PRIVACIDAD EN DNS

Noviembre 2019

RESUMEN EJECUTIVO

El acceso a Internet, tanto desde smartphones como equipos de escritorio, utiliza servicios para facilitar el acceso a los sitios web de una forma que resulte trasparente y cómoda al usuario. Dichos servicios, conocidos como protocolo DNS, implican el tratamiento de datos por terceros distintos de aquellos que proporcionan los servicios a los que queremos acceder. Este tratamiento podría desvelar hábitos de navegación e información de geolocalización, permite generar perfiles y ser conservados de forma indefinida y existe un riesgo serio para la privacidad de los usuarios.

A pesar del aumento de la concienciación sobre la privacidad en Internet, el protocolo DNS es probablemente el gran olvidado. Esta nota identifica los problemas de privacidad que puede generar el uso del protocolo DNS y las implicaciones que podría tener el tratamiento ilegítimo de esos datos. A su vez, identifica las garantías que se pueden implementar para gestionar estos riesgos tanto para los usuarios como para los proveedores de servicios en entornos domésticos y profesionales.

Palabras clave: Privacidad, Internet, Confidencialidad, Integridad, Autenticidad, Cifrado, Dominios, RGPD, LOPDGDD, AEPD, UEET, DNS, TLS, HTTPS, DNSSEC, Innovación.

ÍNDICE

I. INTRODUCCIÓN

Para permitir que los usuarios introduzcan en los navegadores los nombres de los servicios a los que quiere acceder, en vez de un código numérico para identificar a los servidores en Internet, fue desarrollado el Sistema de Resolución de Nombres o DNS por sus siglas en inglés: Domain Name System.

Cuando navegamos por Internet nuestros equipos realizan consultas constantes a través del protocolo DNS a distintas máquinas en la red para determinar la dirección IP a la que acceder. De esta forma en lugar de tener que recordar un número de hasta doce dígitos, se posibilita que escribiendo un nombre comercial o fácil de recordar podamos acceder por ejemplo a la página web del periódico cada mañana. Estas consultas se realizan de forma transparente al usuario, accediendo a determinados servidores, llamados servidores DNS, que se configuran en la red.

Una consulta DNS contiene una dirección IP que identifica al usuario y puede geolocalizar a quien está navegando por Internet, y también contiene el nombre de la página a la que se desea navegar. Esto permite hacer asignaciones de hábitos de navegación a identificadores únicos, perfilar a un usuario al proporcionar las consultas. Por ejemplo, se podría perfilar a una persona según su corriente de opinión política en función de los sitios online que visita para mantenerse informado. Otro ejemplo podría ser deducir problemas de salud en función de los tipos de foros, blog o webs en los que participa.

En la gran mayoría de casos las consultas a través de la red no se encuentran protegidas mediante, por ejemplo, cifrado. Además, a la hora de procesar la solicitud algunos servidores DNS pueden estar configurados para guardar un registro de estas consultas y utilizar esos datos, no sólo de forma legítima para garantizar la seguridad de los servicios[1], sino para otras finalidades distintas al mero funcionamiento del sistema DNS, además de ser una información sensible que podría filtrarse a terceros.

Un problema añadido en el caso de que no se adopten las garantías necesarias, es que tampoco se puede asegurar el origen de las respuestas ni que la respuesta no haya sido modificada por un tercero, por lo que el empleo de técnicas de suplantación de DNS[2] nos pueden hacer navegar a webs que no son las que realmente queremos visitar, con los consiguientes riesgos para la privacidad: robo de información, ransomware, etc.

Esta nota se enfoca en el uso transversal[3] del protocolo DNS en las comunicaciones poniendo énfasis en la falta de medidas de seguridad del protocolo DNS que pueden

[1] El Considerando 49 del RGPD establece: Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

[2] Ataques al DNS: cómo intentan dirigirte a páginas falsas

[3] Transversal en el sentido que todos los servicios en Internet se acceden haciendo uso del protocolo DNS

originar problemas en la privacidad, las mejoras que se ha ido adoptando y las implicaciones que pueden tener el tratamiento ilegítimo de esos datos.

DNS ha evolucionado dando respuesta a la necesidad de seguridad en las comunicaciones, así la (todavía lenta) implementación de DNSSEC está aportando las dimensiones de integridad y autenticidad. En este momento existen dos propuestas para posibilitar la confidencialidad a través del cifrado de las consultas: DNS Over TLS y DNS Over HTTPS. Estas nuevas medidas de seguridad ayudan a mejorar el nivel de privacidad, pero, como se verá a lo largo del presente estudio, no la garantizan.

II. OBJETIVO Y DESTINATARIOS

Al ser DNS un protocolo transversal en los servicios de Internet, las consideraciones en la privacidad deben ser tenidas en cuenta por un gran número de implicados desde desarrolladores de software, administradores de red, los propios prestadores de servicios DNS, y proveedores de acceso a Internet.

El propósito de esta nota técnica es analizar la evolución del protocolo de resolución de nombres DNS desde el punto de vista de las implicaciones en la privacidad de las personas, la forma en la que se utiliza en la actualidad, los riesgos que se presentan, los esfuerzos que se están realizando para mitigar estos riesgos y las implicaciones que estos cambios podrían tener sobre la privacidad de los usuarios en Internet. Así mismo, se incluyen recomendaciones a tener en cuenta en la selección de servicios DNS.

Esta nota técnica se encuadra dentro del plan estratégico de la Agencia, que promueve la concienciación ciudadana sobre los derechos y garantías que les asisten en materia de protección de datos con especial atención a la protección de los ciudadanos con respecto a las actividades que se desarrollan en Internet y pretende ser un impulso a iniciativas que por parte de la industria de la economía digital supongan beneficios en la privacidad de las personas en el uso de Internet.

III. IMPLICACIONES EN LA PRIVACIDAD DEL PROTOCOLO DNS

EL PROTOCOLO DNS Y LOS RIESGOS ASOCIADOS

Las bases del protocolo de resolución de nombres o DNS se establecen inicialmente en 1983 por el IEFT[4], siendo actualizado en 1987, especificando la forma en que se resolverán las direcciones IP de los equipos de Internet en nombres, así como un sistema jerárquico distribuido de nombres de dominio en las que el propietario del dominio, ya sea en sus propios servidores DNS o los que designe, establecerá la relación entre nombres del dominio y direcciones IP. Estos son los conocidos como servidores DNS autoritativos, que serán los que se comuniquen con los servidores DNS consultados por los equipos cliente (PCs, teléfonos móviles…), denominados DNS resolvers.

Posteriormente, para proporcionar medidas de seguridad en el protocolo DNS, se incorporaron las llamadas extensiones de seguridad o DNSSEC que hacen uso de criptografía de clave pública, de manera que se puede garantizar la integridad de la respuesta DNS y su autenticidad. Sin embargo, DNSSEC no facilita mecanismos de cifrado que permita la confidencialidad de las comunicaciones DNS. La realidad es que el uso de DNSSEC no se ha extendido tanto como se pretendía y su empleo en Internet es muy desigual.

[4] Internet Engineering Task Force

Por otro lado, la configuración estándar en las redes de área local utiliza el protocolo DHCP para facilitar a los clientes, a nivel de sistema operativo, información como la dirección IP, puerta de enlace, nombre del dominio de la red y los servidores DNS que consultará el dispositivo. De esta manera, será la red a la que nos conectemos quien fijará los servidores DNS que van a ser consultados, es decir, en redes domésticas normalmente será el operador quien defina el DNS a utilizar, mientras que en redes de trabajo los administradores decidirán si se utiliza un servidor DNS propio, del operador de comunicaciones o cualquier otro DNS público.

Al navegar por Internet desde un dispositivo a diferentes páginas web, lo primero que necesita saber el dispositivo es la dirección IP que corresponde al nombre de la página que hemos escrito en el navegador. Estas consultas se envían (y reenvían) sin cifrar (fig.1) a través de los distintos elementos de la red y son procesadas por los servidores DNS[5]. Este mecanismo es particularmente vulnerable en wifis abiertas o redes de invitados y resulta en dos riesgos de confidencialidad diferenciados.

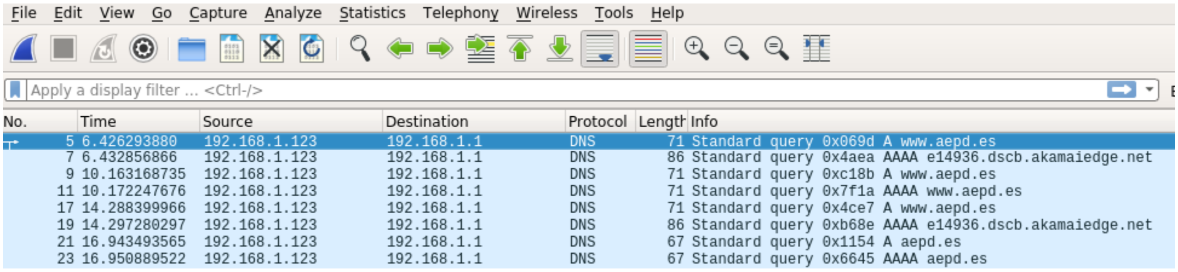


Figura 1. Tráfico de red en consulta DNS.

Por un lado, las consultas DNS pueden ser interceptadas en la red y de esta forma pueden ser leídas y procesadas por un tercero. Por otro lado, los servidores DNS pueden registrar información de las consultas (Figura 2) de cada dispositivo cuando el usuario navega por Internet o usa otros servicios de la red.

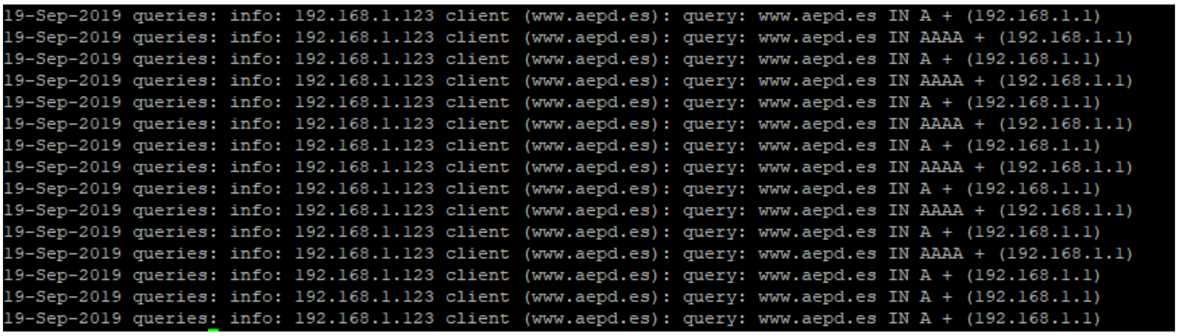


Figura 2. Registro de un servidor DNS.

DNS OVER TLS Y DNS OVER HTTPS

Para proporcionar confidencialidad en las consultas DNS se han desarrollado diferentes alternativas, entre las que cabe destacar recientemente DNS over TLS (DoT) y DNS over HTTPS (DoH). Ambas soluciones están pensadas para mitigar el riesgo de que

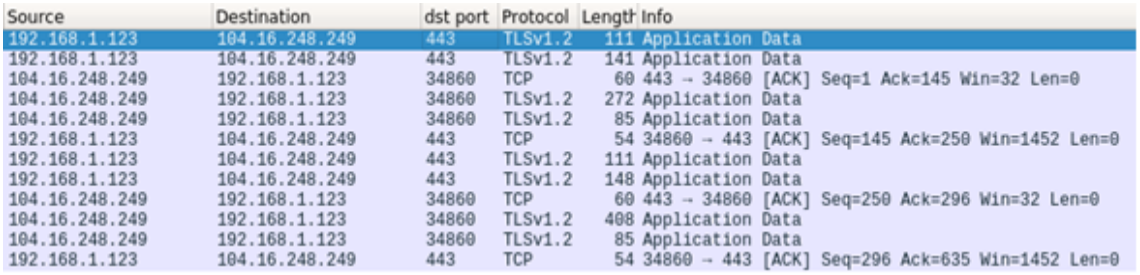
[5] Los establecidos como se ha explicado en el párrafo anterior

las consultas DNS puedan ser interceptadas, y en el caso de que lo sean que la información resulte ilegible, contribuyendo a mejorar la confidencialidad.

Recientemente se ha definido en fase de borrador el protocolo DNS over HTTPS o DoH. De esta forma, se pueden aprovechar funcionalidades presentes en HTTP, como pueda ser compresión, redirección, y cifrado de las consultas DNS a través de TLS. Éste último, TLS, es el protocolo empleado actualmente para cifrar las comunicaciones HTTPS de los navegadores, de esta forma, las consultas DNS pasan a ser consultas HTTPS entre cliente y servidor. En principio, esto supondría una mejora significativa en la privacidad de las comunicaciones, ya que de esta manera se evita que terceros puedan conocer las consultas DNS que realice cualquier dispositivo.

Un tercero que analice el tráfico de red que genera un navegador con DoH activado (Figura 3), solo identificará comunicaciones HTTPS estándar realizadas por el puerto 443 TCP. Las consultas DoH quedarán enmascaradas entre el resto de las comunicaciones con una web segura.

Para poder usar DoH debemos tener acceso a servidores DNS que acepten las consultas basadas en dicho protocolo. En la definición de DoH se establece que se podrá seleccionar de forma manual los servidores DoH (de forma simplificada como si fuera la dirección de una página web) o se podrá seguir facilitando a través de DHCP o protocolos similares.



Source	Destination	dst port	Protocol	Length	Info
192.168.1.123	104.16.248.249	443	TLSv1.2	111	Application Data
192.168.1.123	104.16.248.249	443	TLSv1.2	141	Application Data
104.16.248.249	192.168.1.123	34860	TCP	60	443 → 34860 [ACK] Seq=1 Ack=145 Win=32 Len=0
104.16.248.249	192.168.1.123	34860	TLSv1.2	272	Application Data
104.16.248.249	192.168.1.123	34860	TLSv1.2	85	Application Data
192.168.1.123	104.16.248.249	443	TCP	54	34860 → 443 [ACK] Seq=145 Ack=250 Win=1452 Len=0
192.168.1.123	104.16.248.249	443	TLSv1.2	111	Application Data
192.168.1.123	104.16.248.249	443	TLSv1.2	148	Application Data
104.16.248.249	192.168.1.123	34860	TCP	60	443 → 34860 [ACK] Seq=250 Ack=296 Win=32 Len=0
104.16.248.249	192.168.1.123	34860	TLSv1.2	408	Application Data
104.16.248.249	192.168.1.123	34860	TLSv1.2	85	Application Data
192.168.1.123	104.16.248.249	443	TCP	54	34860 → 443 [ACK] Seq=296 Ack=635 Win=1452 Len=0

Figura 3. Tráfico red consulta DNS over HTTPS

Algunos navegadores web han apostado por el uso de DoH. Por ejemplo, Firefox, permite habilitarlo en las opciones del navegador (Figura 4) y tiene previsto que se pueda establecerse como configuración por defecto. Sin embargo, al tratarse de una configuración establecida en el navegador, únicamente tendrá efecto sobre las peticiones DNS realizadas por el propio navegador, no afectando a otros navegadores o aplicaciones del del dispositivo que accedan a Internet.

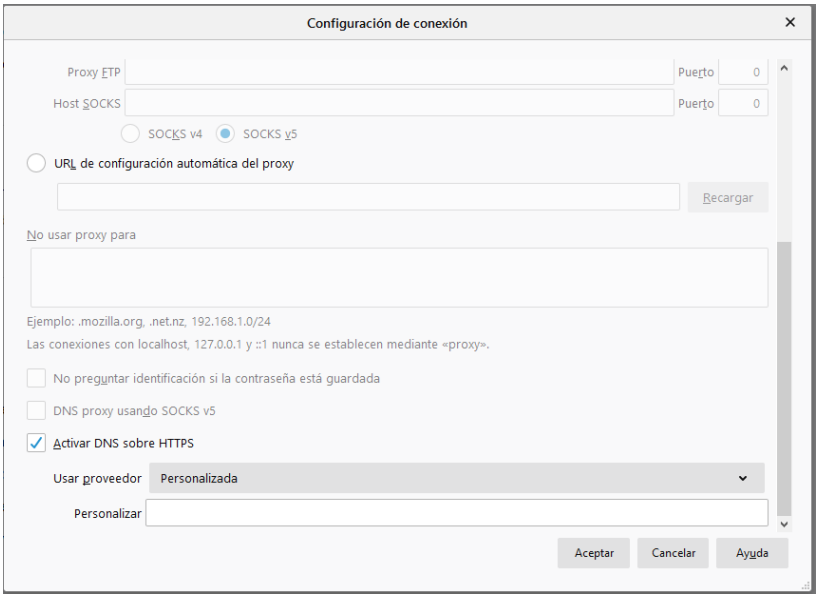


Figura 4. Configuración DoH en Firefox.

Aunque Firefox permite configurar el servidor DoH libremente, al activar esta opción se establece por defecto (Figura 5) el servidor predeterminado de Cloudflare, el cual almacena las consultas realizadas durante 24 horas, como informa en su web.

Figura 5. Proveedor DoH predeterminado en Firefox

Para evitar problemas de conectividad, en caso de que Firefox no pueda resolver las direcciones a través de DoH, detecte un sistema de control parental o configuraciones DNS empresariales, realizará una consulta no cifrada a los servidores DNS establecidos a nivel de sistema operativo una consulta Multicast DNS (Figura 6).

Source	Destination	Info
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question

Figura 6. Consulta Multicast DNS.

Por su parte Google tiene previsto incorporar DoH para la versión 78 de su navegador Chrome, que como indican, de forma experimental incorporará la posibilidad de elegir los siguientes proveedores de servicio DoH: Cleanbrowsing, Cloudflare, DNS.SB, Google, OpenDNS, Quad9.

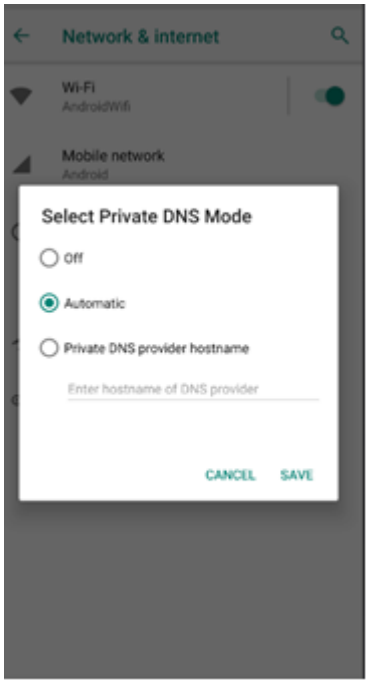


Figura 7. Selección de DNS privado en Android.

DNS over TLS, o DoT, es otra alternativa que implementa sobre el protocolo DNS las capacidades de cifrado que aporta TLS, de tal manera que una consulta DNS estándar es cifrada con TLS y enviada a un servidor configurado para contestar DoT. A nivel de red, el servidor DoT debe estar escuchando por el puerto 853 TCP donde el cliente realizará las peticiones. BIND es el servidor DNS más extendido en la actualidad, y permite configurarlo como servidor DoT de manera sencilla.

En cuanto a los dispositivos móviles, desde Android 9 es posible de forma nativa fijar los servidores DNS que utilizará el Smartphone independientemente de la red en la que esté conectada. De momento los sistemas de Microsoft y Apple no cuentan con esta opción sin recurrir a software de terceros.

IV. CONCLUSIONES

Desde hace más de 35 años el protocolo DNS ha sido uno de los pilares del uso de Internet y de las redes de datos en general, facilitando el acceso a sitios web sin tener que recordar una dirección numérica como es la dirección IP.

A pesar del aumento de la preocupación y concienciación por la privacidad en Internet, el protocolo DNS es probablemente el gran olvidado. Sin embargo, como hemos visto, la información recopilada a través de este servicio puede tener un impacto significativo sobre la privacidad de las personas porque, a través de las consultas que se han realizado al servidor DNS, es posible conocer en detalle los hábitos de navegación y perfilar al dueño de un dispositivo.

Como la mayoría de los protocolos de Internet, DNS se definió sin tener en cuenta la seguridad, desarrollándose posteriormente medidas para asegurar la integridad y autenticidad de la respuesta como DNSSEC y más recientemente medidas para asegurar la confidencialidad como DoT y DoH.

La incorporación de estas soluciones puede suponer un gran avance para la privacidad de las comunicaciones especialmente en redes no confiables, pero no están exentas de algunas limitaciones que deberán superarse cuando la tecnología esté madura y su implementación sea más amplia:

- Actualmente solo los navegadores web implementan DoH, por lo que el resto de las consultas que realizan las aplicaciones de los equipos y el propio S.O. siguen realizándose sin cifrar la comunicación. DoT todavía no está implementado de forma nativa en la mayoría de los dispositivos.
- La implementación de DoH en modo fallback en el navegador supone que, en algunos casos, las peticiones seguirán realizándose a través del protocolo DNS

tradicional, con la incertidumbre de desconocer qué petición se ha realizado cifrada y cual no.

- Aunque los usuarios podrán establecer fácilmente servidores DoH a través de la configuración de su navegador, que a priori es una ventaja para su privacidad, esta opción debe ser cuidadosamente analizada, ya que puede dar lugar a elegir un proveedor que tenga los servidores en países fuera del EEE y/o que utilice los registros de consultas para finalidades distintas a la de proporcionar exclusivamente el servicio DNS dando lugar a posibles actividades de tratamiento sujetas al RGPD. Esta última consideración no es exclusiva de DoH y DoT, sino que también se puede extender al DNS original.
- Al permitir realizar consultas a otros servidores DNS diferentes a los ya definidos por el sistema operativo y tunelizadas a través de HTTPS, DoH va a facilitar al malware el poder eludir mecanismos de detección.
- DOH puede dar una falsa sensación de seguridad, puesto que se puede llegar a identificar el uso de consultas DNS a través de HTTPS con diferentes técnicas como TLS fingerprinting, identificar el destino si corresponde a un servidor DoH o analizando el tráfico no cifrado de HTTPS

Como recomendaciones a la industria y al resto de agentes implicados, cada uno en su área de actuación correspondiente, se proponen las siguientes líneas de actuación:

- Impulsar y facilitar una mayor implantación de DNSSEC, activándolo en todos los DNS, tanto resolvers como autoritativos.
- Impulsar y facilitar el uso generalizado de consultas DNS cifradas con alguno de los métodos mencionados a nivel de sistema operativo sin necesidad de recurrir a software de terceros.
- Los proveedores de servicios DNS deben informar de las condiciones de uso del servicio, incluyendo la base legal aplicable en caso de almacenar y/o procesar los datos de las consultas, así como el resto de información relativa a unas posibles actividades de tratamiento sujetas al RGPD.
- En el caso de las compañías de acceso a Internet que faciliten a sus clientes el acceso a servidores DNS de terceros, deben asegurarse de seleccionar proveedores que se ajusten a las exigencias del RGPD, eligiendo aquellos servicios DNS que ofrezcan garantías suficientes que hagan que los posibles tratamientos de datos garanticen los derechos de los interesados.

Por último, cabe recordar que los datos tratados por el servidor DNS son recogidos para un tratamiento específico, dar el servicio de resolución de nombres de dominio, y que cualquier otro tipo de tratamiento adicional, en particular la comunicación de dichos datos para otras finalidades como el perfilado de los usuarios, supone serias implicaciones para la privacidad. En tal caso, se estaría produciendo un tratamiento de datos personales del que debe identificarse su base jurídica, se debe informar al usuario, se debe garantizar el ejercicio de los derechos del usuario y se debe garantizar el cumplimiento del RGPD en toda su extensión. De no ser así, se estaría ante un tratamiento ilegítimo de esos datos personales.

V. BIBLIOGRAFÍA

[1] Liu, C. and Albitz, P. (2009). *DNS and BIND*. O'Reilly Media, Inc.

[2] Deckelmann, S. (2019). *What's next in making Encrypted DNS-over-HTTPS the Default – Future Releases*. [online] Future Releases. Available at: https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/

[3] McManus, P. (2019). *Improving DNS Privacy in Firefox – Firefox Nightly News*. [online] Firefox Nightly News. Available at: https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

[4] Chromium Blog. (2019). *Experimenting with same-provider DNS-over-HTTPS upgrade*. [online] Available at: https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html

[5] Bradbury, D. (2019). *Mozilla increases browser privacy with encrypted DNS*. [online] Naked Security. Available at: https://nakedsecurity.sophos.com/2019/09/10/mozilla-increases-browser-privacy-with-encrypted-dns/

[6] Hunter, M. (2019). *Encrypted DNS Could Help Close the Biggest Privacy Gap on the Internet. Why Are Some Groups Fighting Against It?*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2019/09/encrypted-dns-could-help-close-biggest-privacy-gap-Internet-why-are-some-groups

[7] GitHub. (2019). *folbricht/routedns*. [online] Available at: https://github.com/folbricht/routedns

[8] ag, u. (2019). *ungleich blog - Mozilla's new DNS resolution is dangerous*. [online] Ungleich.ch. Available at: https://ungleich.ch/en-us/cms/blog/2018/08/04/mozillas-new-dns-resolution-is-dangerous/

[9] Dnscrypt.info. (2019). *Home page of the DNSCrypt project [DNS security]*. [online] Available at: https://dnscrypt.info/protocol/

[10] Tools.ietf.org. (2019). *RFC 7858 - Specification for DNS over Transport Layer Security (TLS)*. [online] Available at: https://tools.ietf.org/html/rfc7858

[11] Tools.ietf.org. (2019). *RFC 8484 - DNS Queries over HTTPS (DoH)*. [online] Available at: https://tools.ietf.org/html/rfc8484

[12] Simplednscrypt.org. (2019). *Simple DNSCrypt*. [online] Available at: https://simplednscrypt.org/

[13] Hashed Out by The SSL Store™. (2019). *What is the difference between DNS over TLS & DNS over HTTPS?*. [online] Available at: https://www.thesslstore.com/blog/dns-over-tls-vs-dns-over-https/

[14] Kb.isc.org. (2019). *DNS over TLS - BIND 9*. [online] Available at: https://kb.isc.org/docs/aa-01386

[15] Android Developers. (2019). *Distribution dashboard | Android Developers*. [online] Available at: https://developer.android.com/about/dashboards

[16] Sans.org. (2019). *SANS Institute: Reading Room - DNS Issues*. [online] Available at: https://www.sans.org/reading-room/whitepapers/dns/needle-haystack-detecting-dns-https-usage-39160