Una cosa es vigilar ciudadanos en procesos judiciales. Otra cosa es espiar por razones de inteligencia. Tras la amarga experiencia de las chuzadas del DAS (q.e.p.d), el PUMA no inspira confianza.

Un PUMA peligroso

En 2007, una resolución del Ministerio de Defensa creó un grupo encargado de administrar la Plataforma Única de Monitoreo y Análisis (PUMA) adscrito a la Dirección de Investigación Criminal e Interpol de la Policía (DIJIN). El propósito del PUMA es registrar o verificar información sobre personas vinculadas con investigaciones judiciales, coordinando tareas de la Policía, de la Fiscalía e incluso de las empresas de telefonía fija.

Cinco años después, los ministerios de defensa, de justicia y de las TIC expidieron el decreto 1704 de 2012, reglamentario de la ley 1453 de 2011. Esta "ley de seguridad ciudadana" no se caracteriza precisamente por garantizar los derechos ciudadanos y fue muy criticada por su sesgo punitivo y por ver a Internet como una herramienta de control más que de libre expresión.

El decreto crea un *sistema de vigilancia de ciudadanos* dentro de procesos judiciales. La vigilancia incluye celular e Internet. En otras palabras, establece la forma como la Policía alimentará al PUMA con información y datos que almacenan los proveedores sobre los ciudadanos.
El decreto también ha sido muy criticado:

· por el reto que supone *equilibrar* la obligación de castigar a culpables de delitos con el derecho a la intimidad, el hábeas data y la libre expresión;
· porque cambia la orden judicial previa por la del propio investigador — el fiscal —, dejando el control judicial para una etapa posterior;
· por los problemas técnicos que implica evitar los abusos o el *espionaje* de los ciudadanos; la memoria de las chuzadas del DAS está viva entre los colombianos.

El decreto se critica también porque impone la obligación a los intermediarios de conservar datos de sus usuarios durante cinco años. En Alemania una medida similar — que mantenía información por 6 *meses* — fue declarada inconstitucional por exceder el estándar de proporcionalidad frente al derecho a la intimidad.

Aunque el decreto no ha sido reglamentado después de un año, todo indica que la vigilancia se hará al estilo del PRISMA de Estados Unidos — usando una interfaz que

facilita la transferencia de datos del intermediario a la plataforma policial — o incluso a través de *backdoors:* puertas traseras en un sistema informático que se saltan los sistemas de seguridad –una especie de entrada secreta para los organismos de vigilancia.

Este tipo de programas son una tentación para que las autoridades cometan espionajes abusivos e implican un riesgo para la seguridad de los datos de los usuarios, como el que hace algún tiempo se presentó en Grecia.

Colombia está lista para adquirir y montar la plataforma, pero seguimos sin ejercer control ciudadano sobre la forma y la tecnología precisa que se usará para hacer la vigilancia. ¿Esperan acaso comprar la tecnología para después regular su utilización?

Diferencia sutil pero importante


Foto: Poster Boy

En todo caso, la propia Policiareconoce que PUMA solo debe emplearse en el marco de *procesos judiciales* y que carece de competencia legal para hacerlo en el marco de operaciones de *inteligencia*del Estado, el ámbito donde estallaron los recientes escándalos en Estados Unidos.

Y en efecto, la ley de inteligencia — que entró en vigor este año — diferencia entre:
· actividades de vigilancia para*procesos judiciales;*
· actividades para *monitoreo*;
· petición de información *técnica* de los suscriptores de proveedores de telecomunicaciones.
Los dos últimos tipos de actividades no están sujetos a control judicial, de manera que en estos casos — y en cualquier otro que el organismo de vigilancia no considere como interceptación de comunicación privada — la autoridad que ordena es el propio director del organismo de inteligencia (o su delegado), sujeto a vagos controles constitucionales.

La diferencia fue avalada por la Corte Constitucional, al afirmar que “no puede confundirse el monitoreo del espectro electromagnético como actividad impersonal y abstracta con los actos propios de una investigación penal, que es individual y

concreta" (sentencia C-540 de 2012).

Esta sentencia deja la impresión de que la Corte falló pensando en las tecnologías telefónicas que le son familiares, aunque aún en ese caso ignoró el riesgo que conlleva acceder por ejemplo a listados de localización de números de celular en lapsos de cinco años. Y de todas maneras no tuvo en cuenta la arquitectura abierta y distribuida de Internet.

Es más: la misma ley de inteligencia se quedó en el pasado. Habla, por ejemplo, de una *solicitud* de información a los operadores de servicios de telecomunicaciones (Art 44), cuando el decreto que la reglamenta ordena a los proveedores de redes y servicios de telecomunicaciones implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones (Art 2). De hecho, aun no es posible establecer con claridad si la definición de *proveedores*incluye o no a los prestadores de servicios en línea — Google, Facebook… — y nada está previsto para ellos.

El alcance del PUMA resulta entonces mucho mayor de lo que imaginaron el legislador y la Corte. El escándalo de PRISMA y los secretos develados por Snowden ponen en evidencia los riesgos del *monitoreo* en Internet, que hace rato dejó de ser sólo mirar tráfico de comunicaciones.

¿Permiso para chuzar?

Y es que el reto proviene de la naturaleza misma de Internet. Como explicó Vivian Newman en su análisis para **Razón Pública**:
"Internet es una red que transporta los datos hacia su destino no por una vía central y cerrada (como en el teléfono), sino por diferentes rutas y diferentes direcciones, dependiendo de factores como la velocidad de la conexión y el tipo y el tamaño de la información."

"Los datos se separan en paquetes en el punto de origen, viajan por la red indiscriminadamente a través de enrutadores o nodos (como el router que uno tiene en su casa y que con los demás enrutadores son la columna vertebral del sistema) y se rearman en su estado original cuando llegan a su destino.

"Así, por ejemplo, si A, desde una dirección IP llama por Skype a B que es otra dirección IP, la voz e imagen de A se descomponen y viajan por diferentes rutas y

en diferentes paquetes mezclados con la voz, datos, video y texto de otra gente que está usando la red y se recomponen al llegar a B".

En consecuencia, el simple *monitoreo* del espectro electromagnético (que ahora incluye comunicaciones relacionadas con los planes de Internet que ofrecen las empresas de celulares) o el pedir información *técnica* de los suscriptores adquiere una dimensión muy cercana a la interceptación de comunicaciones privadas.

De otro lado, si PUMA hace el trabajo para procedimientos judiciales, ¿acaso no sería muy fácil también *monitorear* las redes para los organismos de inteligencia? ¿Dónde y quién está haciendo lo relacionado con inteligencia? ¿Cuál es marco legal?

Requisitos mínimos

Foto: Dan Conley

Al analizar la ley de inteligencia, la Corte Constitucional hizo un recuento de cómo funcionan leyes en varios países — Argentina, Chile, Perú, Estados Unidos, Gran Bretaña — pero no profundizó sobre los problemas que enfrentan. Tampoco se planteó las discusiones más recientes sobre los riesgos para los derechos fundamentales. El análisis está anclado en el pasado.

Los relatores de libertad de expresión de la ONU, Frank La Rue, y de la OEA, Catalina Botero, publicaron recientemente la Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión donde reconocen que hay razones válidas para vigilar las comunicaciones privadas, pero la naturaleza de Internet y de las tecnologías de las comunicaciones pueden hacer que estas actividades afecten desmedidamente derechos como la privacidad y la libertad de expresión.

Por tales razones, indicaron como requisitos para garantizar los derechos en peligro que "los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas; los procedimientos de autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. En todo caso, los

Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas".

Actividades necesarias, pero peligrosas

Al revisar la información disponible acerca de los programas de vigilancia del Estado colombiano sobre la base de estos elementos mínimos, el resultado no es halagador:

a. El marco regulatorio para los programas de vigilancia es escaso y, en algunos temas apenas se ha *anunciado*. Adicionalmente, se han dejado que elementos cruciales sean regulados mediante normas de baja jerarquía: simples decretos o resoluciones.

b. Los órganos que ejecutan y supervisan la vigilancia deben separarse:

i. En lo relacionado con la vigilancia para los *procesos judiciales* será PUMA y la supervisión será judicial, pero posterior.
ii. Pero en cuanto a la vigilancia de los órganos de *inteligencia,* no se sabe a ciencia cierta qué entidad quedará encargada y no existe supervisión. Sólo sabemos que la orden se originará en el *propio*organismo — tras la liquidación del DAS, tampoco sabemos exactamente cuál es — y de hecho hasta ahora es libremente delegable.
c. Sobre los procedimientos de autorización, selección de objetivos y manejo de datos hay algo más de información, pero el diseño general es criticable:
i. Los cinco años de retención no cumplen estándares internacionales de proporcionalidad;
ii. no hay mecanismos de supervisión;
iii. los criterios quedan delegados al juicio de los propios vigilantes;
iv. falta armonizar la legislación existente con las exigencias de la nueva ley de protección de datos.
d. Finalmente, no se contemplan mecanismos de control independientes, que aseguren transparencia y rendición de cuentas por parte de los responsables de estos programas.

Existe una tensión legítima entre la vigilancia para *apoyar la administración de justicia* y los derechos a la intimidad y a la libertad de expresión, que debe ser abordada con más garantías que las previstas hasta ahora en nuestro ordenamiento legal.

Sin embargo, la vigilancia para *inteligencia* es una auténtica amenaza, como afirman La Rue y Botero: los programas de inteligencia tienen que estar sometidos a sistemas de control que prevengan violaciones a los derechos fundamentales. Es necesario definir democráticamente los principios que deben guiar estas actividades.

*** Abogada, magister en Derecho Internacional y de la Cooperación (1993, VUB – Bélgica), candidata al Doctorado (UAB – España), e investigadora sobre temas de Internet, derecho y sociedad. Miembro Fundación Karisma**

@carobotero

http://www.razonpublica.com/index.php/politica-y-gobierno-temas-27/6929-puma-amenazas-a-la-intimidad-y-a-la-libertad-de-expresion.html