Eventual legalización de la vigilancia en Ecuador e impactos en derechos humanos y modelo de desarrollo

1. Contexto

Las revelaciones sobre la vigilancia masiva y la recolección de datos por parte de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos desataron la indignación de los líderes políticos alrededor del mundo, incluyendo al Gobierno y a la Asamblea Legislativa de Ecuador. Algunos países, como Brasil, han indicado que tomarán medidas y redoblarán sus esfuerzos para adoptarán legislación, desarrollarán tecnologías y establecerán mecanismos para proteger a su población de la vigilancia masiva ilegal y desproporcionada y de la interceptación de las comunicaciones y los datos.

Brasil y otros países han demandado al interior del Consejo de Seguridad y en la Asamblea General de la ONU la necesidad de crear condiciones para prevenir que el ciberespacio se torne en un campo de batalla y en un arma de guerra a través del espionaje, el sabotaje y el ataque a la infraestructura de la red. Se ha llamado la atención sobre los impactos que dichas prácticas tienen sobre los derechos humanos.

Adicionalmente, Brasil y ICANN han anunciado el deseo de organizar una cumbre en los primeros meses del 2014 para discutir la situación de la vigilancia masiva y otros temas de gobernanza de internet. Los delegados del gobierno de Brazil al Foro de Gobernanza de Internet (realizado en Bali del 22 al 25 de octubre de 2013), confirmaron su disposición para organizar una reunión de alto nivel para discutir estos temas y avanzar en la definición de:
- principios que orienten el desarrollo de la gobernanza de internet
- un marco institucional para la gobernanza de internet
- mecanismos de toma de decisión sobre la gobernanza de internet

Sin embargo, los desarrollos legislativos en algunos países de la región resultan preocupantes.

Tal es el caso del contenido propuesto para el Código Orgánico Integral Penal (COIP) de Ecuador con relación a la conservación de datos y registro. En efecto, el COIP incluye, al momento, contenido orientado a legislar la manera en la que se conservan los datos y se registran las comunicaciones que, de aplicarse, tendría serios efectos negativos.

El artículo plantea:

Art. 474 Conservación de datos y registros. La conservación de datos y registros se rige por las siguientes reglas:

1. Las o los proveedores y distribuidores de servicios informáticos y de telecomunicaciones deben conservar los datos de los abonados o usuarios sobre la base de un contrato y preservar la integridad de los datos sobre números telefónicos, direcciones IP´s estáticas y dinámicas,

así como el tráfico de conexión, acceso a transacciones y la información de los enlaces de comunicación inalámbricas del servicio y la vía de comunicación por un tiempo mínimo de seis meses, a fin de poder realizar las investigaciones correspondientes. Se siguen los mismos preceptos que las interceptaciones de las comunicaciones.

2. Los abonados de servicios de telecomunicaciones que compartan o distribuyan a terceros su interconexión de datos o voz de forma comercial o gratuita, deben almacenar los datos relativos a un usuario sobre la base de un registro físico de conexión y preservar la integridad de los datos sobre identificación del usuario, fecha y hora de conexión inicial y final, por un tiempo mínimo de seis meses con la aplicación de medidas de cámaras de video seguridad, a fin de poder realizar las investigaciones correspondientes.
3. La integridad de los datos es necesaria para la eficacia probatoria de los mismos. Se deben cumplir los requisitos determinados para el registro de comunicaciones para efectuar Ia grabación.
4. La o el juzgador a pedido motivado de la o el fiscal, puede requerir informes sobre datos que consten en registros, archivos, incluyendo los informáticos. El incumplimiento de este requerimiento, Ia falsedad del informe o el ocultamiento de datos generan responsabilidad penal si la infracción constituye delito.

Un planteamiento de esta naturaleza y alcance contradice la posición de Ecuador sobre la vigilancia masiva ejercida por los Estados Unidos sobre otros países del mundo, su voluntad política de proteger a informantes que revelan información de interés público (hay que recordar que el gobierno de Ecuador ofreció asilo político a Julian Assange) y su intención de avanzar en la protección, defensa y promoción de los derechos humanos.

2. Significado y alcance del artículo 474[1]

Sin ambages, el artículo 474 legaliza la vigilancia en la esfera nacional; desconoce el derecho a la privacidad; elimina la posibilidad de avanzar en el desarrollo de legislación de protección de datos personales[2]; establece, como premisa, la presunción de sospecha y culpabilidad de los individuos; y promueve una cultura de desconfianza entre los ciudadanos.

Conviene ir desglosando los problemas que entraña el artículo 474:

"Las o los proveedores y distribuidores de servicios informáticos y de telecomunicaciones deben conservar los datos de los abonados o usuarios sobre la base de un contrato..."

Esto implicaría modificar todos los contratos mediante los que se establece los

1 Este documento no analiza el alcance e implicaciones de otros artículos contenidos en

2 Una tendencia que se ha ido reforzando en América Latina y que incluye, como dato personal, el número telefónico, las direcciones IP dinámicas y estáticas, el tráfico de conexión, información sobre transacciones en línea, entre otros.

términos del servicio prestado por los proveedores de servicios de comunicaciones (CNT, operadoras de telefonía móvil celular, proveedores de servicios de internet, etc.) a los usuarios. Hay que prever que los usuarios podrían negarse a firmar nuevos contratos y podrían, de ser el caso, emprender acciones judiciales por modificaciones a las condiciones contractuales previamente establecidas.

"...y preservar la integridad de los datos sobre números telefónicos, direcciones IP´s estáticas y dinámicas..."

La aplicación práctica de este lineamiento, demandaría una inversión significativamente elevada a fin de abastecerse de servidores con una altísima capacidad de almacenamiento de datos. O, en su defecto, demandaría el alquiler de capacidad de almacenamiento de datos en servidores externos. La inversión debería darse, además, para instalar o reforzar sistemas de seguridad tecnológica y física de los servidores de los prestadores de servicios. Es de prever que, en última instancia, esos costos sean transferidos y asumidos por el usuario final.

Significaría un viraje en las prioridades de inversión. Los proveedores de servicios de comunicación deberán dirigir sus inversiones a la aplicación de las medidas establecidas por el COIP en lugar de hacerlo a la instalación y ampliación de infraestructura para servir áreas que no cuentan con cobertura. Este aspecto desestimulador de la inversión en despliegue de infraestructura va en línea opuesta a las obligaciones positivas que ha asumido el Estado Ecuatoriano de desarrollar políticas públicas y regulaciones que promuevan la inclusión de todos los sectores en el uso y disfrute de las tecnologías de información y comunicación, incluyendo el acceso a internet, y, avanzar, de manera progresiva, hacia el acceso universal.

El almacenamiento de datos implica un riesgo mayor de interceptación, análisis y uso no consentido de los mismos con fines comerciales o de inteligencia. Si el planteamiento implica que los datos sean archivados en servidores del Estado, estamos ante un caso de centralización del almacenamiento y manejo de datos que incrementa aún más el uso indebido de los datos personales con fines de inteligencia, sobre todo si esas prácticas no están acompañadas de mecanismos de rendición de cuentas, de transparencia en el manejo de los datos y de control sobre la agencia nacional de seguridad.

"...,así como el tráfico de conexión,..."

Esto hace referencia a todos los datos, descargas, contenidos de correo electrónico, mensajes transmitidos a través de servicios de mensajería instantánea, voz sobre IP, y, en general, cualquier tipo de información que circula mediante conexión a internet, incluyendo la programación de televisión provista por servicios como Smart TV.

"...acceso a transacciones..."

Hace referencia al tipo de transacción que se efectúa e implicaría que los proveedores y distribuidores de servicios de comunicaciones tengan acceso a claves de cuentas bancarias, de cuentas para compras en línea, de cuentas en redes sociales, entre otros.

"...y la información de los enlaces de comunicación inalámbricas del servicio y la vía de comunicación por un tiempo mínimo de seis meses, a fin de poder realizar las investigaciones correspondientes."

Esto se traduce en el registro de todas las computadoras, teléfonos inteligentes, tabletas y cualquier dispositivos electrónico que se conecten a una red.

Se siguen los mismos preceptos que las interceptaciones de las comunicaciones. Los abonados de servicios de telecomunicaciones que compartan o distribuyan a terceros su interconexión de datos o voz de forma comercial o gratuita, deben almacenar los datos relativos a un usuario sobre la base de un registro físico de conexión y preservar la integridad de los datos sobre identificación del usuario, fecha y hora de conexión inicial y final, por un tiempo mínimo de seis meses con la aplicación de medidas de cámaras de video seguridad, a fin de poder realizar las investigaciones correspondientes.

En la práctica, esto se traduce en que en cualquier lugar de acceso a internet o que ofrezca la posibilidad de conectarse a internet (restaurantes, zonas wifi abiertas, empresas públicas, universidades, centros comerciales, domicilios particulares, etc.), se registren los datos del usuario y de sus comunicaciones/tráfico. Ello convierte a unos en espías de otros y demanda a los usuarios incrementar su capacidad de almacenamiento de datos. Adicionalmente, este lineamiento contenido en el artículo 474, implica que todos los puntos de acceso a internet y otros servicios de TIC (públicos y privados) instalen sistemas de video y registren la actividad de los usuarios.

3. Referencias para el análisis del alcance del artículo 474

A la luz de instrumentos internacionales de derechos humanos, incluyendo la Convención Americana, la seguridad nacional de un país es un objetivo legítimo. Sin embargo, ese objetivo no puede ser interpretado de manera no democrática. Se podría interpretar que la inclusión del artículo 474 en el COIP corresponde a interpretación del principio de seguridad nacional en el marco de la conocida y cuestionada "doctrina de seguridad nacional". Asigna a la ciudadanía en general, por defecto y como premisa, la condición de fuente interna de amenaza. Lo propuesto en el artículo 474 no debe considerarse como un objetivo genuino y legítimo de proteger intereses conexos e inconexos de seguridad nacional. Tampoco puede justificarse por objetivos relacionados con el combate a la delincuencia y al crimen.

El artículo 474 violenta:

- El Art. 12 de la Carta Universal de Derechos Humanos
- El Art. 66, numerales 19, 20 y 21, de la Constitución de Ecuador
- El Art. 76, numeral 2, de la Constitución del Ecuador
- El Art. 92 de la Constitución del Ecuador

Contradice otros artículos incluidos en el COIP: 228 (Interceptación ilegal de datos), 471 (Retención de correspondencia) y 472 (Interceptación de las comunicaciones o datos informáticos).

En el entendido de que en el Ecuador rige un Estado de Derecho en el que la norma es la protección de los derechos humanos y las limitaciones son la excepción, se espera que se revea la inclusión del artículo 474 en el COIP. El Estado Ecuatoriano debe asegurar el cumplimiento del artículo 66, numeral 20 de la Constitución del Ecuador ya que el derecho a la privacidad es una condición indispensable para el goce pleno del derecho a la libertad de expresión y de pensamiento.

Más aún, la protección de datos personales representa una forma especial del derecho a la privacidad. Los Estados tiene, por tanto, la obligación de regular el almacenamiento, procesamiento, uso y transferencia de datos personales de tal manera que se garantice la protección de las víctimas del mal uso de esa información, ya sea por parte de actores estatales o privados[3].

En última instancia, la aprobación del artículo 474 restaría posibilidades de avanzar en la apropiación de las TIC con fines de desarrollo social, económico y cultural. Inhibiría el avance hacia un modelo de desarrollo basado en una matriz productiva que fomente la innovación tecnológica endógena y la creación libre de conocimiento. Y resultaría nocivo para robustecimiento del sistema democrático del país.

Finalmente, se listan, a continuación, algunas referencias ineludibles que orientan el desarrollo de legislación y regulación de las comunicaciones, incluyendo las comunicaciones en internet, de una manera que refuerce el ejercicio de derechos humanos:

- Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones
https://es.necessaryandproportionate.org/text

- Informe del Relator Especial de Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Frank La Rue A/HRC/23/40, 17 de abril de 2013 (con énfasis en privacidad y vigilancia de las comunicaciones)
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Sessio

---

3 Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. 16 May 2011, párr. 58.

n23/A.HRC.23.40_EN.pdf

- Informe del Relator Especial de Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Frank La Rue, A/HRC/17/27, 16 de mayo de 2011 (con énfasis en libertad de expresión en internet)
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

- Propuesta preliminar de resolución de la Asamblea General de Naciones Unidas sobre el derecho a la privacidad en la era digital, propuesta por Brasil y Alemania
http://columlynch.tumblr.com/post/65706075268/the-right-to-privacy-in-the-digital-age