INTRODUCCIÓN A LAS TECNOLOGÍAS 5G Y SUS RIESGOS PARA LA PRIVACIDAD

v. mayo de 2020

RESUMEN EJECUTIVO

El uso de la telefonía móvil está presente en prácticamente todas las actividades sociales. Desde la tercera generación de telefonía, los dispositivos móviles han crecido exponencialmente en funcionalidades, pero también las amenazas a la privacidad de los individuos que los usan. En estos momentos se está produciendo el salto tecnológico de la cuarta a la quinta generación de telefonía móvil, más conocida por su acrónimo 5G.

En esta nota técnica se hace un repaso a la evolución de la tecnología móvil desde su implantación, se exponen las nuevas funcionalidades de la tecnología 5G (aumento de la precisión de la geolocalización, virtualización, tratamiento distribuido, …) así como la identificación de sus riesgos. También se proponen una serie de recomendaciones y conclusiones para todos los actores implicados, con el objeto de que el 5G no suponga una amenaza a los derechos y libertades de las personas físicas.

Finalmente, se propone realizar una reflexión sobre la necesidad de adaptar la normativa sobre recogida y conservación de datos de tráfico al cambiar la proporcionalidad de los datos recogidos.

Palabras clave: 5G, Edge Computing, IA, IoT, Móvil, Privacidad, Protección de datos, RGPD, Riesgo, Tecnología, Telefonía, Virtualización, Slice.

ÍNDICE

I. INTRODUCCIÓN

La quinta generación de comunicaciones móviles (5G) empezó a desplegarse en Europa a principios de 2019 y se prevé que tenga un gran impacto en la sociedad digital.

Las principales mejoras que 5G ofrecerá a los usuarios son:

- Alta velocidad de transferencia (*enhanced mobile broadband o eMBB*)
- Mayor capacidad de conexión (*massive machine communications o mMTC*)
- Baja latencia[1] en las comunicaciones (*ultra-realiable and low latency communications o URLLC*)

Estas características permitirán la puesta en marcha de productos y servicios en los que se requiera alta velocidad, como aplicaciones multimedia o de realidad aumentada, así como el despegue definitivo del internet de las cosas (*IoT*), por la posibilidad de tener simultáneamente conectados un volumen ingente de dispositivos. Por otro lado, va a permitir hacer realidad las aplicaciones que requieran respuestas en tiempo real, como las típicas de la industria conectada o la cirugía remota asistida, y posibilitando la expansión de servicios basados en decisiones automatizas, muchas veces usando inteligencia artificial.

Para realizar el despliegue de las redes 5G se está planificando una renovación tecnológica sin precedentes en la historia reciente de la tecnología móvil. La arquitectura de red y las funciones de red van a experimentar grandes cambios con la introducción de tecnologías como la virtualización[2] (*software-defined networking* y virtualización de funciones de red), *edge computing*[3] y *network slicing*[4].

II. OBJETIVO Y DESTINATARIOS

El objetivo de este documento es ofrecer una panorámica de las novedades que presenta la tecnología 5G de comunicaciones móviles y realizar un primer estudio no exhaustivo de los riesgos para la privacidad que puede llevar implícita tanto esta tecnología, como otras tecnologías que hagan uso de ella.

Está especialmente dirigido a todos aquellos agentes que, desde un cierto desconocimiento del 5G, tienen inquietudes sobre las implicaciones para la privacidad que puede suponer su implantación generalizada.

También está dirigida a fabricantes, proveedores, operadores de servicios, empresas de telecomunicaciones y desarrolladores de aplicaciones que establezcan modelos de negocio en 5G, que quieran profundizar en las implicaciones para la privacidad de los productos y servicios que desarrollan como, por ejemplo, los desarrolladores de cualquier servicio OTT[5].

III. EVOLUCIÓN DE LA TELEFONÍA MÓVIL

A partir de 1980, en cada década ha habido un avance significativo en telefonía móvil, que se ha descrito en forma de generaciones. En cada generación aparecen nuevas funcionalidades que han contribuido a la popularización de los dispositivos móviles, pero a su vez a la aparición de nuevas amenazas a la privacidad de las personas:

[1] Latencia es el tiempo de respuesta entre acción y reacción. En comunicaciones es el tiempo que transcurre desde se inicia el envío de un mensaje y llega el primer bit a destino. La velocidad de transmisión es el tiempo que transcurre desde que llega el primer bit hasta que llega el último. Son valores independientes. Una baja latencia permite aplicaciones en tiempo real.

[2] Tecnología que permite ejecutar diferentes sistemas operativos independientes dentro de un mismo equipo anfitrión.

[3] Tecnología que permite tener los sistemas que realizan tratamientos y los datos más cerca físicamente del usuario, para así minimizar los retardos producidos durante la transmisión de la información en largas distancias.

[4] Tecnología que permite utilizar una misma infraestructura física de red para multiplexar redes virtuales en una misma infraestructura de red física

[5] Servicios de difusión y comunicaciones que utilizan los servicios de los operadores de comunicaciones (Over The Top)

- 1G: a principios de la década de 1980 aparecen los primeros teléfonos móviles analógicos con unas capacidades muy reducidas pudiendo únicamente realizar llamadas. En ese momento se primaba la funcionalidad, sin tener en cuenta la protección de datos, pues, si bien su uso era testimonial, las comunicaciones entre las personas eran menos privadas de lo que los usuarios podían pensar.
- 2G: en 1991 la segunda generación, ya de telefonía digital, aporta la funcionalidad de envío de mensajes de texto a través de terminales de usuarios, como los conocidos SMS. En esta generación se introducen, por ejemplo, técnicas de cifrado en las comunicaciones que mejoran la confidencialidad, aunque siguen quedando muchos flecos sin resolver en la dimensión de autenticidad. Los usuarios sufren los primeros ataques de SPAM y la interceptación de las comunicaciones a través de estaciones base falsas.
- 3G: para el año 2000 aparecen los primeros dispositivos 3G con funcionalidades multimedia, acceso a Internet y televisión. Estos teléfonos también trajeron las primeras vulnerabilidades por código malicioso, de localización por GPS, y otras.
- 4G: en 2010 se empezó a desplegar la telefonía 4G, que permitía acceso de alta velocidad a internet, y se implementaron técnicas de cifrado más robustas. Al ser una red fundamentada en la tecnología IP todas las amenazas tradicionales presentes en las redes LAN e Internet se trasladaron al mundo de la telefonía: APTs[6], DDoS[7], virus, etc. y con ellas también los riesgos asociados para la privacidad. La utilización masiva los móviles supuso un aumento en la escala de las amenazas.
- 5G: es la tecnología de esta década y para la que ya se están comercializando los primeros terminales y servicios.

IV. PRINCIPALES NOVEDADES EN 5G

La quinta generación (5G) de telefonía móvil supone un cambio sustancial con relación a las generaciones anteriores. Por primera vez, deja de utilizarse hardware específico de telefonía para dar paso a equipos de propósito general, que no difieren de los que podemos encontrar en cualquier centro de procesamiento de datos TIC, haciendo uso de tecnologías de virtualización, contenedores y orquestación. Esto representa una ventaja a nivel de costes y flexibilidad de implementación, y por otro lado hace que la infraestructura sea interoperable y accesible por equipos en Internet.

Hay tres características que permiten hablar de 5G como una tecnología disruptiva, y de cambio de paradigma en la concepción de las redes de comunicaciones móviles: virtualización, *edge computing*, y localización; además de cambios importantes en las estrategias de seguridad.

Antes de describirlas, y para poder entender mejor todos los conceptos empleados, es preciso conocer las dos partes diferenciadas de la arquitectura de una red de telefonía móvil:

- Red de Acceso o *Access Network*: Es la parte de la red que conecta a usuarios finales (dispositivos móviles) con la red central del operador. Es la parte de la infraestructura que posibilita la conexión aérea, por radio, entre los dispositivos móviles y la red del operador.
- Red Core o *Core Network*: Es la parte central de la red de un operador de telecomunicaciones. La que gestiona todas las funcionalidades y servicios del operador o, dicho de otro modo, contiene las funciones de red.

[6] Amenaza persistente avanzada es conjunto de procesos informáticos ocultos con la intención y la capacidad de atacar de forma avanzada y continuada en el tiempo, un objetivo determinado.
[7] Ataques distribuidos de denegación de servicio.

Con 5G llegan novedades a ambas partes de la red, pero las más disruptivas aplican a la *red core*. En la figura 1 se incluye un diagrama con la arquitectura básica de una red 5G.

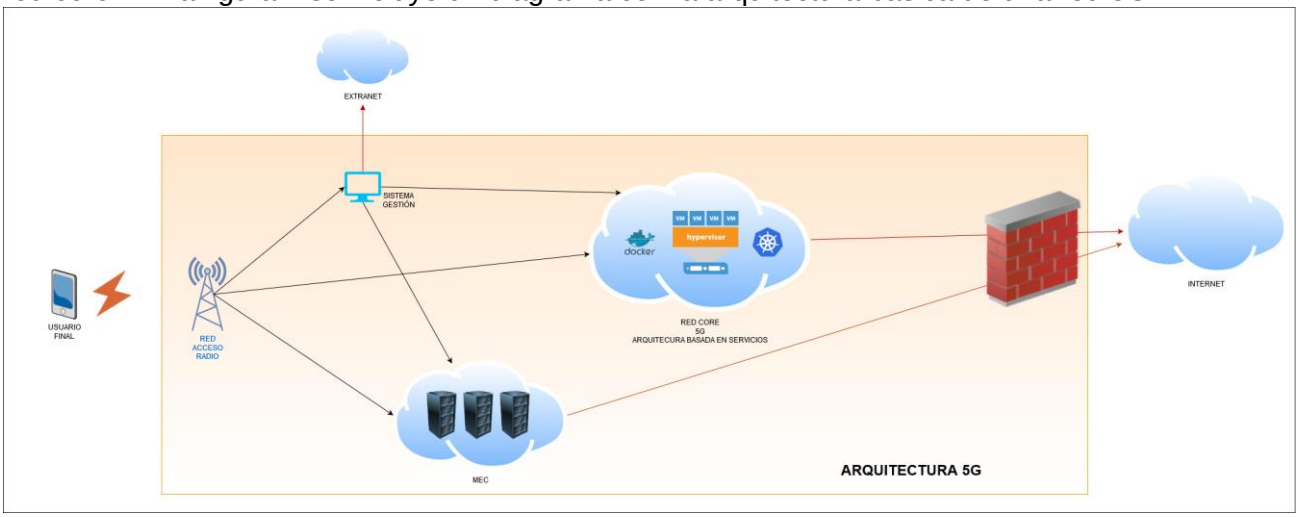

Figura 1. Arquitectura básica de red 5G.

A. VIRTUALIZACIÓN

Sin duda, la mayor revolución y lo que puede tener un impacto más importante en la privacidad es la utilización de tecnologías de virtualización, que comprende nuevos conceptos como:

- *Software Defined Networking* (SDN): las actuales redes de telefonía son muy estáticas, y cualquier cambio implica modificaciones de hardware, con costosos procesos manuales. El SDN facilita a los operadores realizar cambios en la red de forma rápida y en algunas circunstancias también de forma automática, adaptándose a las necesidades de demanda en la red.
- *Network Function Virtualization* (NFV): supone una forma novedosa de crear, desplegar y gestionar servicios de red virtualizando todas y cada una de las funciones que proporciona la red.
- *Network Slicing* (NS): implica mejorar y adaptar el soporte a diferentes tipos de tráfico en las redes 5G, mediante la virtualización de un conjunto de funciones de red que forman parte de la *red core*. Conceptualmente sería equivalente a decir que cada *red core* puede estar formada por un conjunto de *slices* o *redes core virtuales*.

La virtualización es ya una tecnología madura en el ambiente TIC, pero el 5G supone su debut en el entorno de las comunicaciones móviles, trasladando con ello sus ventajas e inconvenientes.

La *red core*, estará dividida en lo que se conocen como *network slices*. *Network slicing* permite establecer redes lógicas, con funciones de red propias, sobre una única infraestructura física de telecomunicaciones, con parámetros configurados específicamente para dar respuesta a distintos requisitos de cada aplicación. Las funciones de red vienen a ser un conjunto de componentes virtuales parametrizables y dinámicamente creables, cada una con una función específica, que se diseñan sin estado y separando funciones de computación de funciones de almacenamiento de datos. Cada *slice* está formada por un conjunto de funciones de red definido en el estándar 5G.

La conexión de los dispositivos será gestionada por los propios fabricantes de dispositivos o proveedores de servicio a través de una SIM integrada (eSIM) y conectada a una *slice* de

red también bajo su control. De esta forma, el usuario ya no tendrá que gestionar la conexión con un operador, ni que introducir una SIM en el dispositivo.

La especificación de 5G define tres *network slices* estándar, cada una de ellas definida para proporcionar uno de los requisitos funcionales de 5G (uLRLLC[8], eMBB[9], mMTC[10]), pero no establece una limitación en el número de *slices* que se pueden establecer. Las *network slices* funcionan como redes virtuales independientes formadas por un conjunto completo de funciones de red, pero no están totalmente aisladas entre sí porque hay una función de red que puede ser compartida entre varias *slices*.

Así, la *red core* de cada operador estará formada por varias *slices*, cada *slice* está formada por un conjunto de funciones de red, y las *redes core* de los diferentes operadores estarán conectadas entre sí a través de una función de red específica que realizará funciones de proxy.

La única función de red que puede ser compartida entre varias *slices* de una misma *red core,* según el estándar 5G, es la *Access and Mobility Management Function* (AMF). Se trata de una función clave ya que gestiona el registro, acceso y movilidad de los dispositivos de usuario, servicios de geolocalización y la posible interceptación legal de las comunicaciones por las fuerzas del orden.

La red de acceso es conocedora de las *slices* disponibles y los requerimientos en cuanto a capacidades de acceso que tiene que dar a cada dispositivo de usuario, gestionando a qué *slice* debe conectarse. Si los requerimientos de un dispositivo son muy exigentes, y el dispositivo está preparado para ello, un mismo dispositivo podría conectarse a varias *slices*.

Por ejemplo, un teléfono móvil se conectará a través de la red de acceso a la *slice* correspondiente a telefonía de propósito general, mientras que una señal de tráfico inteligente podría ser conectada a una *slice* diferente, destinada específicamente a la gestión de tráfico en una ciudad. Ambos dispositivos compartirían *red de acceso*, pero acaban recibiendo servicio desde diferentes *slices.*

Esta arquitectura basada en virtualización y *slices* posibilita la implementación de modelos de gestión que permiten ofrecer *slices* como servicios (NSaaS). Es decir, un operador podría ofrecer comercialmente la gestión de un *slice* a un tercero, como podría ser el caso de operadores virtuales, pero no limitado a este caso concreto.

A su vez la tecnología *network slice* podría permitir sustituir a las redes dedicadas tradicionales, así podríamos ver *slices* con diferentes prioridades y calidades según los SLA[11] contratados. Por ejemplo, se podrían establecer *slices* para dar servicio a emergencias, señalización de tráfico, eventos deportivos, defensa nacional, etc., y también *slices* gestionadas por el propio ayuntamiento, una administración responsable del servicio, y organizaciones privadas.

Este modelo de gestión de *slices* unido a las características de baja latencia y conectividad masiva que proporciona 5G, previsiblemente facilitará el desarrollo definitivo del binomio IoT e Inteligencia Artificial, con un aumento exponencial del número de dispositivos conectados a la red 5G a través de las *slices* que necesiten para satisfacer sus requerimientos de operación.

[8] Baja latencia en las comunicaciones.
[9] Gran incremento en el ancho de banda.
[10] Conectividad masiva de dispositivos.
[11] SLA: acuerdos de nivel de servicio.

B. EDGE COMPUTING

La computación en la nube, o *cloud computing*, se basa en el uso de grandes centros de proceso de datos en localizaciones repartidas por la geografía mundial, destinadas a almacenar y procesar cantidades ingentes de datos. El modelo de servicio en los dispositivos móviles, tal y como la conocemos hoy en día, utiliza aplicaciones móviles (Apps) que intercambian datos con servidores de Internet sin que el usuario tenga que gestionar, al menos a priori, su ubicación física. Aunque esta arquitectura es útil en muchos casos, hay situaciones en las que no se puede aplicar por tener una latencia muy alta, o impredecible, y lo que no permite aplicaciones en tiempo real.

El uso de hardware de propósito general para contener servicios virtualizados del operador, o de otros proveedores de servicios, permite la implementación de uno de los elementos más novedosos de 5G, como son los denominados MEC (*Multi-Access Edge Computing*). La tecnología *edge computing* permitirá desplazar el "centro de gravedad" del tratamiento de datos desde los servidores hacia ubicaciones más cercanas al dispositivo terminal del usuario, cuando sea necesario. En definitiva, podrá existir un flujo de información y/o servicios entre diferentes ubicaciones acordadas por operadores de la red y gestores de servicios, en puntos cercanos al usuario final y dentro de la red de telefonía móvil de un operador de telecomunicaciones, en principio sin estar en Internet.

Al realizar las tareas de computación lo más cerca posible del usuario final, 5G permitirá una reducción en la latencia de las comunicaciones tal que permitirá contar con capacidades próximas al tiempo real, que son indispensable en escenarios como, por ejemplo:

- Vehículos autónomos
- Automatización industrial
- Realidad aumentada
- Hogares y oficinas conectadas
- Videojuegos
- Cirugía remota asistida

C. LOCALIZACIÓN

En el despliegue de 5G está previsto el uso de frecuencias de transmisión más altas (en la banda de los 26GHz) de las que se utilizan actualmente en las redes de telefonía móvil anteriores, lo que permitirá alcanzar transmisiones mucho más veloces. Sin embargo, el alcance de la señal será más reducido en campo abierto y muy sensible ante obstáculos como paredes y muros en interior.

La forma de superar los inconvenientes será la instalación de una red más densa de puntos de acceso en exteriores y un despliegue de puntos de acceso de telefonía móvil sin precedentes en interiores de edificios, especialmente en grandes superficies públicas de elevada concurrencia.

En definitiva, se necesita una *red de acceso* mucho más compacta, con muchos puntos de acceso y menor distancia entre ellos. Esta mayor densidad proporcionará al operador y a otros agentes vinculados a la explotación de los datos de la red, la capacidad de localizar el terminal de usuario con una precisión mucho mayor de la que tiene en la actualidad, alcanzando resoluciones de localización inferiores a un metro y, al contrario que las generaciones previas a 5G, incluyendo posicionamiento en tres dimensiones. Por ello, es de esperar el desarrollo de servicios novedosos basados en localización (LBS).

D. SEGURIDAD

Desde el punto de vista de la seguridad, la especificación de la tecnología 5G incorpora importantes mejoras en las medidas de seguridad respecto a las generaciones anteriores, tanto en la red de acceso como en la *red core*.

Algunas de ellas son:

- Una nueva estructura de identificadores de usuario permanentes y, además, cifrados para evitar que pueda transmitirse en claro vía radio como ocurría en determinadas circunstancias con las generaciones anteriores a 5G.
- Mejoras en los mecanismos de **autenticación** con la introducción de 5G-AKA[12], cuyas principales mejoras son que la red del operador con la que se contrata el servicio (*red home*) es quien autentica tanto al terminal de usuario como a la red donde el móvil pretende conectarse (*red de servicio*), la *red de servicio* no tiene claves para descifrar las comunicaciones hasta que no ha sido autenticada por la *red home*, además cuenta con diferentes mecanismos de control de fraude.
- Datos de usuario protegidos en **integridad** en la interfaz de radio, adicional a la protección en confidencialidad que ya se proporciona en 4G.
- Posibilitar el acceso desde redes no 3GPP[13] creando un túnel cifrado mediante una clave proporcionada por el operador.
- **Cifrado** TLS de las comunicaciones entre funciones de red dentro de la *red core*.
- Incorporación de opciones de **trazabilidad** que facilitan el registro de las operaciones para auditar la seguridad de la red.

Las capacidades de virtualización, la implementación de una arquitectura basada en servicios (*Service Based Architecture* SBA) y a la separación del plano de usuario del de control (*Control and User Plane Separation* CUPS) permitirían que las redes 5G puedan desplegarse respetando el principio de seguridad por defecto.

Estas mejoras a nivel de seguridad suponen un gran avance tanto en la confiabilidad de las comunicaciones aéreas de la *red de acceso* (dispositivo de usuario-antena) como dentro de la *red core.* Sin embargo, la especificación deja la implementación de alguno de estos mecanismos a criterio del operador, por lo que el incremento de seguridad en las redes 5G puede ser muy diferente entre distintos operadores de telefonía en función del despliegue de la tecnología, afectando las decisiones de un solo actor a la seguridad global de las comunicaciones de redes 5G.

Además, potencialmente se podrían producir circunstancias en que la seguridad se vea degradada por acceder al servicio a través de una red con deficiencias de implementación en situaciones de itinerancia. La necesidad de mantener la compatibilidad con protocolos de generaciones previas a 5G hace que las vulnerabilidades presentes en los mismos se extiendan en el tiempo.

V. RIESGOS PARA LA PRIVACIDAD

5G se espera que sea el gran canal de comunicaciones de esta década. Todos los datos de redes públicas o privadas podrían acabar utilizando las infraestructuras de comunicaciones de 5G, y ligando esto al incremento de dispositivos conectados hace pensar que en la práctica todas las personas serán usuarios de esta red y todos los dispositivos estarán conectados.

[12] *Authentication and Key Agreement*

[13] 3GPP: *3rd Generation Partnership* Project Asociación de grupos de telecomunicaciones que participa en la estandarización de las redes móviles desde el 3G

De forma no exhaustiva y conforme a lo expuesto anteriormente, se pueden identificar al menos los siguientes riesgos para la privacidad de los datos. Muchos de estos riesgos están interrelacionados entre sí y no son nuevos, sino que estaban presentes con las anteriores generaciones de telefonía móvil, pero pueden verse exponencialmente incrementados si la implantación de 5G alcanza las expectativas de éxito previstas.

- Geolocalización precisa del usuario: El hecho de que 5G emplee muchas más estaciones base y menos distancia entre ellas, hace que la localización geográfica basada en la red sea mucho más precisa.
- Perfilado y decisiones automatizadas: el incremento en cantidad y en categorías de datos circulando por la red, multiplicado por la cantidad de dispositivos que cada ciudadano tendrá conectado mediante 5G (IoT), va a permitir llegar a una individualización precisa de las personas y el desarrollo de servicios que permitan la toma de decisiones automáticas sobre las personas (IA y servicios en tiempo real).
- Reparto de responsabilidad entre fabricantes, operadores de red y proveedores de servicios: se prevé un aumento sustancial en el número de agentes que pueden participar en el tratamiento de datos personales con el despliegue de redes 5G y con la explosión de nuevos servicios. Esto podría llevar a problemas de ambigüedad en cuanto a la responsabilidad por el tratamiento de los datos, es decir que la responsabilidad de cada una de las partes quede diluida.
- Diferentes objetivos de privacidad e intereses entre las partes implicadas: vinculado a lo anterior, los agentes que intervendrán en las redes de telefonía tendrán diferentes intereses de privacidad, comerciales, seguridad nacional, etc., con fabricantes, operadores de telecomunicaciones, y proveedores de servicios sometidos a diferentes regulaciones, entre estas las obligaciones de proporcionar acceso legal a las comunicaciones a fuerzas y cuerpos de seguridad de los diferentes estados.
- Falta de un modelo homogéneo de seguridad: al permitir el 5G la existencia de numerosos agentes en la cadena de comunicaciones, incluso dentro de la *red core* de los operadores, a través de servicios desplegados por diversos proveedores de servicio dentro de los MEC. Cada agente puede cumplir con distintos estándares de seguridad y podrá incluir segmentos que correspondan a protocolos de las primeras generaciones, por lo que la seguridad global será equivalente a la del elemento más débil.
- Aumento exponencial de la superficie de exposición a ciberataques: el incremento de servicios, conectividad, interoperabilidad y puntos de entrada y gestión a la red incrementaran las oportunidades de que se materialicen amenazas a la privacidad.
- Herencia de los problemas de privacidad derivados de infraestructuras estándar interoperables: al implementarse el 5G con equipos de propósito general, una infraestructura que antes estaba tecnológicamente diferenciada será permeable a los mismos ataques que sufren las tecnologías de la información convencionales.
- Vulnerabilidades derivadas de los entornos virtuales y funciones compartidas: en el mismo sentido que el apartado anterior, se heredaran los problemas de privacidad de las tecnologías de virtualización, así como el riesgo de filtrado de datos entre funciones compartidas entre distintos slices, como la citada *Access and Mobility Management Function* (AMF).
- Dinamismo en las funciones de gestión de las comunicaciones: si en las generaciones previas las funciones de gestión de red estaban, de facto, cableadas, la posibilidad de actualización de esta mediante software introduce problemas de estabilidad, trazabilidad de versiones, actualizaciones por diversos intervinientes, puertas traseras, malware de fábrica y hacking.

- Posible pérdida de control del usuario: esto puede producirse sobre los flujos de datos, con posibles implicaciones transfronterizas, así como en el ejercicio de derechos. El 5G usa un modelo de procesamiento distribuido y dinámico, donde está previsto que los datos y procesamientos se muevan en tiempo real a la ubicación física en el que sean más necesarios o sea más eficaz su procesamiento.

A pesar de tratarse de una lista de riesgos no exhaustiva, éstos deberán tomarse en consideración desde las primeras fases de diseño de los tratamientos para la implementación de medidas técnicas y organizativas que los mitiguen integrándose en la naturaleza de los productos y servicios que utilicen o se apoyen en la tecnología 5G con el fin de dar cumplimiento a lo exigido en el artículo 25 del RGPD. También se deberán realizar los esfuerzos necesarios para la identificación y mitigación de nuevos riesgos a través de procesos de gestión de riesgos y evaluaciones de impacto de protección de datos pertinentes tanto en los proveedores de servicios, operadores y, sobre todo, en los fabricantes.

VI. CONCLUSIONES Y RECOMENDACIONES

Cuando la tecnología 5G alcance un grado de madurez adecuado, se darán las condiciones necesarias para que la terna 5G-IoT-IA proporcione servicios novedosos y disruptivos. Esta situación probablemente tenga un impacto alto e impredecible sobre la privacidad de las personas.

Las decisiones de los operadores en la implementación de la red, la gestión de la configuración y su operativa tendrán un impacto definitivo en el nivel de privacidad alcanzado, por lo que se les insta a que definan las infraestructuras de 5G bajo el marco de la privacidad desde el diseño y por defecto. Los desarrolladores y fabricantes de equipos de la tecnología base de red para 5G tendrán el deber de suministrar productos con un adecuado nivel de cumplimiento del RGPD que facilite el despliegue de redes. A su vez, el resto de los agentes que presten servicio dentro de esas redes de comunicaciones, creando y gestionando nuevos productos y servicios, tendrán también un nivel de responsabilidad en la implementación de medidas y garantías.

Será necesario que todos los intervinientes en la implementación, gestión y explotación de la red 5G tengan en cuenta las siguientes recomendaciones:

- En las nuevas aplicaciones y servicios basados en el 5G la información que se debe proporcionar a los interesados según establece la normativa de protección de datos ha de ser particularmente clara y comprensible, especialmente, sobre los responsables de los tratamientos, las finalidades, la adopción de decisiones automatizadas y la elaboración de perfiles, así como sobre el acceso y uso de las medidas de control por parte de los usuarios. Esta última de forma destacada.
- A su vez, implementar mecanismos de trasparencia y trazabilidad tanto en los casos de conexión de los dispositivos al servicio 5G como en los casos en que se realice tratamiento distribuido.
- Definir cuidadosamente los roles y los correspondientes ámbitos de responsabilidad (desde el punto de vista de protección de datos) y delimitar claramente las obligaciones de desarrolladores, fabricantes, operadores y agentes. La delimitación de responsabilidades de los agentes intervinientes debe responder a las decisiones que efectivamente tomen sobre los medios y fines del tratamiento, para evitar desplazamientos de responsabilidades por la vía contractual.
- Implementar medidas de control de los propios usuarios sobre los datos personales, tanto sobre aquellos recogidos de los usuarios como aquellos

inferidos sobre su actividad o la actividad de otros dispositivos conectados a la red en el marco del IoT.

- Implantar medidas de minimización de datos, en particular, con relación a la georreferenciación, teniendo en cuenta el principio de privacidad por defecto desde la fase inicial del diseño de productos que utilicen servicios 5G.
- Establecer medidas que garanticen la compartimentación de los datos que eviten el filtrado de información entre procesos en los casos de tratamiento distribuido y en la compartición de funciones de red.
- La aplicación de criterios homogéneos de seguridad en los distintos agentes y segmentos de red que estén basados en un análisis de riesgos para los derechos y libertades, como estable el RGPD. El análisis de riesgos ha de estar orientado a gestionar amenazas en la red 5G como un todo y no solo en la operación singular de cada agente.
- Garantizar comunicaciones cifradas extremo a extremo y, además, desarrollar modelos de cifrado que protejan el proceso y transmisión de información en el modelo de *edge computing* (como es el cifrado homomórfico, técnicas de *network coding* u otras).
- Adecuar el uso de decisiones automatizadas a lo establecido en el RGPD.
- Establecer las necesarias garantías en el caso de transferencias internacionales de datos.
- La auditoría independiente de infraestructuras y servicios, incluida la adhesión a mecanismos de certificación en protección de datos a los que se refiere el RGPD.
- Recoger las lecciones aprendidas en el mundo de Internet y no importar directamente modelos que han demostrado ser vulnerables.

Previsiblemente surgirán modelos de infraestructura, casos de uso y nuevos servicios que implicarán tratamientos de datos personales que podrían enmarcarse entre aquellos a los que el RGPD requieren una evaluación de impacto relativa a la protección de datos (EIPD). Incluso, si el riesgo residual sigue siendo elevado, exigirán una consulta previa a la autoridad de control al inicio de las actividades de tratamiento en virtud de los listados elaborados por las autoridades de control para dar cumplimiento al artículo 35.4 del RGPD.

Este nuevo escenario de diversidad de servicios y productos supone una ventana de oportunidad para el desarrollo de esquemas de certificación previstos en el RGPD. Los esquemas de certificación son de gran utilidad para la implementación y demostración del cumplimiento de medidas de responsabilidad proactiva en los tratamientos de datos personales. El establecimiento de un marco de confianza en la seguridad de los tratamientos de datos en 5G es un factor imprescindible para garantizar su éxito.

Finalmente, es necesario realizar una reflexión sobre las normativas y estándares relativos al tratamiento y conservación de datos de tráficos por los operadores de telecomunicación, en particular, con relación a la georreferenciación. Por ejemplo, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, es aprobada cuando la resolución estándar de georreferenciación de las redes 1G a 3G exigía a los operadores localizar a los usuarios con una precisión de entre 100 y 300 en el plano. Actualmente, en el 2020, las redes 4G exigen una precisión de 50 metros, pero con 5G se alcanzarán resoluciones inferiores a 1 metro en tres dimensiones. La amenaza a la privacidad que suponía en el año 2007 la conservación de información de geolocalización no es comparable a la que puede suponer un escenario en el que se han desplegado redes 5G. Por lo tanto, es necesario adaptar la normativa para establecer garantías adecuadas al tratamiento de la nueva información de tráfico y, sobre todo, en relación con su conservación.

VII. REFERENCIAS

5G Americas TM, "The Evolution of Security in 5G"

Delegados de Protección de Datos y equipos de Ericsson España, Huawei España, Movistar, Orange España y Vodafone España, información facilitada en reuniones mantenidas en AEPD.

European 5G Observatory, 5G Observatory Quarterly Reports

European Commission, EU coordinated risk assessment of the cybersecurity of 5G networks

Federal Communications Commission, 5G Edge Computing Whitepaper

Federal Communications Commission, 5G Network Slicing Whitepaper

R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," in IEEE Communications Surveys & Tutorials.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne and M. Ylianttila, "5G Privacy: Scenarios and Solutions," 2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, 2018, pp. 197-203.

Manuel Lorenzo, Ericsson España, charla en t3chfest - The Convergence of 5G, AI and IoT

José Picó J., Pérez D., CCN-CERT, Plataforma Vanesa, Seguridad en los protocolos de comunicaciones 5G

Privacy International - "Welcome to 5G: Privacy and security in a hyperconnected world (or not?)"

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales