La evolución del Whois en los dominios de nivel superior genérico.

AMPPI

Santiago Hidalgo Enríquez

El Whois.

Derivado de su relación contractual con ICANN (*Internet Corporation for Assigned Names*), los agentes registradores han tenido la obligación de recolectar y publicar cierta información de registrantes de nombres de dominio, en lo que comúnmente se le denomina el Whois.

La información en cuestión comprende nombre, organización, dirección, correo electrónico, número telefónico del registrante, y en su caso, los datos de contacto administrativo, técnico y de facturación. También refleja otra información importante como es la fecha de registro del nombre de dominio, su fecha de expiración, y cuales son los servidores configurados.

Por años, el Whois ha sido la fuente principal para usuarios que han buscado información respecto a los nombres de dominio y sus registrantes. En particular, el Whois ha sido una herramienta a la que han recurrido los titulares de marcas (y sus representantes), agencias policiales y equipos de respuesta a incidentes de seguridad informática, para monitorear y combatir ciertas actividades ilegales y/o abusivas en internet.

En términos generales, ha habido cierta preocupación respecto a la precisión y fiabilidad de la información contenida en el Whois. No obstante lo anterior, cualquier información disponible en este registro (aún y cuando se hayan proporcionado datos falsos) puede ser fundamental para detectar actividad ilícita en internet, especialmente cuando dicha información se reutilice en varios dominios relacionados.

Desde sus orígenes mismos, el protocolo Whois ha experimentado profundos cambios, frecuentemente en respuesta a acontecimientos importantes que afectan la industria de nombres de dominio. El Whois que se conoció en una época se ha

ido transformando con el paso del tiempo, por múltiples razones que se explicarán a continuación.

Los servicios de privacidad y los servicios proxy.

Uno de los acontecimientos más importantes en relación con el Whois y los dominios de nivel superior genérico ("gTLDs") se refiere a la introducción y desarrollo de los servicios de privacidad y de los servicios proxy[1]. Este tipo de servicios son ofrecidos por algunos agentes registradores a sus clientes (algunos de manera gratuita), y tienen un efecto muy concreto: evitar que los datos de contacto del registrante aparezcan públicamente en el Whois. En su lugar, dependiendo del proveedor de servicios de que se trate, pudieran aparecen los datos de contacto del servicio de privacidad mismo o datos de contacto anonimizados.

De esta manera, terceros interesados pueden contactar al registrante del nombre de dominio a través del servicio de privacidad mismo o a través de un correo electrónico anonimizado. En cualquier caso, estos servicios imposibilitan la consulta pública de los datos del registrante de los nombres de dominio que estén bajo este esquema.

El objetivo general de estos servicios es proteger los datos personales y la seguridad de los registrantes en internet. A título ilustrativo, un servicio de privacidad puede impedir o dificultar comunicaciones no solicitadas (*spam*), e incluso puede prevenir un ataque dirigido (*spear phishing*), fabricado a partir de los datos generales del registrante, que de otra manera hubieran sido de libre acceso al público.

RGPD.

[1] En adelante, se hará referencia solo a "servicios de privacidad" para referirse a ambos. Consúltese la Especificación sobre registraciones de privacidad y proxy del Acuerdo de Acreditación de Registradores disponible en https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-es, para ver las diferencias entre ambos tipos de servicios, de acuerdo a la ICANN.

Otro acontecimiento de gran impacto ha sido el surgimiento y desarrollo de legislación en materia de protección de datos personales. Esto es especialmente cierto con la aparición del Reglamento General de Protección de Datos ("RGPD") en 2018[2], en sustitución de la Directiva de Protección de Datos, que estuvo en vigor desde 1995.

El RGPD es una regulación de aplicación para todos los particulares ubicados en la Unión Europea y en el Espacio Económico Europeo. Este Reglamento fue introducido para armonizar legislación en materia de datos personales en Europa, y entre otras disposiciones, contempla la recolección y envío de datos fuera de la Unión Europea.

El RGPD ha dejado una marca muy notable en la industria de los nombres de dominio, cambiando significativamente el rol del Whois, probablemente a permanencia. En la proximidad a la entrada en vigor del RGPD, había especulación respecto a si la práctica de los agentes registradores (en cumplimiento a sus obligaciones contractuales con la ICANN) de recolectar, retener y publicar en el Whois la información de los registrantes ubicados en la Unión Europea (muchas veces sin su consentimiento expreso), estaba o no acorde con lo establecido en el RGPD. La preocupación era considerable, especialmente si se tiene en cuenta que las multas contempladas en este reglamento pueden llegar hasta los 20 millones de euros por infracción.

En atención a lo anterior, el 17 Mayo de 2018, ICANN anunció la adopción de la *Temporary Specification for gTLD Registration Data* ("Especificación Temporal"), que comprendía una serie de medida interinas en respuesta a la inminente entrada de vigor del RGPD el 25 de Mayo de ese mismo año. Bajo esta, se establecieron lineamientos para la recolección, retención y publicación de información en los Whois de todos los gTLDs, en línea con el marco jurídico determinado por el RGPD.

[2] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=ES

En la Especificación Temporal se introdujeron diversos cambios y obligaciones importantes para los agentes registradores, incluyendo las siguientes: remover información personal del Whois, incluyendo nombre, dirección, número telefónico y correos electrónicos; establecer un mecanismo para enviar comunicaciones al registrante (y a los contactos administrativos, técnicos y de facturación) a través de formularios de contacto o correos electrónicos anonimizados; establecer un sistema de acceso progresivo, que permita a particulares y organizaciones que tuvieran un interés legítimo, consultar la información restringida; establecer un mecanismo para que los registrantes interesados puedan dar su consentimiento expreso, para que sus datos personales sean publicados en el registro Whois.

La vigencia de la Especificación Temporal fue extendida respecto a lo contemplado originalmente y de facto se encuentra aún aplicable. Actualmente, ICANN está en proceso de desarrollar una política más formal y posiblemente definitiva, que tome en consideración los requisitos establecidos en el RGPD, y que a su vez tome en cuenta las necesidades de las partes interesadas en acceder a la información contenida en los registros Whois.

Problemas y desafíos.

El hecho es que en la actualidad, en la mayoría de los Whois de gTLDs, es imposible consultar la información completa del registrante. El surgimiento de los servicios de privacidad, y especialmente el desarrollo en normativa en materia de datos personales, hizo que esto fuera inevitable. Un estudio formulado por Intersile Consulting Group señala que en 2020, solamente en un 13.5% los datos de contacto del registrante estaban disponibles sin restricciones en el Whois[3].

No cabe duda que las medidas referidas anteriormente han probado ser efectivas en resguardar la privacidad de los usuarios. A pesar de ello, y de manera evidente, este desarrollo no viene exento de inconvenientes. Los abusos relacionados con el uso no adecuado de nombres de dominio han existido desde

[3] https://interisle.net/ContactStudy2021.pdf

los orígenes mismos de estos. Desafortunadamente, y de manera alarmante, en los últimos años estos abusos se han multiplicado exponencialmente, volviéndose además cada vez más sofisticados y peligrosos.

Es una realidad que algunos cibercriminales se han visto beneficiados de cierto modo con los cambios que el Whois ha experimentado con el tiempo, al haberse dificultado su identificación y/o contacto. Esto ha creado desafíos concretos para diversas partes involucradas, incluyendo los titulares de marcas, quienes se han visto más limitados en cuanto a las posibles acciones y la rapidez en que estas se pueden tomar.

Bajo el marco jurídico actual, pareciera que el concepto de "abuso"[4] en relación con el uso de un nombre de dominio, frecuentemente está sujeto a interpretación por parte de los agentes registradores. Es importante recordar que hay cientos de ellos en todo el mundo, con diferentes características y capacidades.

Ante solicitudes de los interesados, los agentes registradores pueden llegar a suspender un nombre de dominio, cuando se haya presentado evidencia que conecte a este con actividad claramente ilícita, como lo es el *phishing,* el *pharming* o el uso de *botnets*.

Tratándose de reportes sobre violación a derechos de propiedad intelectual de terceros, las reacciones de los agentes registradores pueden variar mucho dependiendo de sus propias políticas. Algunos pueden llegar a tomar medidas concretas (ej. revelar los datos del registrante al solicitante), pero habrá otros que se mostrarán menos activos, invitando a los solicitantes a acudir a las autoridades administrativas o jurisdiccionales que correspondan. Muchas veces los agentes registradores adoptaran una posición en extremo cautelosa, por temor a incumplir alguna disposición del RGPD.

La realidad es que no siempre hay certidumbre para los solicitantes de información, los cuales a menudo tienen que lidiar con múltiples agentes registradores y con diferentes procedimientos, sin que necesariamente se vaya a

[4] Ver la definición de "abuso" de acuerdo al *DNS Abuse Institute* en https://dnsabuseinstitute.org/about-the-dns-abuse-institute/

obtener un resultado favorable. Por otro lado, tampoco existe un sistema que permita una verdadera rendición de cuentas por parte de los agentes registradores, quienes cuentan con una casi completa discrecionalidad en la identificación del "abuso" y de las posibles acciones que en su caso tomarán al respecto.

Al margen de lo anterior, la problemática fundamental es la aparente colisión de intereses legítimos contrapuestos. Por un lado, se tiene la posibilidad de conocer la identidad e información del registrante de un nombre de dominio, particularmente cuando existen razones válidas para esto (violación de derechos de propiedad intelectual, actividad abusiva, dificultades técnicas), y por otro lado se tiene el interés de proteger los datos personales de los registrantes, así como su privacidad en internet.

La problemática es compleja, particularmente si se toma en cuenta que son muchas las partes involucradas en la industria, incluyendo: los agentes registradores, los servicios de privacidad, los proveedores de servicios *escrow*, los proveedores de servicios *hosting*, los registrantes, los inversionistas de nombres de dominio (*domainers*), los promotores/defensores de la propiedad intelectual, los usuarios de internet, en fin, una gran cantidad de grupos y asociaciones de diferentes tipos, muchas veces con intereses diferentes y en ocasiones aparentemente contrapuestos.

¿Qué se avecina?

Poco después de la adopción de la Especificación Temporal, en ICANN se empezó a manejar la idea del posible desarrollo y adopción del denominado *System for Standardized Access/ Disclosure* ("SSAD"), consistente en un sistema centralizado capaz de atender y resolver, todas las solicitudes de acceso a información personal restringida en gTLDs.

El concepto fundamental era que las partes interesadas pudieran concentrar en una sola plataforma todas las solicitudes de acceso a información, en lugar que tener que acudir separadamente ante cada agente registrador. Además, entre otras cosas, con el SSAD se contemplaba implementar: un proceso de acreditación ante

una autoridad central creada especialmente para esos efectos; un proceso de verificación de identidad de solicitantes de información; y un proceso de trasmisión de datos de manera automatizada, bajo ciertas circunstancias (ej. agencias policiales).

En atención a los altos costos estimados (de 20 a 27 millones USD por su desarrollo, y de 14 a 107 millones USD anualmente por su operación), uno de los principales objetivos del SSAD era que este fuera sostenible financieramente, por lo que se contemplaba que los solicitantes tendrían que pagar diversas tasas por su utilización.

Después de extensos estudios y análisis, a mediados de 2022, se decidió suspender temporalmente este proyecto. Había surgido preocupación respecto a los altos costos, incertidumbre respecto a la cantidad de potenciales usuarios, y finalmente, dudas sobre el posible impacto real y la utilidad misma del SSAD.

En seguimiento a lo anterior, la Junta de ICANN solicitó el desarrollo de un proyecto que sea menos costoso, más simple y de uso gratuito para los solicitantes. El resultado de esto es el surgimiento del denominado más adelante *Registration Data Request Service* ("RDRS"), que sería ejecutado en un programa piloto de 2 años y que usaría gran parte de la tecnología con que ya cuenta ICANN.

Este nuevo sistema no incluiría algunas de las ventajas originalmente contempladas en el SSAD, como es la existencia procesos de acreditación de solicitantes. No obstante lo anterior, la implementación del RDRS permitirá generar información que será fundamental en las futuros estudios y conversaciones en torno al por ahora pausado SSAD.

Hay que decir que uno de los principales inconvenientes del RDRS (también presente hasta ahora en el concepto SSAD), es que no se puede garantizar a los solicitantes el acceso a la información requerida, y ni siquiera se puede garantizar que los agentes registradores atenderán las solicitudes correspondientes. Como está concebido el sistema al día de hoy, los agentes registradores que participen voluntariamente (otro gran inconveniente) deberán proveer un "acceso razonable"

a la información, pero no existe un marco legal (contractual o derivado de una política) que les obligue a sujetarse directamente al RDRS.

El tiempo dirá si sobre estas bases se materializa un sistema funcional y efectivo. De ser el caso, será de especial interés ver bajo qué condiciones y de qué manera se manejarán las solicitudes de acceso a información de registrantes de nombres de dominio, cuando estas provengan de partes con intereses legítimos.

El concepto de un sistema progresivo que permita a los titulares de intereses legítimos acceder a información restringida de registrantes no es del todo nuevo y ha sido ya incorporado en las políticas de algunos dominios de nivel superior geográfico ("ccTLDs"), como lo son la Unión Europea ".eu" y Suecia ".se". Bajo estas, se puede conceder diferentes niveles de acceso a información en atención al tipo de intereses legítimos con que cuenten los solicitantes. Por ejemplo, a las agencias policiales o a los titulares de marca se les puede conceder un mayor grado de acceso a información que al público en general.

Finalmente, vale la pena hacer referencia a la adopción de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)[5] ("la Directiva") en noviembre de 2022.

El objetivo general de esta, es mejorar la ciberseguridad de la infraestructura crítica y de los servicios digitales en la Unión Europea (incluyendo el sistema de nombre de dominio), y también promover la cooperación y el intercambio de información entre Estados miembros y proveedores de servicios digitales, para responder adecuadamente a ciberataques y amenazas.

Entre muchas otras cosas, la Directiva obligará a los agentes registradores a obtener y mantener información completa y correcta de los registrantes, publicando la información que no constituya datos personales. Asimismo, de conformidad con este ordenamiento, los agentes registradores deben proporcionar acceso a

[5] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555&from=EN

información de los registrantes (en un plazo no mayor a 72 horas) cuando esta provenga de solicitudes fundadas en intereses legítimos. Aunado a lo anterior, las políticas de los agentes registradores respecto a estos procedimientos deberán hacerse públicas.

Al tratarse de una Directiva Europea, próximamente los Estados miembros de la Unión deberán adoptar normativa nacional que se alinee con esta. La regulación que surja tendrá un impacto significativo en diversos ccTLDs, pero además, similar a lo ocurrido con el surgimiento del RGPD, pudiera tener un impacto importante a nivel global, que pudiera afectar también a los gTLDs.

Conclusiones.

ICANN tiene una estructura compleja que involucra a representantes de diferentes sectores de la industria (la sociedad civil, la comunidad técnica, el sector privado, etc.) en la toma de decisiones de la organización. El objetivo de este modelo (*multistakeholder model*) es evitar que un solo grupo tenga el control sobre el gobierno de internet, fomentando el intercambio de ideas, en búsqueda de consensos para el desarrollo y adopción de políticas y procesos. Se trata de un enfoque verdaderamente global, para un tema tan mundial como es el internet.

En el caso de los ccTLDs, los procedimientos para adoptar y modificar políticas son comparativamente simples, toda vez que solo involucran instituciones y organizaciones de tipo nacional/regional. Por lo que hace al sistema de gTLDs sin embargo, que es manejado fundamentalmente por ICANN, implementar cualquier tipo de cambio puede ser en ocasiones complicado y tardado.

Es interesante mirar hacia algunos casos de ccTLDs (por ejemplo Australia ".au"), donde en sus políticas[6] claramente se ha señalado que cierta información personal proporcionada será publicada en el Whois, y los registrantes deben dar su consentimiento expreso para ello, en caso de que quieran proceder con el registro del nombre de dominio en cuestión.

[6] https://www.auda.org.au/policy/2014-07-whois-policy

Esta dirección probablemente nunca se seguirá tratándose de gTLDs, en vista de los diferentes acontecimientos y discusiones que ha habido en la comunidad de ICANN en los últimos años. Queda claro que los días en los que se podía acceder sin restricciones a la información en el Whois han pasado y no volverán.

ICANN, con su *multistakeholder model*, debe demostrar que cuenta con la capacidad de reaccionar adecuada y oportunamente ante los cambios y necesidades que han ido surgiendo en la materia. En lo concerniente al Whois, uno de los desafíos más importantes es definir con claridad donde está el balance entre la información que debe estar disponible al público y aquella información de acceso restringido. También se deben definir y establecer los procesos necesarios para ello. Desafíos aún más complejos sobre otros temas se pueden presentar en el futuro, que pondrían a prueba la capacidad de la organización para resolverlos eficazmente.

Hay que decir que uno de los principales temas tratados en ICANN 76, celebrado en la ciudad de Cancún en marzo de este año, fue precisamente el del desarrollo del RDRS. Si bien aún existen algunos detalles por definir (ej. lograr garantizar la confidencialidad de las solicitudes de acceso a la información por parte de las agencias policiales), se espera que el sistema empiece a operar en menos de un año.

Estos y otros desarrollos (ej. la migración completa a un modelo *Thick Whois* e implementación completa del *Privacy and Proxy Services Accreditation Implementation*) en curso, confirman que se avecinan cambios importantes en torno a la manera como el Whois opera, que habrá que seguir con interés. De cualquier manera, los avances continuarán, y el vasto sistema de nombres de dominio se irá perfeccionando con el tiempo.