ARI 74/2018
14 de junio de 2018

Impacto de nuevas tecnologías en la interceptación de telecomunicaciones

Javier Alonso Lecuit | Miembro Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

El ARI analiza el impacto de las nuevas tecnologías de telecomunicaciones en la interceptación legal de las comunicaciones electrónicas, junto a los distintos aspectos de ciberseguridad relacionados.

Resumen

Los disruptivos desarrollos de las tecnologías de las comunicaciones electrónicas e Internet son determinantes en el ámbito de la ciberseguridad, en general, pero lo son mucho más en relación a las capacidades técnicas con las que cuentan las autoridades para llevar a cabo la interceptación legal de las comunicaciones electrónicas.

La progresiva implantación de las plataformas de comunicaciones móviles 5G, la lenta migración de Internet a direccionamiento IPv6, así como las futuras redes de acceso inalámbrico híbridas (*mesh networks*) junto al masivo uso de cifrado robusto de comunicaciones electrónicas, aplicaciones y terminales, entre otros, son ejemplos de cómo los cambios tecnológicos, además de demandar soluciones robustas en el ámbito de la ciberseguridad pueden alterar significativamente las investigaciones criminales y antiterroristas.

En este ARI se analizan las implicaciones de estas tecnologías en materia de ciberseguridad y muy en particular los retos que plantean estos cambios tecnológicos para mantener las capacidades de los instrumentos de vigilancia e intercepción de las comunicaciones electrónicas utilizados por las fuerzas de seguridad en la actualidad y destinados a un uso muy selectivo bajo el control judicial.

Análisis

Los cuerpos de seguridad operan en un entorno de creciente complejidad tecnológica y algunos gobiernos evalúan con preocupación las implicaciones de estas tecnologías en relación a las capacidades de interceptación legal de las comunicaciones, señalando la necesidad de revisar los instrumentos legales en materia de interceptación. En la actualidad, el debate público se halla particularmente polarizado sobre la conveniencia de regular o contrarrestar el uso del cifrado mediante la adopción de alternativas técnicas y operativas que permitan a las autoridades el acceso a las comunicaciones y dispositivos en el curso de las investigaciones, sin por ello debilitar la protección a la privacidad y el secreto de las comunicaciones. En particular, los mecanismos de cifrado de terminales y servicios en Internet son imprescindibles para la protección de la privacidad de los usuarios y empresas, así como para asegurar la confidencialidad de

las comunicaciones en la Red, es decir, para sustentar la confianza de la Sociedad de la Información. En Europa, las Autoridades Comunitarias mantienen la recomendación de adoptar mecanismos de cifrado robustos establecidos entre los extremos de la comunicación, así como desautorizan la adopción por las autoridades policiales y judiciales de puertas traseras o llaves maestras de descifrado[1].

La delincuencia, el crimen organizado y las organizaciones terroristas utilizan las nuevas tecnologías de comunicaciones electrónicas como instrumentos centrales en la preparación, consecución y propaganda de los delitos, operando a una escala industrial globalizada y careciendo de fronteras territoriales o jurisdiccionales. Grupos extremistas, organizaciones criminales, organizaciones terroristas o pedófilos emplean las plataformas de comunicación en línea o las redes sociales para comunicarse, promover sus actividades e intercambiar contenidos ilícitos eludiendo la intervención de las autoridades mediante el uso de servicios de comunicaciones cifradas o servicios almacenamiento en la nube (*cloud*) emplazados donde no tienen jurisdicción los países en los que se cometen los delitos[2]. Las pruebas electrónicas se encuentran emplazadas en terceros países, almacenadas frecuentemente en infraestructuras de información virtualizadas, utilizadas éstas por servicios Internet de uso común tales como mensajería electrónica, correo electrónico y almacenamiento en *cloud*.

En el ámbito de las telecomunicaciones, las redes móviles 5G, la prolongada migración de Internet a direccionamiento IPv6 o las próximas redes de acceso inalámbrico híbridas (*mesh networks*) junto con la aplicación de técnicas que refuerzan el anonimato de los usuarios en la red, plantean dificultades añadidas en materia de ciberseguridad y en la interceptación legal de comunicaciones. En contrapartida, el uso de las nuevas tecnologías también refuerza las capacidades operativas de los cuerpos de seguridad y autoridades judiciales en la prevención y neutralización de actividades criminales y contribuye a la defensa de los derechos y libertades individuales de los ciudadanos, pero les obliga a sostener un elevado ritmo de innovación tecnológica en sus procedimientos de investigación.

Las redes de comunicaciones móviles 5G

La tecnología 5G es uno de los principales habilitadores tecnológicos de la Sociedad de la Información. La conectividad inalámbrica entre dispositivos y sistemas autónomos (máquina a máquina, M2M) desempeñará un rol esencial en la transformación industrial (Industria 4.0) y en servicios basados en el despliegue de dispositivos conectados del Internet de las Cosas (IoT). La tecnología 5G permite multiplicar 10 veces la disponibilidad de espectro (x10), la eficiencia espectral (x10) y la densificación de la red de acceso (x10), lo que multiplica por mil (X1000) sus mejoras técnicas respecto a las redes 4G/LTE. Conlleva la completa transformación de las redes de

[1] "Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU", Bruselas, 11 abril 2018, p. 2.

[2] Más de la mitad de las investigaciones penales incluyen hoy en día una solicitud transfronteriza para obtener pruebas electrónicas que obran en poder de prestadores de servicios establecidos en otro Estado miembro o fuera de la UE. "Security Union: Commission facilitates access to electronic evidence", Nota de prensa, Bruselas, 17 abril 2018.

(cont.)

telecomunicaciones, incluida la virtualización de las funciones de red (Network Function Virtualization, NFV) y la centralización de las redes definidas por software (Software Define Network. SDN)[3]. La infraestructura del operador de telecomunicaciones estará formada por varios centros de procesado de datos próximos a las estaciones base 5G (*clouds* de acceso) interconectados a un *cloud* central. Esta nueva arquitectura permitirá que cada cliente corporativo del operador -por ejemplo, el propietario de una plataforma M2M de automoción- gestione en tiempo real los recursos de telecomunicaciones que necesite para su plataforma M2M mediante a la definición de unos elementos y capacidades de red virtualizados e individualizados ("*network slice*"[4]) pertenecientes a la red del operador de telecomunicaciones y adaptados en tiempo real a sus particulares necesidades técnicas.

Los servicios M2M requieren de una adaptación muy flexible, dinámica y eficiente de las capacidades técnicas de conectividad ofrecidas por los operadores de comunicaciones electrónicas para aplicar a los distintos sectores (automoción, sanidad, energía, *smart grid*, entre otros). En este contexto, surge la necesidad de garantizar que determinados parámetros críticos, por ejemplo, la latencia o la disponibilidad de servicio sean apropiados a las necesidades de cada sector, pero la arquitectura de Internet no es adecuada para interconectar determinadas aplicaciones M2M al no poder garantizar la calidad prefijada del servicio[5].

Por consiguiente, surge la necesidad de ofrecer una nueva tipología de servicios de conectividad móvil de datos ("*servicio gestionado*") que, además de incorporar la escala y resiliencia de Internet, proporcione una calidad de servicio asegurada de extremo a extremo, gestionada y particularizada ésta a cada clase de servicio y cliente en combinación con los apropiados niveles de seguridad. Para garantizar la calidad de la conexión extremo a extremo los operadores habrán de coordinar la gestión de recursos técnicos entre las distintas redes. Adicionalmente, los clientes de los servicios M2M habrán de disponer de capacidades de gestión remota del servicio de comunicaciones electrónicas mediante las *application programming interfaces* (API) estandarizadas y segurizadas que permiten la conexión entre distintos módulos de software.

[3] Sustitución del actual equipamiento de propósito específico interconectado físicamente (*routers*, *catchers*, servidores de acceso, DPIs, etc.) por agrupaciones de máquinas virtuales de propósito general que repliquen a nivel lógico y funcional la actual red del operador.

[4] "Network slicing", "*rebanado*" o "*segmentación*" es una tecnología que permite a los operadores de redes móviles 5G gestionar y operar múltiples redes virtualizadas sobre una misma infraestructura de red común, donde los recursos de la red física son adaptados a cada tipo de uso o de cliente. Esta "*segmentación*" hace posible una partición virtual de la red de acceso por radio (RAN), de los componentes de la red de conmutación y de agregación, así como de los centros de datos, donde se alojan los contenidos y las aplicaciones. Cada *slice* se conforma según los distintos tipos de uso y cliente, quienes establecen el desempeño demandado de la red caso a caso, en base a parámetros tales como la capacidad de transferencia, latencia, seguridad, confiabilidad o cobertura geográfica, entre otros.

[5] Por este motivo, las aplicaciones de Internet son diseñadas para maximizar la experiencia del usuario contando con la mejor calidad proporcionada por Internet en cada instante (*best effort*), calidad de servicio que es indiferenciada a las aplicaciones (sean correo electrónico, red social, video *streaming*, juegos en red, etc.). Así, el ancho de banda y latencia que ofrece la Red responde a los recursos disponibles en cada instante junto al grado de utilización carga) entre la red del operador de acceso a Internet y los restantes segmentos de la conexión entre el usuario y el proveedor de Internet, segmentos éstos que escapan a la gestión técnica del operador de acceso a Internet (ISP).

(cont.)

El actual estadio de la tecnología 5G presenta algunos retos para la seguridad y la privacidad de las comunicaciones. Por un lado, no se ha conseguido todavía poner de acuerdo a los distintos organismos de estandarización: European Standards Organization (ETSI), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE) y Claud Security Alliance (CSA), entre otros, para definir y estandarizar los protocolos 5G, a pesar del esfuerzo de la industria y autoridades europeas para lograr el liderazgo mundial a través de iniciativas como el "5G Action Plan" de la Comisión Europea.

En concreto, la seguridad de las plataformas 5G ha de tener en consideración los siguientes elementos:

- Los riesgos vinculados a nuevos modelos de relación entre la plataforma tecnológica del cliente y el servicio de red ofrecido por el operador 5G[6], así como los relacionados con la virtualización de la plataforma de red y servicios.

- La evolución en las amenazas de ciberseguridad focalizadas éstas hacia distintos entornos de criticidad crecientes, en particular a los centros de datos del operador de telecomunicaciones y los sistemas IoT de los operadores de infraestructuras críticas.

- La exigencia de ciudadanos, corporaciones y reguladores en preservar la privacidad y confidencialidad de los datos y metadatos de las comunicaciones en un contexto donde la explotación comercial de la información (Big Data) junto al empleo de inteligencia artificial en el nuevo modelo de producción (Industria 4.0) adquieren una importancia central.

En el ámbito de la ciberseguridad aparecen nuevos factores a tener en cuenta en la gestión del riesgo tales como la muy diversa tipología y criticidad de las aplicaciones M2M (domótica, servicios y dispositivos sanitarios, conducción autónoma, infraestructuras críticas, etc.); el gran número de dispositivos IoT junto a la dificultad de realizar actualizaciones, las limitaciones en el uso de cifrado en los dispositivos alimentados por baterías debido al mayor consumo de energía (entre 10 y 100 veces superior); la apertura al cliente de funciones de gestión y supervisión de la red del operador de telecomunicaciones con la consiguiente necesidad de blindaje lógico entre los distintos *network slices* o la concentración de funciones y recursos de la red virtualizados en unos pocos centros de datos (*cloud*) del operador.

En el ámbito de la interceptación legal de las comunicaciones existe una estrecha relación entre las nuevas características de las redes 5G, las soluciones de ciberseguridad establecidas y las capacidades de interceptación de las comunicaciones. De este modo, las plataformas 5G habrán de ofrecer medios técnicos que permitan mantener las actuales capacidades de interceptación de las comunicaciones, considerando nuevos factores tales como, por ejemplo, la masiva transferencia de datos

[6] El cliente corporativo de plataformas M2M y terceros agentes que intervengan su cadena de provisión tendrán acceso a las capacidades del *network slice* de red asignado al cliente, pudiendo instalar y gestionar aplicaciones de su servicio M2M en la red del operador.

entre plataformas M2M a través de las redes inalámbricas, el significativo aumento en el número de estaciones radio 5G o la arquitectura de red virtualizada.

Por ambos motivos, es necesario redefinir y estandarizar los mecanismos de seguridad establecidos extremo a extremo a todos los niveles de la arquitectura de comunicaciones (terminales, red de acceso móvil, núcleo de red, plano de control, etc.) y evaluar la adecuación de los actuales mecanismos de seguridad implantados en las redes 4G. En esta línea, ENISA ha publicado las directrices "Threat Landscape and Good Practice Guide for Software Defined Networks/5G" que establecen una taxonomía de amenazas, recomendaciones y buenas prácticas en torno a la virtualización y el acceso inalámbrico (RAN) a las estaciones base de las plataformas 5G[7]. Los mecanismos de seguridad en actual desarrollo para las redes 5G se centran en las siguientes funciones:

- El aislamiento de los recursos virtualizados de cada *network slice* mediante cifrado robusto, la adopción de políticas de seguridad del *slice* particularizadas cliente a cliente y por clases de servicio, junto a certificaciones de seguridad específicas;

- La gestión segura de identidades de los agentes que interactúan en la plataforma 5G (dispositivos IoT, terminales, usuarios, operadores interconectados a la red, personal técnico, entre otros);

- Una monitorización y gestión de la seguridad del plano de control (SDN) y del plano de conectividad (NFV) diferenciada;

- La escalabilidad y flexibilidad de las arquitecturas de seguridad, adaptadas éstas a la evolución de las amenazas;

- La seguridad del segmento de acceso radioeléctrico (ej. estaciones base) frente a ataques de denegación de servicio realizados desde terminales manipulados o la inyección de tráfico malicioso en el plano de usuario.

Adicionalmente, la seguridad, privacidad y resiliencia de las plataformas móviles 5G excede aspectos de orden tecnológico siendo preciso tener en cuenta exigencias legales establecidas por los distintos sectores verticales (banca, sanidad, seguridad vial, operadores de infraestructuras críticas, etc.) junto a la evolución de la regulación sectorial de telecomunicaciones (Digital Single Market), de la privacidad (GDPR y e-Privacy) o neutralidad de red, entre otras.

Por último, cabe destacar consideraciones en el ámbito la seguridad nacional y económica que trascienden los aspectos tecnológicos. En este sentido, la disruptiva transformación de las actuales redes y servicios podría incrementar la dependencia tecnológica de operadores y países de unos pocos suministradores. La vasta renovación tecnológica obligará a los operadores de comunicaciones electrónicas a rentabilizar las

[7] En EE.UU. el regulador de telecomunicaciones (FCC) ha emitido unas recomendaciones sobre ciberseguridad en redes 5G orientadas a la industria IoT accesibles en https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/TAC-5G-Cybersecurity-Subcommittee-09-12-16.pdf

importantes inversiones realizadas en espectro e infraestructura, exigencia que puede alterar la dinámica competitiva al conducir al sector de las telecomunicaciones a una concentración oligopólica del mercado. En este contexto, una posible separación estructural entre las infraestructuras de red y los servicios de comunicaciones, la fuerte competencia entre los operadores de telecomunicaciones y proveedores de aplicaciones de Internet en ofrecer servicios en Internet, así como la intervención de los estados en este proceso de transformación o la creciente dependencia tecnológica en terceras regiones geopolíticas serán aspectos determinantes a tener en cuenta en el marco de la seguridad de las redes y servicios 5G.

En el ámbito de la interceptación de las comunicaciones cabe reiterar el importante papel que han de desempeñar los organismos de estandarización en la definición de las apropiadas capacidades que faciliten la interceptación de las comunicaciones del conjunto de servicios y la escala que ofrecerá esta nueva tecnología, así como afrontar nuevos escenarios tecnológicos que pueden dificultar el curso de las investigaciones policiales. Por ejemplo, la tecnología 5G permitirá simultanear distintos medios de acceso a la red (en lugar de solo medio por conexión como hasta ahora) o encaminar la transferencia de datos a través de redes privadas, evitando el tránsito a través de redes de comunicaciones móviles públicas. La multiplicidad de identificadores asignados por la red 5G a una conexión de usuario y terminal dados agrava las dificultades que ya experimentan las investigaciones actuales por la conmutación automática de los terminales móviles entre redes wifi y 4G.

La migración de Internet a direccionamiento IPv6

Conocer la dirección IP de una comunicación en Internet es imprescindible en el curso de las investigaciones e interceptaciones de las comunicaciones, ya que proporciona información de la comunicación (metadatos) y el acceso al tráfico intercambiado entre el usuario e Internet, es decir, al contenido de la comunicación.

El direccionamiento IPv6 soluciona la actual escasez de direcciones IPv4 en las redes públicas, una vez hayan migrado la práctica totalidad de usuarios de Internet, haciendo innecesaria la reasignación de direcciones IP públicas. El actual esquema de direccionamiento público (IPv4) utiliza 32 bits, es decir, tiene capacidad para establecer 4.3 mil millones de conexiones en Internet. El enorme aumento de dispositivos conectados a Internet ha superado con creces el número de direcciones IPv4 disponibles, esta escasez de direcciones hubiera hecho insostenible el crecimiento del Internet de las cosas (IoT).

Para suplir temporalmente esta limitación, los operadores de red utilizan técnicas que permiten la reutilización y compartición de una misma dirección IP pública al tiempo que el IETF, el consorcio de colaboración técnica más importante en Internet, procedió en 1998 a ampliar el campo de direcciones IP a 128 bits (IPv6) siendo posible establecer un número prácticamente ilimitado de conexiones simultáneas en Internet (2^{128} o 340 sextillones de direcciones). El uso de direcciones IPv6 públicas se extendió a los proveedores de servicio de Internet (redes sociales, comercio electrónico, buscadores, entre otros).

Habida cuenta de la necesidad de adaptar las redes y dispositivos al nuevo direccionamiento, los operadores y fabricantes de terminales han establecido

mecanismos técnicos para que resulte prácticamente transparente al usuario la transición de IPv4 a IPv6 (mientras dura la transición, las redes y terminales han de tener la capacidad de procesar tráfico direccionado con ambas versiones o *dual stack)*. Desafortunadamente, la lentitud, costes e incompatibilidades de esta migración plantean dudas acerca de la finalización de la transición iniciada hacia 2011, existiendo la posibilidad de que se prolongue a largo plazo el uso de doble direccionamiento en Internet. Se estima que a inicios de 2018 ha migrado menos del 25% del tráfico global de Internet (Google señala que el uso mundial de IPv6 entre sus usuarios aumentó del 0,1%, en enero de 2009, a más del 20% en diciembre de 2017), con una implantación muy irregular en función de las geografías, siendo los operadores de telecomunicaciones e ISPs quienes lideran el proceso[8].

Desde el punto de vista de la ciberseguridad, la migración a IPv6 podría acentuar notablemente la escala e impacto de los ataques de denegación de servicio en Internet (DDoS), dado que los sistemas anti DDoS están dimensionados para hacer frente a tráficos IPv4[9]. Desde la perspectiva de la interceptación de las comunicaciones, la incorporación de IPv6 a Internet tiene varias implicaciones. Los mecanismos de traducción entre direcciones IPv4 e IPv6 (Network Address Translation, NAT) y las técnicas utilizadas para que un elevado número de usuarios de un operador dado compartan una misma dirección IP pública dificultan notablemente la trazabilidad de las comunicaciones, así como la interceptación de un usuario determinado. Por ello, en febrero de 2018, Europol y el European Cybercrime Center solicitaron a los operadores de telecomunicaciones que aceleraran la migración a IPv6, dado que el seguimiento individual de las conexiones a través de los registros de los NAT es muy costoso y poco escalable.

En un futuro, es previsible que los operadores de telecomunicaciones empleen un direccionamiento IPv6 estático, en lugar de una dirección IP debido al número prácticamente ilimitado de direcciones, o semipermanente entre el usuario y la red (en la actualidad la asignación de direcciones IPv4 es dinámica o temporal), facilitando de este modo la identificación e interceptación del terminal del usuario y dispositivos IoT. No obstante, esta ventaja se verá contrarrestada por la aplicación de mecanismos de autoasignación de direcciones IPv6 privadas desde el terminal de usuario, modificando continuamente el valor de la dirección IPv6 con el fin de proteger la privacidad de la conexión[10]. Cabe asimismo señalar el impacto que tiene para los operadores gestionar la complejidad e incremento de coste de mantenimiento de los registros de los servidores de acceso a Internet[11] ocasionado por el elevado número de direcciones IPv6

[8] "IPv6 deployment on the global Internet", The Internet Society http://www.worldipv6launch.org/measurements/, http://www.worldipv6launch.org/infographic/

[9] En febrero de 2018 se registró el primer ataque DDoS originado desde direcciones nativas IPv6 hacia servidores DNS, "First true native IPv6 DDoS attack spotted in wild", 28 febrero 2018, https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-in-wild/article/747217/

[10] IBM RFC 4941, "IPv6 privacy extensions e IPv6 Privacy Addresses Provide Protection Against Surveillance And Tracking", accessible en https://www.internetsociety.org/blog/2014/12/ipv6-privacy-addresses-provide-protection-against-surveillance-and-tracking/

[11] La legislación sobre retención de datos exige a los proveedores de acceso a Internet que mantengan los registros que vinculan las direcciones IP asignadas a los clientes para cada sesión con el fin de que esta información esté disponible para las agencias de seguridad durante el periodo de retención máximo y condiciones de acceso a los metadatos establecidos por ley.

en uso, en particular si la asignación de direcciones viene dada por proveedores de servicios de Internet externos al operador de acceso.

Desde esta misma perspectiva, es importante indicar que IPv6 facilitará la incorporación generalizada de mecanismos de cifrado en la conexión a los proveedores de Internet sin la intervención del usuario, aumentando significativamente el volumen de servicios de Internet cifrados, y por lo tanto dificultando la interceptación de estas comunicaciones. Por último, apuntar que un usuario podrá tener asignadas simultáneamente varias direcciones IPv6 públicas a un mismo servicio de acceso a Internet (por ejemplo, una persona que se comunique a través de una red social podría utilizar una dirección IPv6 pública distinta a la asignada para navegar por Internet), dificultando esto su identificación e intercepción.

Las redes de acceso inalámbrico en malla (*mesh networks*)

El acceso inalámbrico a Internet a través de redes en malla[12] planteará nuevos retos para llevar a cabo la identificación del terminal del usuario, del operador de acceso de telecomunicaciones o para realizar el trazado de las conexiones, complicando la interceptación de estas comunicaciones. Por una parte, la relación entre el contratante del punto de acceso al servicio de Internet y el usuario queda desdibujada ya que varios usuarios podrán compartir uno o varios puntos de acceso a Internet. Por otra, se desvanece la frontera entre la terminación de la red pública de los operadores de acceso a Internet y las distintas redes privadas conectadas entre sí en malla.

Adicionalmente, la escala que podrían alcanzar estas mallas, en las que la vinculación entre el acceso a red y el usuario no es estática ni pre-establecida, añadido al cifrado de las conexiones necesario para garantizar la confidencialidad de las distintas comunicaciones en la malla dificultará la identificación e intercepción de las comunicaciones de un determinado usuario.

En este sentido, el diseño de los protocolos de comunicaciones que implementen las redes malladas debería incorporar mecanismos que permitan la trazabilidad en tiempo real e interceptación de las comunicaciones, así como facilitar la atribución de las responsabilidades que adquieren los distintos usuarios en caso de que más de un operador de red ofrezca el servicio de acceso a Internet en la red mallada.

Conclusiones

La evolución de las tecnologías de telecomunicaciones tiene distintas implicaciones en la interceptación de las comunicaciones electrónicas. Para afrontar las crecientes dificultades que experimentan las autoridades de seguridad y judiciales, es de gran

[12] Una red en malla se caracteriza por contar con una topología en la que cada nodo se haya conectado a todos los restantes nodos. Así, por ejemplo, el enrutador de un usuario puede formar parte de la misma malla que sus vecinos, cuyos nodos se configuran automáticamente estableciendo, por ejemplo, la ruta de salida a internet a través del acceso al operador que resulte en cada instante óptima y los dispositivos reciban un nivel de señal wifi óptimo, con independencia de su ubicación o de su punto de acceso a Internet. De esta manera, en circunstancias adversas el usuario accederá de forma automática a Internet a través de la conexión de su vecino. Las redes en malla de uso personal son cada vez más frecuentes entre teléfonos inteligentes, relojes y otros dispositivos; sin embargo, las redes malladas wifi para el acceso a Internet se encuentran en fase de desarrollo.

relevancia mantener las actuales capacidades de interceptación desde las primeras etapas de la definición y estandarización técnica de protocolos y redes de comunicaciones, maximizando su seguridad por diseño.

En respuesta a los retos suscitados, gobiernos y legisladores estudian cambios del marco legal que permitan revertir las crecientes dificultades que experimentan las fuerzas de seguridad y autoridades judiciales en el curso de la interceptación de las comunicaciones e investigaciones, analizando entre otros puntos:

- La incorporación de instrumentos de vigilancia e intercepción alternativos más intrusivos destinados a un uso muy selectivo bajo el control judicial (puertas traseras, distintas técnicas de descifrado, infiltración en los terminales, entre otros) u otras técnicas de investigación alternativas para el acceso a comunicaciones cifradas;

- La adecuación y márgenes que ofrece el marco legal a la monitorización generalizada de los metadatos de las comunicaciones (*bulk interception*);

- El empleo por las agencias y fuerzas policiales de tecnologías de interceptación anteriormente restringidas a determinadas agencias y cuerpos de seguridad, gracias a su mayor operatividad, disponibilidad comercial y menor coste (ej. IMSI *catchers* portátiles);

- Establecer medidas de control para evitar que el crimen organizado y el terrorismo se beneficie de la comercialización y uso de los más recientes avances en las tecnologías de comunicaciones e interceptación.

Asimismo, la adaptación de los instrumentos jurídicos para la interceptación ha de tener en consideración otros ámbitos no tecnológicos, entre ellos, los aspectos jurisdiccionales de Internet, el rol, obligaciones y la seguridad jurídica de los operadores de telecomunicaciones y proveedores de internet o los mecanismos de control judicial para la protección de los derechos fundamentales.