصي به مجلس حقوق الإنسان والجمعية العامة لاحقاً.

سادساً- الاستنتاجات

٥٦- تأثر المقرر الخاص بالترحيب الحماسي الحار الذي تلقاه من معظم شرائح المجتمع ومعظم فئات أصحاب المصلحة.

(ر) انظر الرابط: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

(ش) الرابط نفسه.

٥٧- ولم يسبق للخصوصية أن حظيت بمثل الاهتمام الذي حظيت به في عام ٢٠١٦، سواء على الصعيد السياسي أو القضائي أو على مستوى الوعي الشخصي.

٥٨- وفي حين لا تزال العلاقة متوترة بين الأمن ونماذج الأعمال التجارية للشركات والخصوصية، فإن الأشهر الإثني عشر الماضية اتسمت بمؤشرات متضاربة، حيث واصلت بعض الحكومات، على صعيد الممارسة و/أو في البرلمانات، اتخاذ مواقف مناوئة للخصوصية، فيما وجهت المحاكم في مختلف أنحاء العالم، ولا سيما في الولايات المتحدة وأوروبا، رسائل واضحة تساند الحق في الخصوصية، وتقف تحديداً ضد عدم التناسب والتدابير التي تقتحم الخصوصية، كالمراقبة الجماعية واختراق البيانات المشفرة.

٥٩- وهناك مؤشرات قوية على أن الخصوصية أصبحت اعتباراً تجارياً هاماً لدى بعض الشركات الكبرى التي اعتمدتها منتجاً صالحاً للبيع. فعندما تكون هناك سوق للخصوصية، فإن قوى السوق ستتسابق لتوفيرها. وتعدّ الزيادة المطردة في الأجهزة المشفرة والخدمات البرمجية مؤشراً قوياً على أن المستهلكين في مختلف أنحاء العالم باتوا أكثر وعياً بالمخاطر التي تحف بخصوصيتهم، وسيبدون ميلاً أكبر لاختيار المنتجات والخدمات التي تحمي خصوصيتهم على تلك التي لا تهتم بهذا الجانب أو تفرّط فيه.

٦٠- وفي حين تواصل بعض الحكومات مساعيها التي تفتقر إلى الرشد أو حسن المشورة أو سداد الحكم أو حسن التوقيت، بل تفتقر أحياناً إلى التهذيب، لشرعنة تدابير غير متناسبة ولا مبررة لاقتحام الخصوصية، مثل جمع البيانات بالجملة أو اختراق الحسابات بالجملة واعتراض الاتصالات دون مسوغ، فإن ثمة حكومات أخرى، تتصدرها في هذه الحالة هولندا والولايات المتحدة، قد اتخذت خطوات أكثر انفتاحاً نحو انتهاج سياسة رفض الأبواب الخلفية في تكنولوجيا التشفير. ويودّ المقرر الخاص أن يشجع المزيد من الحكومات على التوحد حول هذا الموقف.

٦١- ولم تتيقظ البلدان في مختلف أنحاء العالم لمسؤولياتها ولمعطيات الضمانات التقنية، كالتشفير، فحسب، وإنما بدأت تدرك أيضاً، ببطء ولكن بثقة، محدودية المكاسب وجسامة المخاطر التي قد تنجم عن تدمير الفضاء الإلكتروني جراء انتشار الأعمال الحربية والتجسسية فيه. ولا يزال يُنتظر إحراز التقدم في هذا المجال، مع أن عام ٢٠١٥ شهد بعض البدايات الهامة على هذا الصعيد. ولذلك يشجع المقرر الخاص الحكومات – وليس فقط حكومات مجموعة العشرين – على التحلق حول مائدة الحوار لمناقشة السلوك المناسب للدول والتدابير ذات الصلة بإدارة الفضاء الإلكتروني، على نحو يتناول الحقوق المدنية، ولا سيما الخصوصية وحرية التعبير والمراقبة.

٦٢- وينبغي أن تكون أساليب عمل المقرر الخاص وخطة النقاط العشر مؤشراً على نهج شمولي إزاء موضوع حماية الخصوصية وتعزيزها في العصر الرقمي. ويساعد النهج الشمولي على تحديد ملامح الصورة الإجمالية لما يُراد تحقيقه، وإن كان توقيت ما يتعين تحقيقه

بدقة وعلى يد من مرهوناً بعاملين رئيسيين هما: أولاً، الموارد المتاحة لتنفيذ خطة العمل وإنجاز الدراسات المواضيعية، وثانياً، مدى استعداد أصحاب المصلحة المتعددين لقبول برنامج عمل يؤيد الخصوصية، بدلاً من التمسك بعقلية "القيادة والسيطرة". ويوجه المقرر الخاص رسالة واضحة وبسيطة لمن يرون للوهلة الأولى أن خطة عمله ليست طموحة فقط بل مغالية في الطموح، ومفادها: إذا كنتم تتفقون مع أهداف الخطة وإدماجها عدداً من المسائل المعقدة ولكن المترابطة، فما عليكم سوى التقدم والمساهمة بموارد إضافية لتنفيذها. فهو ما سيساعد في جعلها قابلة للتنفيذ. ويستند المقرر الخاص إلى تجربته كمدير مشاريع له سجل ناجح في تعبئة عشرات الملايين من الدولارات لصالح الأبحاث المتعلقة بالخصوصية، للعمل على وضع استراتيجية لزيادة الموارد المتاحة لصاحب الولاية، ونجاح خطة النقاط العشر مرهون فعلاً بنجاح تلك الاستراتيجية. وحتى لو حققت الاستراتيجية نجاحاً باهراً، فإن المقرر الخاص يتوقع أن تنتقل مسؤولية استمرارية عناصر خطة النقاط العشر و"إمكانية" إنجازها إلى صاحب الولاية المقبل. أما التحدي الخاص بهذه المرحلة فيتمثل في توفير رؤية واضحة وشاملة وأسس راسخة من شأنها أن ترسي قاعدة لتقرير سياسات متينة قائمة على الأدلة في ميدان حماية الخصوصية.

Annex I

Challenges faced by the Special Rapporteur and his vision for the mandate

1. The Special Rapporteur immediately set about building up his team composed of persons working for the mandate on a part-time or full-time basis. One of these persons is currently a full-time United Nations (UN) Human rights officer, hired on a temporary contract, while the position is under recruitment. The work of this person is supervised by a more senior UN employee who is also responsible for supporting the work of six other mandate holders. A second part time professional and a part time administrative officer will soon be recruited, as well as a part-time consultant. The SRP is grateful that the Human Rights Council endowed his mandate with this still limited (given the scope of his mandate) but unprecedented level of support to a mandate holder. The other persons in the SRP team are not employed by the UN but are resourced by extra-mural funding obtained by the SRP or may be volunteers. The team is often physically spread across at least three geographical locations (currently Malta, the Netherlands and Switzerland) and, as befits the digital age, most of the team meetings are carried out in cyber-space with the working day being opened by an on-line conference call involving all team-members who may be available. During the "morning meeting" team members typically report on work carried out in the previous day, consult about tasks planned for the rest of the working day and plan tasks and events for the following weeks and months. When doing so, their tasks reflect the fact that the work of the SRP may be broadly divided into four categories and any team member may be working concurrently on tasks from each of these categories.

2. The fact that the mandate on privacy is a new one presents both advantages and disadvantages. Amongst other things it means that the Special Rapporteur on Privacy (SRP) had no roadmap to follow and indeed one of his first priorities in this case is to work on designing and developing such a roadmap. This means that some of the issues identified in this and later reports are not necessarily capable of being resolved within the time-constraints imposed by one or even two three-year mandates. They are mentioned however in order to provide a more holistic picture of what needs to be done in the short, mid and long-term. In doing so, this incumbent is conscious of possibly identifying issues which may possibly be more appropriately tackled in a more timely manner by later holders of the mandate.

3. One of the recurring themes of this and later reports will undoubtedly be the time dimension. The rapid pace of technology and its effects on privacy means that action on some already-identified issues may increase or decrease in priority as time goes by while new issues may emerge fairly suddenly. It may also mean that sometimes it may be more opportune to launch or intensify action on a particular issue not necessarily because it is much more important than other issues but rather because the timing is right, because the different international audiences and classes of stakeholders may be far more sensitive and receptive to that particular issue for reasons and circumstances over which the Special Rapporteur may have absolutely no control but in which case it would be foolish not to take advantage of favourable opportunities which may result in the creation or improvement of privacy safeguards and remedies.

4. The later prioritisation of action will also depend on the extent of the resources made available to the Special Rapporteur and the extent to which he can succeed in attracting fresh resources to support the mandate on privacy. This resource issue is fundamentally important and will directly affect the extent of the impact the mandate on Privacy may have

in practice in real life. It is clear that, however good in quality in some respects, the quantity of resources provided to the mandate by the UN is woefully inadequate and even if the mandate's human and financial resources are increased tenfold, it would still be hard-pressed to achieve the minimum required to persuade the incumbent that the work of the mandate is really making a difference to the protection of privacy of ordinary citizens around the world. The experience of the first six months in office has persuaded the mandate-holder that not only must the SRP be omni-present 24/7 on the many privacy-related issues which arise literally every day in many countries around the world but that he must also act as rainmaker, somehow attracting funds and human resources in order to make the work of the mandate both possible and sustainable in the short, mid and long-term. The effort required by what is, in essence, a part-time, un-paid position which must, by definition, co-exist with a demanding day-job, should not be under-estimated. This effort can be encouraged by the positive response of all stakeholders not least that of the nation-states, members of the UN to whom this report is addressed. If these stakeholders do not support the mandate adequately, if they do not put their money where their mouth is, then this will only serve to increase the frustrations already inherent to any work being carried out within the UN's systems and bureaucracy.

5. The incumbent's vision of the mandate is therefore analogous to the process required to design, finance, project manage and complete the building of a house or other building suitable for human beings to live and/or work in safely. Firstly we need to understand the function of the building: is it a residence for an individual living alone or for one nuclear family, or for a large and extended family or indeed for several of such individuals and families? Should it include a working space and if so for what type of work: is this to be a farm-house, a baker's *casa bottega* or a black-smith's lodge or an urban block of multi-rise apartments? Form follows function so the function or functions must be clearly identified and understood in-depth. Secondly, form follows function so the design of the house — or the mandate's range of activities — must be completed on the basis of the function. Thirdly, the size of the building and its interior may be basic, cramped, spartan i.e. just barely enough to provide basic shelter and sanitation or else it may be more comfortable and spacious and functional or else it may be downright luxurious. Whether it is one or the other will depend on the resources and especially the finances which can be projected to be available to the builder — and these will influence the final design of the plan for the building — and the mandate. Fourthly, the time available to complete essential parts of the building will also influence the design of the plan. Fifth, it will need to be borne in mind that life gets in the way of the best-laid plans and the design may, from time to time, have to be more of an emergent design process rather than the fulfilment of a rigid, prescriptive pre-ordinate design. This analogy is useful to explaining the scope of this report especially to emphasize that while the building itself may not necessarily be capable of completion within the time-frame of one or even two three-year mandates, it is very important to decide on what the final building needs to be like, otherwise we would be unable to design the type of the foundations we require to build...and unless the foundations are sound and fit-for-purpose the building will ultimately prove to be unsustainable and collapse.

Annex II

A more in-depth look at open data and big data

1. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality.

2. At first sight Open Data sounds fine as a concept, a noble and altruistic approach to dealing with data as a common good, if not quite "common heritage of mankind". Who could object to data sets being used and re-used in order to benefit various parts of society and eventually hopefully all of humanity? It is what you can do with Open Data that is of concern, especially when you deploy the power of Big Data analytical methods on the data sets which may have been made publicly available thanks to Open Data policies. Of course, it is important to differentiate between data sets of one type and another. If what is put into the public domain consists of, say, the raw data arising out of tens of thousands of questionnaire responses about perceptions of privacy which responses would have been gleaned from across 27 EU member states and processed in an anonymised manner, the risk to individual privacy from aggregated data sets would appear to be very low if not non-existent. If, on the other hand, one uses Big Data analytical methods to develop links between supposedly anonymized medical data and publicly available electoral registers in a way that links identified or identifiable individuals to sensitive patient information then society has genuine cause for concern. Pioneers like Latanya Sweeney in the USA have demonstrated these abilities and exposed these risks on numerous occasions over the past two decades but the question remains: how should society intervene? More precisely how should policy-makers act in the face of such risks? Which is the correct information policy to develop and adopt? Especially since society has already intervened in a number of ways. Open Data is an information policy born out of specific information politics. For example, the EU legislated in favour of re-utilising public data more than 12 years ago (Directive 2003/98/EC), indeed five years after Prof Sweeney's first eye-opening discoveries.[a] Is this one of many cases where Open Data Policies were embraced before unintended consequences were properly understood and may now need to be remedied?

3. It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide. For the best part of forty years, our entire *forma mentis* has been founded upon something we call the purpose-specification principle. Put simply, personal data should be collected, used, stored and re-used for a specified legitimate purpose or for a compatible purpose.

[a] "In 2000, Sweeney analyzed data from the 1990 census and revealed that, surprisingly, 87 percent of the U.S. population could be identified by just a ZIP code, date of birth, and gender" according to Caroline Perry, SEAS Communications "You're not so anonymous" October 18, 2011 last accessed on 13 Jan 2016 at http://news.harvard.edu/gazette/story/2011/10/you%E2%80%99re-not-so-anonymous/ . However, in testimony to the Privacy and Integrity Advisory Committee of the Department of Homeland Security ("DHS") on 15 June 2005 Sweeney states that it was in 1997 that she "was able to show how the medical record of William Weld, the governor of Massachusetts of the time could be re-identified using only his date of birth, gender and ZIP. In fact, 87% of the population of the United States is uniquely identified by date of birth (e.g., month, day and year), gender, and their 5-digit ZIP codes. The point is that data that may look anonymous is not necessarily anonymous". http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf last accessed on 13 January 2016.

Once the time required for the data to be stored by that specified purpose runs out then the data should be deleted permanently. Re-using personal data is not part of our privacy or data protection DNA.

4. The purpose-specification principle is not something invented by Europeans. One of the first places where it is articulated as such is in a 1973 report by an Advisory Committee to the US Department of Health[b] where it was held that "There must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent". This quickly became a fundamental value in many other fora. The OECD Guidelines of 1980 have the Purpose specification Principle as the third out of eight principles "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose". In this context it is also important to note the OECD's corollary fourth principle usually recognised as the Use Limitation Principle whereby "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 3 above except a) with the consent of the data subject; or b) by the authority of law" These principles are also found in the Council of Europe's influential Data Protection Convention of 1981 and the EU's Data Protection Directive (46/95).

5. In an important regional development, the European Union is now at an advanced stage of devising and implementing the next generation of its data protection laws. When one examines the texts produced by the EU between 2012 and 2015, it is not as if the European Union appears ready to abandon the principle of purpose limitation. In the latest available version[c] of the draft text of the EU's General Data Protection Regulation (GDPR) the importance of the purpose specification principle does not appear to be in any way to be diminished. Article 5 b retains the principle prominently, stipulating that personal data shall be

> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

an approach reinforced by the next principle to be found in the GDPR's Article 5 which lays down that personal data shall be

> (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

[b] DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U S Govt. Printing Office, Washington USA 1973 at p. 41.

[c] s_2014_2019_plmrep_AUTRES_INSTITUTIONS_COMM_COM_2015_12-17_COM_COM(2012)0011_EN.pdf.

6. The meaning of these key principles had been similarly announced in the recitals of the GDPR

> (30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

7. It is clear therefore that the current thinking in Europe on Data Protection still relies on the purpose specification principle taken in tandem with anonymization or deletion despite all the risks inherent in the use of Big Data Analytics and Open Data. Likewise, in the United States where on May 9, 2013, President Obama signed an executive order[d] that made open and machine-readable data the new default for government information",[e] some have attempted to downplay the concerns raised by Latanya Sweeney and have generally held that the risks of de-identification are not as great as previously made out.[f] Yet, a detailed analysis of the output of Prof Sweeney's Data Privacy Lab[g] and some of her more recent research[h] persuade the SRP that we are running the risk of using outmoded safeguards, almost twenty years after our attention was drawn to the fact that stripping personal data of some basic identifiers may not be enough to protect privacy.

8. A careful examination of the pivotal thinking in Europe in 2015-2016 does not provide much reassurance especially if one carefully examines the pertinent part of the latest version[i] available of the draft EU General Data Protection Regulation which holds that

> (23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

---

[d] https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government- last accessed on 13 Jan 2016.

[e] https://www.whitehouse.gov/open last accessed on 13 January 2016.

[f] See for example Barth-Jones, Daniel C. "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now" June 2012 last accessed on 13th January at https://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf.

[g] http://dataprivacylab.org/index.html.

[h] Sweeney L, Matching Known Patients to Health Records in Washington State Data, 2012 last accessed on 13th January 2016 at http://dataprivacylab.org/projects/wa/1089-1.pdf.

[i] http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884 last accessed on 13th January 2016.

9. This latest version from December 2015 after negotiation with the Council is less detailed than the one approved by the Parliament in October 2013 which held that

> (23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.

10. Is the change an improvement, a factor which strengthens privacy protection in the era of Open Data or Big Data or is it a compromise which weakens protection? Whereas, it seems to the SRP that the very standard formulation of October 2013,[j] dependant as it was on the costs and time required to identify an individual, is rapidly becoming archaic in the era of big data analytics, the rather vaguer 2015 version seems to be a bit more elastic, but that could be a double-edged sword. If we are to insist on maintaining information policies built around the principles of Open Data then we need to develop much stronger, complex algorithmic solutions and procedural safeguards. The application of the newest EU proposals pivot almost entirely on what constitutes anonymous data yet Latanya Sweeney[k] and others have clearly demonstrated that there are huge limits to anonymization and it would seem that practically most personal data may actually be identifiable with such minimal effort that they would not meet eligibility criteria to qualify as anonymous data, thus bringing the GDPR into play.

11. Things get even more complicated when taking into consideration the factors legitimising research[l]

> (88) For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

12. While the issue of sensitive data such as health information still presents a quandary within the EU's GDPR

> (42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

---

[j] "inofficial consolidated version" https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf last accessed on 13th January 2016.

[k] http://latanyasweeney.org/publications.html.

[l] Though this recital 88 has been expanded in the latest 17 Dec 2015 version.

13. How do Open Data and Big Data analytical capabilities fit into the scenarios and thinking portrayed above? Which would be the suitable safeguards to apply in Open Data policies which would protect privacy in the era of Big Data? Are the latest legal innovations being contemplated in Europe the right response to the evidence presented by Sweeney and do they represent best practice for the world to follow or dubious practice for the world to shun? The only thing that is certain is that if we are to get things right then it is clear that we need much more in-depth analysis of both the risks of Open Data as well as existing and new safeguards. Moreover, in this field too there appears to be a huge need for increasing public awareness. Relatively few people seem to know about the existence of open data policies or the consequences of applying big data analytics to different data sets put into the public domain by Open Data policies. In the course of participating in debates about Open data and Big data during tenure as SRP, one reinforced the impression that Open Data policies and their privacy and autonomy implications remain very much an area of interest to a tiny group of domain specialists and then again may be restricted further by the language in which they are made available to the public. The SRP is very sensitive to and is working with NGOs interested in protecting personal data in a number of sectors, including medical data and will, during 2016-2017 be engaging in events aimed at promoting discussion and on-going, in-depth investigation of related matters. The SRP is also very concerned that entire nations or trading blocs including major nations or regional federations such as China, the European Union and the United States have adopted or are adopting Open Data and Big Data policies the far-reaching consequences of which may not as yet be properly understood and which may unintentionally put in peril long-standing social values as well as the fundamental rights to privacy, dignity and free development of one's personality. Some studies on posthumous privacy suggest that in 2016 the citizens of some countries may be better off dead from a privacy point of view since their rights to privacy are better protected by law if they are dead than if they are alive in a world where Open data and big data analytics are a way of life endorsed by the information policies of the countries concerned. These developments may well be unintentional but the impact on privacy, autonomy, dignity and free development of personality may be far-reaching.

Annex III

Further reflections on the notion of privacy

A. Core values and cultural differences

1. As a result of the processes described in Section III of the report, an improved, more detailed understanding of privacy should be developed by the international community. This understanding should possibly result in some flexibility when it comes to addressing cultural differences at the outer fringes of the right or in privacy-neighbouring rights while clearly identifying a solid and universally valid core of what privacy means in the digital age.

2. This global concept of privacy has to pass the test of being positively describable and definable as a precious substantive right on the one hand. On the other hand there also needs to be a negative understanding of the right which hints at legitimate limitations should it be legitimate and necessary to restrict privacy in a proportionate manner. The Special Rapporteur invites all actors in the field to contribute to the development of this urgently needed and improved understanding of the right to privacy and is convinced that significant progress is possible.

B. Enforcement

3. Apart from the absence of a clear universal understanding of privacy, the lack of effective enforcement of the right is an issue which is evident at most turns of the debate. Thus, not only is it not entirely clear what needs to be protected but also how to do it. Regretfully though perhaps hitherto inevitably, the super-fast development of privacy-relevant technologies and especially the Internet has led to a huge organic growth in the way in which personal data is generated and the exponential growth in the quantity of such data. This is especially evident in an on-line environment where, when seen from a global perspective, it would appear that the triangle of actors consisting of legislators, private (mostly corporate) actors and citizens all try to shape cyberspace using their possibilities in an uncoordinated manner. This may lead to a situation where none of the three is able to unleash the full potential of modern information technology.

4. In order to disentangle this triangular relationship an ongoing and open dialogue needs to be set up which eventually would provide for a more clear and harmonious regulation of cyberspace. This can only be achieved as a result of a sincere, open and committed dialogue of all parties which is to be held in a respectful and open manner. Sturdy and reliable bridges need to be built between all actors which are shaping the developments. It is the intention of the Special Rapporteur to listen closely to all parties and to facilitate this dialogue. In this way a basis for a positive and sustainable long-term development in the field of privacy protection should be achieved.

Annex IV

A “State of the Union” approach to privacy

It would appear to be useful to, at least once a year, have the SRP present an independent stocktaking report on where the right to privacy stands and this may be one of the primary functions of both the reports to be made to the Human Rights Council (HRC) and the General Assembly (GA). Since these reports are constrained by a word-limit it is clear that they can be little more than an extended executive summary of the findings and activities of the mandate throughout the reporting period. It should follow that the reports will also reflect the working methods of the mandate as outlined in Section II of the main report, in particular the thematic investigations as well as salient developments identified in the country monitoring activities carried out by the SRP team. It is expected that the report presented to the March 2017 session of the Human Rights Council would be the first such report reflecting a “State of the Union” approach. The report to the March 2016 session of the HRC will not attempt to prioritise risks or landmark improvements in privacy protection but simply refer to a few cases which illustrate particular progress or difficulties.