lacigf Preparatory meeting for the Internet Governance Forum

Miércoles 1 de agosto 15:00 hs.
Sesión 7 "Desafíos en la Gestión de Identificadores de Internet"

Bajo la premisa "Privacidad bajo el enfoque de GDPR y su impacto en el DNS" presentada por Rodrigo de la Parra, Vicepresidente para América Latina y el Caribe de ICANN, se reunió un nutrido grupo de participantes para dialogar sobre la temática.

Rodrigo presentó los antecedentes de GDPR, tema que ha ocupado la agenda de ICANN, y que trata sobre las medidas de protección y privacidad de datos de ciudadanos y residentes de la Unión Europea (GDPR)

Este tema se ha vuelto relevante para la comunidad técnica y en esta oportunidad, se le ha dado un enfoque más amplio y no tan técnico para que sea de mayor interés para la comunidad en general. Se formularon unas preguntas para el trabajo en el grupo hoy que no solo se enfocan en cuestiones técnicas sino en las implicancias que tiene este tema para la gobernanza de internet.

Antecedentes

El GDPR entró en vigencia el 25 de mayo pasado y tiene como objetivo proteger a los ciudadanos y residentes de la UE de violaciones a la privacidad y mal uso de datos personales. "El reglamento es un paso esencial para fortalecer los derechos fundamentales de los ciudadanos en la era digital y facilitar negocios simplificando las normas para las empresas en el mercado único digital."

El mismo se aplica a todas las empresas que procesan y mantienen los datos personales de los sujetos que residen en la UE, independientemente de su ubicación geográfica.

Frente al incumplimiento se puede dar lugar a multas de hasta 20 millones de euros o el 4% de la facturación anual global. Las autoridades europeas de protección de datos interpretarán los acontecimientos que ocurran y harán cumplir la regulación y los tribunales europeos resolverán cualquier disputa.

Menciona que no es muy diferente de las leyes o reglamentaciones de protección de datos que ya existen en nuestros países.

Pero ¿Cuál es el vínculo de esto con el DNS, con internet y con ICANN?

A ICANN lo afecta desde dos frentes:

Internamente, como cualquier organización que recibe **datos personales** tiene que observar el cuidado en su tratamiento. Se refiere a datos que recopila y procesa para dar servicios internos o externos.

Pero además hay una dimensión especial que afecta a las partes contratantes de ICANN que son los **registros y los registradores de los dominios**, que siguen las reglas que ICANN ha establecido: cada vez que un registrante, ya sea una persona o una empresa u organización, registra un dominio se le solicita cierta información, relacionada con datos personales, que se recopila en un Directorio público denominado **WHOIS**. El Whois contiene la información de cada dominio: registrador y el registro. Anteriormente poseía más datos de carácter personal. Este WHOIS entra en contradicción con la disposición de la Unión Europea y esto, por consiguiente, repercute en cualquier empresa que registre dominios y mantenga datos de ciudadanos de la UE. Hace cerca de dos años la comunidad de ICANN comenzó el proceso de discusión sobre cómo cumplir con la disposición y, a la vez, cómo preservar los datos del directorio de WHOIS. En este sentido, se viene dando una discusión participativa de abajo hacia arriba.

De esta forma, se presentan dos temas muy importantes para la gobernanza de internet:

-Privacidad y Protección de datos en internet **vs.**

- Mantener este directorio de información que es parte de la misión de ICANN, por un lado, para mantener la estabilidad técnica y operativa de internet y, al mismo tiempo por otro lado proveer la información a la procuración de justicia. Por ejemplo para casos en lo que se investigue un delito que esté relacionado con algún sitio o página de internet, la justicia se sirve de la información de este directorio para dar con la persona o ubicación donde se utiliza la red de forma maliciosa.

Este proceso de discusión se está dando entre los distintos grupos de internet para poder llegar a una política que defina muy bien esta aplicación.

La discusión sobre el WHOIS ya se venía dando antes, donde algunos sectores buscaban un WHOIS más robusto y otros querían uno más delgado sin información sensible, pero la aplicación del GDPR aceleró este proceso en la comunidad. De esto surge una propuesta: "Especificación Temporal", es decir, un modelo interino que garantice un marco común para el manejo de los datos de registros de los gTLDs, mientras continúa el proceso de discusión entre los distintos grupos de interés de ICANN para llevar a una política que defina cómo seguir utilizando el WHOIS.

Algunas de las medidas propuestas es que no hubiera una sola capa de información frente a las personas que consultan el WHOIS sino distintas (modelo estratificado/escalonado) atendiendo al nivel de información necesario y cumpliendo, así, con el GDPR. Es decir, que el WHOIS solo muestre de manera pública una parte de la información y el resto que solo sea accesible por aquellos que lo soliciten a través de registradores u operadores y demuestren tener un interés legítimo (legal, por ejemplo). De acuerdo a esta Especificación temporal las partes contratadas de ICANN (registros y registradores) tienen que seguir recopilando la información de los usuarios que registran dominios. Esta propuesta aún se está discutiendo hoy.

<u>Las siguientes preguntas se dejan planteadas para el grupo reunido para discutir esta temática.</u>

<u>GDPR y su impacto en el DNS</u>

- ¿Cómo puede lograrse un equilibrio entre objetivos de privacidad/protección de datos personales y objetivos de seguridad y estabilidad operativa?
- ¿Cuáles han sido las lecciones aprendidas en torno al impacto de una regulación en aspectos globales de internet?
- ¿Cómo el modelo de las múltiples partes interesadas ha podido reaccionar eficientemente ante eventos externos?

Tal como se mencionó en la presentación, este tema ha sido parte de la agenda de todos los actores involucrados en el ecosistema de internet durante este año.

Las principales posturas comentadas en el grupo frente a las preguntas planteadas fueron:

Johanna Falliero (sector académico): sostiene que la dicotomía entre privacidad y protección de datos vs seguridad es errónea.

Enrique Chaparro (Sociedad civil): cree que es una contradicción el planteo principal. La recolección sobreabundante de datos en el DNS no hace a la estabilidad del DNS, hace al lobby del copyright. Para lograr que un paquete llegue a una dirección de destino no se necesita saber la dirección social. Para la función del DNS los datos de dirección física de la persona no tienen sentido. Si hay una contradicción en cuanto con las

agencias de cumplimiento de la ley. También el lobby de protección de datos que va en contra del poder principal en ICANN.

El GDPR no ha nacido de un día para el otro, y por ende ha sido una falla institucional de ICANN no haber tomado una decisión a tiempo. Existe algún mecanismo diferente para el guardado de los datos para grandes entidades que permitan ante un incidente de seguridad poder actuar rápidamente para salvar el problema de seguridad. Los datos que se van a guardar con una necesidad especifica no debería generar un problema. En el fondo no debería existir una contradicción entre ambos. ICANN está trabajando actualmente en una definición final.

Se aclara que en ICANN hay dos tipos de dominios. Códigos de país o genéricos: ccTLDs y gTLDs. Las políticas globales de ICANN afectan a los genéricos., los códigos de país tienen cierta flexibilidad según el tipo de administración que posean.

Erick Iriarte .pr: Menciona que el GDPR no es aplicable en su país por dos conceptos. Existe legislación propia de datos personales de 2011 y es funcionalmente operativa, protegemos los datos que nos han sido entregados bajo la legislación peruana (Ley 29733 Art 3 inc 23). Cuando es un servicio que se entrega y es transfronterizo ahí se aplica el GDPR, solo cuando se prestan servicio directo a ellos, en la moneda de ellos (euro). Actualmente solo 3 datos se almacenan: dirección postal, correo electrónico y DNS. Menciona que para él no existe el estándar para la publicación de datos de WHOS.

Luis Aranciabia, .cl: Si existen casos de registry y registrars y la mayoría son europeos. Ahí si tienen una función de controller y van camino a un standard distinto a la industria, es una tutela de los datos de los usuarios.

Alberto Soto: Cada gobierno puede tener su ley de protección de datos personales pero el caso es que la problemática de ICANN es que se trata de una organización global que tiene que respetar las leyes del estado de California y a cualquier temática en cualquier parte del mundo. Para tratar los datos de WHOIS hay que enumerar 1, 2 y 3, si está ocupado. A partir de ahí hay intereses particulares y se debe partir de ahí para ver a cuáles se accede y vía pedido a través de la ley.

Otras preguntas que surgen en el debate:

¿Cuál es el balance de qué los delitos no se investiguen y cuales la protección?

¿Cuáles son los datos mínimos necesarios para operar?

Nombre de dominio, método de contactar al usuario. El problema operativo es poder comunicarnos rápido con el registrante por un problema técnico o delictivo.

¿Cuáles son esos datos?

E.C.: Se puede tener un punto de contacto, intermediado o no. El resto de los datos hacen a otro propósito.

Actualmente se mantiene un juicio entre ICANN vs EPAG, quien ha roto contrato con ICANN (La ICANN inició esta acción porque EPAG le informó que, a partir del 25 de mayo de 2018, dejaría de recolectar información de contacto técnico y administrativo al vender nuevas registraciones de nombres de dominio. EPAG considera que la recolección de dichos datos sería contraria al GDPR. La recolección de esta información se requiere en virtud del contrato entre la ICANN y EPAG.)

J.F.: Problemas como regulaciones de corte local y seguridad de datos se da acá o en cualquier lado. Deberíamos avanzar todos a partir de los mismos principios. Pensar estándares para todos más allá de los regionalismos. Se entiende que hay reticencia institucional para aplicarlo porque son más abarcativos y no menos de lo que tenemos.

¿Cuáles serán los principios a los que vamos a adherir de los planteados en el GDPR? Se debe tener en cuenta el Consentimiento expreso y tácito.

Conclusiones del debate:

Privacidad vs. Seguridad: Se acordó que no existe antagonismo entre privacidad y seguridad, que son dos principios fundamentales que deben existir y coexistir. Asimismo se acordó que se deben recolectar los datos pertinentes al uso que se le quiere dar y no tomar datos en sobreabundancia ya que sería un abuso. Por ejemplo: para asegurar la función del DNS no es necesario contar con la dirección postal del titular de dominio.

Se conversó acerca de la discusión y definición que se está dando desde ICANN sobre la necesidad de conjugar el próximo funcionamiento del WHOIS a partir de la aplicación del GDPR.

Se planteó la diferencia entre los ccTLDs y gTLDs, ya que los genéricos tienen un contrato con ICANN que deben cumplir y, por ende, seguir recolectando los datos de WHOIS, mientras que los ccTLDS varían en su forma de administración y cuentan con una situación más flexible. Estamos de acuerdo en mantener un punto de contacto con el titular, ya sea mediado o no. Se mencionó que no puede existir un estándar de WHOIS para todos.

Se actualizó acerca de la legislación local de los países representados en el grupo y se expresó que más allá de si se contara o no con legislación al respecto, no se modificaban sus prácticas dado que no impactaba el GDPR en su territorio.

Finalmente se mencionó que todos de alguna forma, deberíamos apuntar a los mismos principios más allá de los regionalismos y particularidades de cada país, y pensar en una definición global donde el centro sea el ciudadano, y que sea un acuerdo común para todos dado que la protección de datos en la región y en el mundo debería ser la misma.