Ciberseguridad, privacidad e interceptación legal en las redes 5G: una realidad poliédrica

Javier Alonso Lecuit | Investigador sénior asociado y miembro del Grupo de Trabajo de Ciberpolítica, Real Instituto Elcano.

Tema

La definición de estándares técnicos 5G responde principalmente a motivaciones comerciales y tecnológicas, por lo que no garantizan el adecuado equilibrio entre ciberseguridad, protección de los derechos civiles y capacidades para la interceptación legal.

Resumen

El despliegue de las redes 5G se está llevando a cabo con fuerte apoyo institucional y una atención geopolítica y mediática sin precedentes. Su arquitectura de referencia, protocolos de comunicación e interfaces (interoperabilidad) se concretan en estándares técnicos definidos en el marco de los organismos internacionales especializados. Su definición la lideran agentes del mercado cuya prioridad es el desarrollo de negocio y la hegemonía tecnológica, por lo que la estandarización técnica de aspectos como la ciberseguridad o la interceptación legal, entre otros, no se aborda simultáneamente, con lo que las autoridades policiales y judiciales tienen que buscar *a posteriori* soluciones técnicas y normativas que no son las óptimas mientras los operadores se ven obligados a asumir costes regulatorios adicionales.

Análisis

Los estándares técnicos de las nuevas redes 5G, desarrollados al ritmo de la acelerada innovación tecnológica para ocupar posiciones de mercado dominantes, no han tenido suficientemente en cuenta en su elaboración los problemas que podrían plantear en relación con la ciberseguridad, la interoperabilidad, la certificación, la identidad o la protección de la privacidad y el secreto de las comunicaciones móviles, tal y como se analiza a continuación.

La ciberseguridad de las redes 5G

La importancia de garantizar la confidencialidad, disponibilidad e integridad de las redes 5G responde a razones sustanciales. En primer lugar, es una de las principales palancas tecnológicas habilitadora del proceso de digitalización de la sociedad. Después, es resultado de la evolución natural de las actuales redes de acceso móvil, que integrará en una única red los accesos de fibra, por lo que su seguridad afecta al conjunto de los ciudadanos, corporaciones, Administraciones Públicas y fuerzas de seguridad, además de las infraestructuras críticas y sistemas para misiones críticas. También incorporan cambios tecnológicos significativos como la virtualización de las infraestructuras, la

descentralización de las arquitecturas, la computación en el borde de la red, el aumento en el número de antenas o una mayor dependencia de componentes de *software*, de modo que se incrementa el número de tipos de suministradores de los operadores de telecomunicaciones, lo cual aumenta notablemente las potenciales vulnerabilidades y la superficie de exposición a ciberataques[1].

Las exigencias de seguridad y resiliencia de las redes 5G han llevado a adoptar una aproximación basada en la gestión del riesgo que asegure las funciones críticas –entre ellas, la interceptación legal–, habida cuenta de la complejidad de una arquitectura de red en constante evolución[2]. En esta línea, la Comisión Europea aprobó en enero de 2020 un conjunto de medidas (*EU Toolbox of Risk Mitigating Measures*) que tienen por objeto identificar escenarios y categorías de riesgos tales como la criticidad de los elemento de red, la dependencia de proveedores únicos o la interferencia de terceros en la cadena de suministro, entre otros, en función de los cuales los Estados pueden regular las condiciones de seguridad en el plano de señalización y gestión de la red y restringir, prohibir o imponer requisitos en el suministro, despliegue y operación de los equipos de las redes 5G.

En julio de 2020 se publicó un informe de situación[3] que resalta la importancia de considerar la red como un todo e introduce criterios más restrictivos para los elementos que forman el núcleo de la red y también para otros activos críticos tales como las funciones para la gestión de la red o la red de acceso a las estaciones de radio. El informe recomienda mitigar los riesgos derivados de la dependencia de suministradores, establecer medidas y periodos de transición que limiten el despliegue de suministradores ya establecidos en función del perfil de riesgo y adoptar estrategias de despliegue basadas en varios suministradores por operador o por país.

Mientras que en el sector privado, principalmente operadores de comunicaciones electrónicas y suministradores, habrán de implantar y asumir el coste de estas directrices para garantizar la seguridad de las infraestructuras 5G, los Estados son responsables de los impactos en la seguridad nacional, por lo que es sustancial potenciar la colaboración público-privada entre los agentes privados y las autoridades gubernamentales, fuerzas y cuerpos de seguridad, adjudicatura y autoridades regulatorias.

[1] El informe elaborado por ENISA (2019), "ENISA threat landscape for 5G Networks", noviembre de 2019, establece una taxonomía y evaluación de las ciberamenazas, los activos de la red afectados en cada caso, los agentes de las amenazas y los distintos cursos de acción: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

[2] Existen discrepancias entre las autoridades de distintos países sobre la frontera que delimita el núcleo de la red 5G (*core*) y su periferia (*edge*) tomando en consideración las interdependencias y los impactos en la seguridad entre ambas partes. Por ejemplo, el Reino Unido sostiene que existe una separación clara, mientras que las autoridades australianas consideran que existen importantes interdependencias de seguridad entre el núcleo y el borde de la red. Por otro lado, funciones como la segmentación de red (*network slicing*) añaden complejidad a la gestión de la seguridad, porque ofrecen al cliente capacidades de control de la red virtualizada.

[3] NIS Cooperation Group (2020), "Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity", julio de 2020, https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

El rol de los estándares y la interoperabilidad en la seguridad

El estándar 5G –actualmente en la versión 16[4]– ha sido elaborado y aprobado por el consorcio 3GPP en diciembre de 2019[5]. Los estándares de telecomunicaciones desempeñan un papel determinante en el despliegue de nuevas tecnologías, evitan que los operadores sean cautivos de tecnologías propietarias, promueven la competencia entre suministradores y mejoran la seguridad de las redes, no solo desde el punto de vista técnico, sino también estratégico y geopolítico. La normalización de una solución técnica –es decir, arquitecturas de referencia, protocolos de comunicación e interfaces– permite la interoperabilidad entre sistemas de distintos suministradores y la interconexión entre operadores. Es una labor técnica compleja y lenta, liderada por suministradores y operadores de telecomunicaciones que ponen en juego su liderazgo tecnológico, la titularidad de patentes y, en estos últimos años, los equilibrios geopolíticos en materia de seguridad. No obstante, la aprobación de un determinado estándar no implica *per se* la completa interoperabilidad y uniformidad entre redes, porque factores como una interpretación equivocada, parcial o sesgada del estándar o una implementación incorrecta o provisional, entre otros, pueden afectar a su funcionamiento. En cualquier caso, el despliegue de una red es un complejo y lento proceso iterativo de depuración técnica y puesta en operación en el que la confianza y la estrecha colaboración entre el operador y el suministrador son esenciales. Desde la perspectiva de la ciberseguridad, el uso de estándares abiertos facilita la resolución de vulnerabilidades y la disponibilidad de múltiples suministradores, genera sinergias, reduce la dependencia tecnológica e incentiva la competencia del mercado.

Certificaciones de ciberseguridad

Una de las principales herramientas habilitadas por las autoridades regulatorias europeas para verificar el cumplimiento de unos niveles mínimos de seguridad ha sido la creación de un marco europeo de certificación de productos, servicios y procesos, incluido en el paquete regulatorio Cibersecurity Act de diciembre de 2018, para cuya supervisión se ha creado el grupo European Cybersecurity Certification Group (ECCG) en apoyo de ENISA y la Comisión Europea. Incluye el desarrollo de los esquemas de certificación de equipos y programas de las redes 5G, tal como incide el EU Toolbox, que se ha encontrado con la oposición de la industria de los integradores de IT –muy activos en ofrecer soluciones para la virtualización de red– y proveedores de servicios digitales (Information Technology Industry Council, ITIC) porque consideran que una regulación de la ciberseguridad basada en la certificación no es el mecanismo más apropiado para reducir los riesgos debido a su carácter estático comparado con el alto ritmo de actualización de las versiones con las que se corrigen los errores y

[4] 5G Americas (2020), "The 5G Evolution: 3GPP Releases 16-17. 5G Americas", enero de 2020, https://www.5gamericas.org/wp-content/uploads/2020/01/5G-Evolution-3GPP-R16-R17-FINAL.pdf.

[5] Otros organismos de normalización también participan en la estandarización de redes 5G y en ocasiones compiten por la aprobación de una determinada propuesta. Entre ellos cabe mencionar la UIT (Unión Internacional de Telecomunicaciones), liderado por los Estados; ETSI (European Telecommunication Standardization Institute), o ISO (International Organization for Standardization), así como alianzas entre distintos agentes del mercado creadas para establecer desarrollos específicos que pueden acabar siendo estándares *de facto*, como por ejemplo la iniciativa OpenRAN, establecida para la mejora de la interoperabilidad entre estaciones de radio 5G de distintos suministradores, que promueve la apertura de las interfaces y arquitecturas mediante código abierto.

vulnerabilidades de los productos, además de resultar un proceso muy lento y costoso[6]. En su lugar, aconsejan a los Gobiernos que valoren la adopción de modelos alternativos basados en la transparencia, las declaraciones de conformidad del suministrador o evaluaciones realizadas por terceros de confianza.

La gestión de la identidad

Asimismo, hay que señalar la importancia que adquieren las arquitecturas para la gestión de identidades, la autenticación y acceso a los sistemas de operación y la gestión de servicios de las redes 5G. Tal y como se ha indicado a propósito de la relación entre identidad digital y seguridad virtual, una diferencia de las redes 5G respecto a las redes actuales es la virtualización de funciones mediante *software*, el cual se ejecuta en máquinas de propósito general alojadas en centros de datos. En la implementación y operación de estas intervienen múltiples suministradores, por lo que la seguridad perimetral pierde validez en la prevención de ataques centrados en la identidad, ya que a diario habrá de acceder a estos sistemas un variado perfil de usuarios a través de redes externas al operador; entre otros, suministradores de la cadena de provisión, empleados, clientes de los servicios virtualizados (*slices*)… Igualmente, habrán de gestionarse de forma automática el alta, acceso y operación entre un elevado número de terminales y máquinas de servicios IIoT.

En este sentido, las redes 5G son un claro caso de uso de la gestión de la identidad y acceso basado en el paradigma de confianza cero (*zero trust network access*), es decir, en la gestión del riesgo a través de la verificación activa de la identidad de los usuarios, de la integridad de las transacciones y de la integridad y estado de los dispositivos[7]. Desaparece así, a efectos de la gestión de la identidad y acceso, la distinción entre red pública (por ejemplo, internet) y privada (intranet) en un escenario de desconfianza mutua por defecto entre equipos de red, usuarios, servicios y datos. En efecto, bajo este paradigma la confianza entre pares es la mayor vulnerabilidad posible: cada solicitud de acceso, tenga origen desde el interior o el exterior de la red, ha de tratarse como potencialmente hostil y otorgar, por tanto, el acceso a las aplicaciones y servicios caso a caso en función de la identidad del usuario en combinación con otros atributos e información de contexto.

Protección de la privacidad y secreto de las comunicaciones móviles

En el ámbito del usuario, la necesidad de asegurar la privacidad y confidencialidad de las comunicaciones se amplía con el 5G debido a la transmisión de grandes volúmenes de información sensible hombre-máquina y máquina-máquina: datos privados, datos industriales y secretos comerciales vinculados a la digitalización y la transformación de la industria 4.0. La tecnología 5G ha reforzado el aseguramiento de estos derechos protegiendo la identificación e interceptación directa sin garantías legales de las

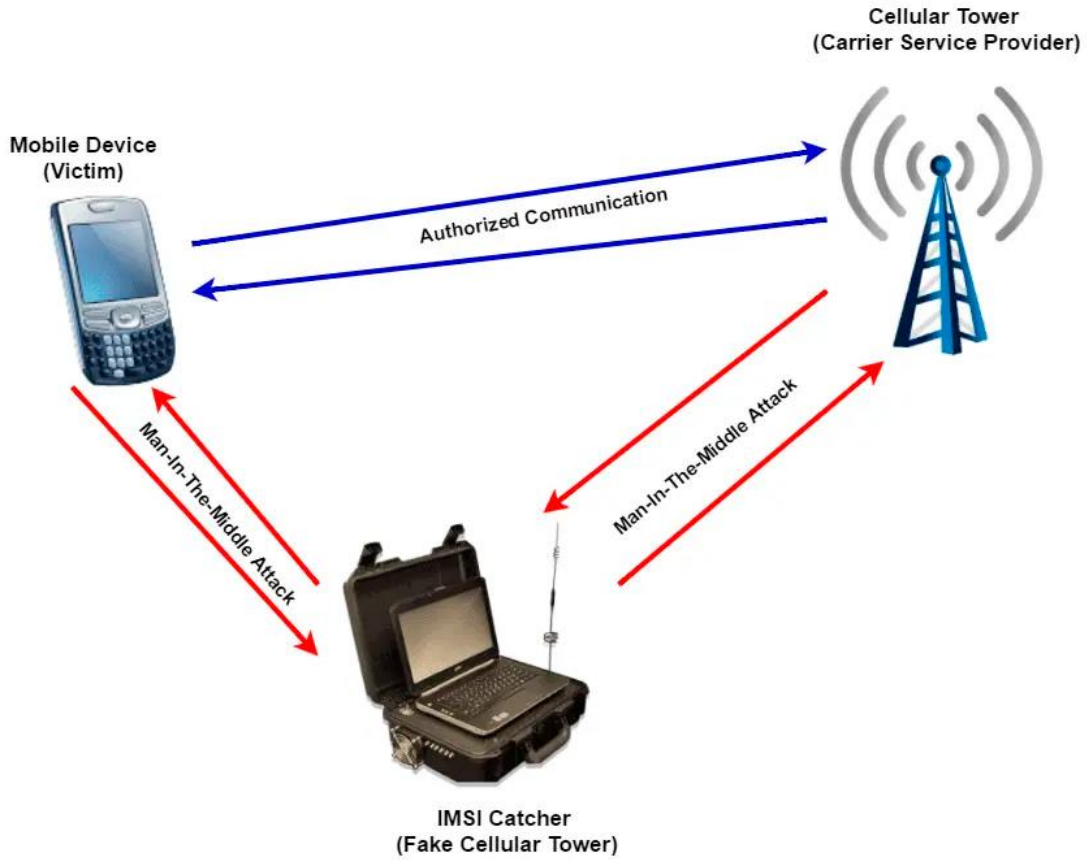
[6] ITIC (2020), “Policy Principles for Cybersecurity Certification”, septiembre de 2020, https://www.itic.org/policy/ITI_PolicyPrinciplesforCybersecurityCertification_Final.pdf.

[7] El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) publicó en agosto de 2020 la guía “Zero Trust Architecture”, orientada a corporaciones y Administraciones Públicas, de obligado cumplimiento para la Administración Federal de Estados Unidos: https://csrc.nist.gov/publications/detail/sp/800-207/final.

comunicaciones realizadas mediante el uso de equipos llamados *IMSI catchers* (con este fin, 3GPP ha estandarizado el uso del cifrado, tal como se explica más adelante). En consecuencia, las fuerzas de seguridad y judiciales perderían la capacidad de realizar, amparadas por el marco legal, la identificación, seguimiento e interceptación de comunicaciones 5G a personas investigadas en el campo mediante estos equipos.

Un *IMSI catcher* es un dispositivo que se interpone entre el terminal del usuario y la antena de la estación base de telefonía emulando una estación base mediante la captación del identificador IMSI de la comunicación, el cual permite identificar un determinado terminal móvil, el operador al que está suscrito y el usuario al que pertenece (es un ataque de tipo *man-in-the-middle*, como el de la Figura 1). Los operadores asignan un identificador denominado International Mobile Subscriber Identity (IMSI) en las redes 4G o Subscription Permanent Identifier (SUPI) en las 5G, que integran en la tarjeta SIM de cada dispositivo. El identificador IMSI se forma con el identificador del país (MCC), de la red móvil (MNC) y de la estación móvil (MSIN)[8].

Figura 1. Funcionamiento de un interceptor de comunicaciones móviles



Fuente: Noa Ozuiel, FirstPoint[9].

[8] Distinto del código IMEI (Mobile Station Equipment Identity) del terminal, código pregrabado en los terminales móviles que identifica el aparato de forma exclusiva a nivel mundial y es transmitido por este al conectarse a la red. De este modo, el operador conoce quién y desde dónde se hace la llamada (tarjeta SIM) y también el terminal telefónico utilizado; el IMEI permite verificar el estado del aparato mediante una base de datos denominada EIR (Equipment Identity Register) y bloquearlo en caso de robo.

[9] Noa Ozuiel (2020), "Top 7 IMSI catcher detection solutions ", FirstPoint, 31/01/2020, https://www.firstpoint-mg.com/blog/top-7-imsi-catcher-detection-solutions-2020.

El *IMSI catcher* lo utilizan habitualmente las autoridades policiales y judiciales en el curso de investigaciones y para la prevención de delitos. Permite identificar y realizar el seguimiento de terminales móviles que se encuentren en su área de cobertura e interceptar los contenidos de la comunicación (llamadas de voz, mensajes SMS, datos), los metadatos asociados a la comunicación (geolocalización, duración, número llamado, etc.) y la configuración del terminal (potencia de transmisión, claves de cifrado, etc.), lo que conlleva que toda comunicación que no esté cifrada es susceptible de ser analizada.

El crimen organizado y las organizaciones terroristas también emplean estos equipos para la comisión de chantajes, espionaje industrial, extorsión o la preparación de actos terroristas, entre otros. Asimismo, se dan otros usos que atentan contra la privacidad de los ciudadanos, tales como recoger información (metadatos) masiva e indiscriminada de asistentes a eventos sociales, promocionales, deportivos, etc., o enviar mensajes SMS directamente a los teléfonos situados en su radio de cobertura, habitualmente con fines publicitarios, razón por la que algunos movimientos por los derechos civiles han solicitado a los organismos de estandarización un mayor nivel de protección técnica de la privacidad frente al uso ilegal de estos dispositivos.

El organismo de estandarización 3GPP ha introducido en la versión 16, mencionada anteriormente, una nueva función opcional que cifra[10] el código IMSI, valor que se vuelve a cifrar cada vez que la red lo lee del terminal para evitar su rastreo y la asociación por deducción del terminal asignado. La nueva función de cifrado requiere su activación desde la red del operador y que la SIM del terminal 5G incorpore la función de cifrado. El terminal podría emular esta función para proteger el código IMSI, aunque previsiblemente surjan incompatibilidades o deficiencias en la implementación. Añadido a lo anterior, el 5G incorpora una función que permite al operador y al terminal del usuario detectar y notificar estaciones base falsas (*IMSI catchers*). Las dificultades para el uso de los *IMSI catchers* en redes 5G con cifrado obligarían a las fuerzas de seguridad y judiciales a solicitar la información a los operadores de red, proceso estático y en ocasiones inapropiado para llevar a cabo determinadas investigaciones en el campo.

La interceptación legal en las redes 5G. Nuevos retos para las autoridades policiales y judiciales

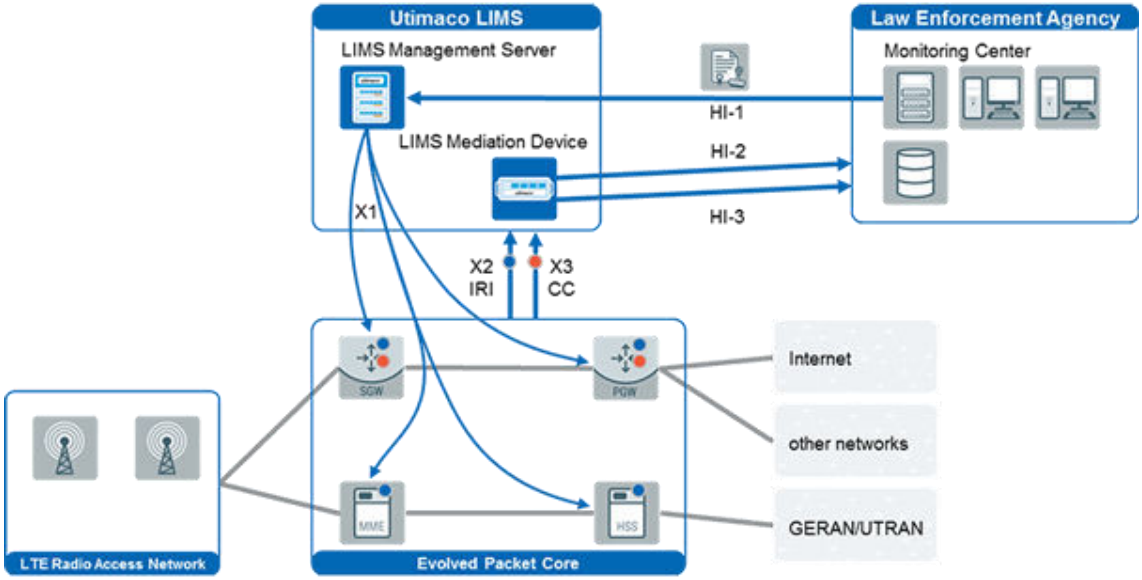
La interceptación legal de las comunicaciones electrónicas es un requisito altamente regulado que han de cumplir los operadores de red en colaboración con los cuerpos de seguridad y judiciales, a quienes deben entregar en tiempo real una réplica exacta de las comunicaciones de los usuarios investigados (contenido y metadatos), previa solicitud mediante mandato judicial.

Para llevar a cabo las interceptaciones, el operador entrega las comunicaciones a los centros de monitorización y supervisión de las agencias de seguridad mediante una plataforma centralizada de interceptación, la cual accede a las comunicaciones objeto de la interceptación capturadas en el núcleo de la red (enrutadores y sistemas de control) por las interfaces normalizadas internas de la red (X1, X2, X3). La plataforma

[10] El código IMSI se cifra mediante un esquema de clave pública (almacenada en la SIM) y privada utilizando criptografía de tipo ECC (*elliptic curve cryptography*).

de interceptación del operador se comunica con los centros de monitorización de las agencias de seguridad mediante interfaces de transferencia normalizadas (HI-1, HI-2, HI-3).

Figura 2. Arquitectura de la interceptación legal 5G



Fuente: Ultimaco, https://lims.utimaco.com/solutions/lawful-interception-management-solution/for-mobile-network-operators/.

Los organismos 3GPP y ETSI han estandarizado los protocolos de comunicación e interfaz entre la plataforma del operador y el sistema de monitorización de las autoridades, en particular los requisitos generales de las plataformas, mecanismos de intercambio de datos y medidas relativas a la seguridad y privacidad. La adaptación al 5G de los sistemas de interceptación de los operadores y de monitorización de los cuerpos de seguridad con el fin mantener las actuales capacidades de interceptación plantea notables desafíos tecnológicos, entre ellos:

- Mantener las funciones de interceptación de los servicios tradicionales de voz y datos de las actuales redes 2-4G al tiempo que adaptar sus capacidades y protocolos a la interceptación de las redes 5G contemplando los distintos escenarios de funcionamiento cruzado entre servicios 4G y 5G. En particular, los sistemas habrán de poder interceptar a un usuario que transite entre estaciones base y nodos de tecnologías de acceso legadas 2-4G y 5G sin que se produzcan interrupciones en la captura del tráfico y metadatos. Los sistemas habrán de interoperar con estas redes a través de distintas interfaces armonizadas. La migración al 5G de usuarios y tecnologías inalámbricas de acceso legadas (acceso radio, núcleo de red y terminales) será progresiva y durará al menos una década (Ericsson prevé que el 36% de sus ingresos provenga de suscripciones 5G en 2025[11]).

[11] Ericsson (2020), "Ericsson Mobility Report", junio de 2020, https://www.ericsson.com/49e7b3/assets/local/mobility-report/documents/2020/emr-june2020-spanish.pdf.

- Operar en los distintos escenarios de provisión de los servicios de telefonía 5G en el curso de las sucesivas fases de despliegue del operador y asegurar la integridad de la comunicación interceptada con independencia de las tecnologías por las que transite la llamada[12].

- Ampliar las capacidades de los equipos de interceptación para la recepción, procesamiento y entrega de tráfico interceptado debido al significativo incremento en las velocidades de conexión, volúmenes previstos de tráfico (tres veces mayores de promedio para 2025) y número de conexiones interceptadas en tiempo real, calculadas en decenas de gigabits por segundo (gbps) por agencia de seguridad atendida.

- Adaptar los sistemas del operador y de monitorización de las agencias de seguridad a las nuevas interfaces y estándares de la arquitectura 5G[13].

- Adaptar los sistemas del operador para la interceptación de nodos de red virtualizados (NFV y SDN) y, en particular, la de subredes virtualizadas (*network slices*), en ocasiones gestionadas por corporaciones y operadores virtuales clientes del operador de la red 5G[14].

En abril de 2019, Europol presentó al Consejo Europeo un documento en el que exponía su preocupación en relación con las dificultades a las que se enfrentan en determinados casos los cuerpos de seguridad y judiciales para llevar a cabo las interceptaciones legales, en particular para la identificación y localización de usuarios y para cursar la solicitud, acceso y disponibilidad de la información en redes 5G[15]. En mayo de 2019, el coordinador de la Unión Europea para la lucha contra el terrorismo, Gilles de Kerchove, reafirmó las dificultades operativas anticipadas por Europol y reclamó con urgencia una mayor coordinación y anticipación entre las autoridades policiales y judiciales, los

[12] El despliegue de la red 5G se ha iniciado con el acceso radio 5G sobre el núcleo de la red LTE/4G (5G Non Stand Alone). A continuación se desplegará el núcleo de red 5G (5G Stand Alone), ofreciendo inicialmente a clientes 5G servicios de telefonía compatible con LTE/4G, cuya migración a telefonía VoNR/Vo5G coincidirá con la madurez del despliegue 5G, aunque manteniendo la compatibilidad con VoLTE/4G. Los operadores de 5G ofrecerán servicios de telefonía basados en tres tecnologías: VoNR/Vo5G, LTE Fallback y CS Fallback.

[13] El núcleo de la red 5G (5G Packet Core) utiliza nuevos protocolos de red, identificadores de usuario, interfaces para la interceptación del traspaso entre celdas RAN (interfaz HI del LI) e interfaces con el suministrador de sistemas de interceptación (interfaz X del LI), especificadas en el estándar 3GPP versión 16 (33.126, 33.127 y 33.128).

[14] Las capacidades y configuraciones de los nodos 5G virtualizados se adaptan dinámicamente a las necesidades establecidas por los servicios y clientes, lo que aumenta la complejidad para interceptar y monitorizar un determinado tráfico, sumado a la dificultad de identificar el emplazamiento o la titularidad de un determinado segmento (*slice*) de la red 5G.

[15] Consejo Europeo (2020), “Position paper on 5G by Europol”, 11/04/2020, https://www.statewatch.org/media/documents/news/2019/jun/eu-council-europol-position-paper-5g-8268-19.pdf.

organismos de estandarización, los suministradores y los desarrollos normativos europeos y nacionales[16].

En relación con la identificación y localización de usuarios conectados a redes 5G y a consecuencia del cifrado –anteriormente mencionado– del código IMSI de los terminales, las autoridades no podrían por sí mismas localizar e identificar mediante dispositivos *IMSI catchers* dispositivos móviles objeto de seguimiento e interceptación ni por consiguiente asociarlos a una determinada persona, Tal como se ha señalado, los *IMSI catchers* son herramientas tácticas indispensables para el seguimiento, monitorización y obtención de metadatos (localización, marca de tiempo, duración de la llamada, número llamado, etc.), en particular de usuarios que cambian con frecuencia de tarjeta SIM en el curso de una investigación, al estar el código IMSI vinculado al identificador del terminal.

Las redes 5G plantearán dificultades adicionales para la solicitud, acceso y obtención de información sobre los metadatos y comunicaciones de los sujetos interceptados. Primero, la segmentación de la red (*network slicing*)[17] dificultará significativamente la accesibilidad a las comunicaciones debido a la fragmentación de la información en distintas redes virtualizadas, por lo que los operadores de la infraestructura 5G podrían no tener acceso a las comunicaciones y datos de los segmentos (*slices*) asignados a clientes privados emplazados en países extranjeros, salvo que la legislación nacional obligue a ello expresamente. Esta casuística no se ha contemplado en la Directiva e-Evidence para la obtención y conservación de pruebas electrónicas en el curso de investigaciones llevadas a cabo entre países de la UE. En segundo lugar, la descentralización del procesamiento y almacenamiento de información en el borde de la red de acceso radio 5G (*multi-access edge computing*, MEC) ofrecerá a los desarrolladores de aplicaciones y proveedores de servicios un entorno en la nube (*cloud*) descentralizado y emplazado en el borde de la red de acceso móvil que comunicará directamente dispositivos próximos sin necesidad de que sus comunicaciones transiten hasta el núcleo de la red con el fin de conseguir valores óptimos de latencia, disponibilidad y seguridad. En estos casos, las comunicaciones e identificadores de usuario no estarán directamente disponibles en los nodos del núcleo de la red, punto de recolección de la plataforma de interceptación para su entrega a las agencias de seguridad. Finalmente, el uso de cifrado entre los extremos de las comunicaciones 5G es una opción que el estándar 3GPP-R16 ofrece a los operadores de red, función que también puede implementarse voluntariamente en el terminal del usuario. En ambos casos, impediría o, al menos, dificultaría significativamente el acceso al contenido de las comunicaciones en investigaciones policiales y judiciales.

[16] "5G will make it harder for law enforcement and judicial authorities to carry out lawful interception. Due to 5G's high security standards and a fragmented and virtualised architecture, law enforcement and judicial authorities may lose access to valuable data". Gilles de Kerchowe (2019), "Law enforcement and judicial aspects related to 5G", p. 3, 06/05/2019, https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

[17] GSMA (2017), "An introduction to network slicing", https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf.

Más allá de estas dificultades para la identificación y localización de usuarios, Europol expone diversos riesgos operativos vinculados a la virtualización de las infraestructuras físicas de la red y la posible transferencia de listas de números o personas monitorizadas a terceros países o empresas debido a la externalización de la gestión de la red. La sustitución de los actuales nodos de red implementados mediante equipamiento *hardware* emplazados y protegidos en las dependencias del operador con elevadas medidas de seguridad física y lógica por nodos y funciones de red virtualizadas puede facilitar el acceso no autorizado y la alteración de las listas de usuarios objeto de interceptación.

Ambos informes apuntan que esta situación es consecuencia de que los estándares 5G elaborados bajo el paraguas de 3GPP respondan principalmente a motivaciones comerciales y de innovación de la industria. La dinámica de los organismos internacionales de normalización, en los que el derecho de voto está vinculado a la contribución económica de las organizaciones, no permite ejercer el derecho al veto o votaciones por unanimidad. Añadido a lo anterior, la participación de las agencias de seguridad en el subgrupo técnico 3GPP dedicado a temas de interceptación legal (SA3-LI) es reducida. En consecuencia, los estándares técnicos no garantizan el adecuado equilibrio entre ciberseguridad, protección de los derechos civiles y capacidades para la interceptación legal.

Para contrarrestar esta situación, Europol y el coordinador de la UE para la lucha contra el terrorismo resaltan la necesidad de que los Estados miembros establezcan legislación específica que obligue a los operadores de telecomunicaciones al cumplimiento de obligaciones no contempladas en los estándares sobre 5G en el campo de la interceptación legal; es claramente preferible que estos organismos incorporen estos requisitos a los estándares. Asimismo, señalan la conveniencia de establecer un marco legislativo europeo que permita una mayor efectividad y adecuación a la interceptación de comunicaciones 5G entre Estados miembros, evite la fragmentación de estándares y facilite la implantación de legislación común para la obtención de pruebas electrónicas (Directiva e-Evidence). En su documento proponen el registro obligatorio de la totalidad de los proveedores en un territorio dado; la obligación de todos los proveedores de ofrecer un duplicado no cifrado, exacto y completo de las comunicaciones interceptadas; estructurar la arquitectura de red de modo que siempre esté disponible la información sobre la localización del usuario, y ofrecer medidas técnicas que permitan el uso de *IMSI catchers*. Hay que destacar cierto continuismo con el que ambos informes analizan las capacidades de interceptación en las futuras redes 5G sin plantearse, por ejemplo, el nuevo paradigma que implica la interceptación de objetos conectados en el contexto industrial (IIoT) y en el ámbito personal (domótica, asistentes virtuales, etc.).

Conclusiones

El gran potencial de innovación que aporta la tecnología 5G en la digitalización de la sociedad ha sido posible gracias a una vertiginosa evolución tecnológica materializada a partir de la evolución de las redes 4G, fruto del acuerdo entre los distintos agentes de la industria de las telecomunicaciones en los organismos de estandarización.

La complejidad y enormes posibilidades que ofrecen las nuevas arquitecturas virtualizadas 5G, entre otros avances significativos, no deberían restar relevancia a asegurar un adecuado equilibrio desde el inicio del proceso de estandarización de los distintos factores en torno a la seguridad, que se interrelacionan en su conjunto como un todo: ciberseguridad, privacidad, interceptación de las comunicaciones.

La corrección de carencias y desequilibrios en las fases iniciales de diseño y estandarización, junto con las medidas regulatorias establecidas *ex ante* por las autoridades regulatorias nacionales que recaen sobre los operadores de telecomunicaciones, evitaría posteriormente enormes sobrecostes económicos y de oportunidad al conjunto de la industria.