Council of European National
Top-Level Domain Registries

Registros de nombres de dominio y contenidos en línea

Contenido

Resumen ejecutivo 4

Introducción 6

Objetivos de este documento 6

Esquema de este documento 6

Internet, el sistema de nombres de dominio y el contenido en línea 7

El DNS como parte de la infraestructura de Internet 7

La infraestructura IP y de Internet 7

El Sistema de Nombres de Dominio 7

El contenido en línea 8

Poner a disposición los contenidos en línea 8

Utilización del DNS como una herramienta de ayuda para encontrar contenidos 9

Actuar contra el contenido ilegal en la red 11

¿Qué es el contenido ilegal? 11

¿Quién puede juzgar la legalidad del contenido? 12

¿Dónde se encuentra el contenido en línea? 13

Ubicación en Internet 13

Localización física 13

Eliminar el contenido ilegal 13

Contactar al editor de contenidos o al proveedor de alojamiento 13

Contactar al titular del nombre de dominio 14

Dificultar la localización de contenidos 14

Otros pasos a seguir cuando la eliminación del contenido ilegal no tiene éxito 14

Riesgos e inconvenientes al eliminar un nombre de dominio en el registro 15

Prácticas actuales de los ccTLD 18

Educación y sensibilización, con especial atención al diálogo abierto y a la cooperación con las autoridades y Agentes del cumplimiento de la ley (LEA) 18

Educación y sensibilización a nivel comunitario 18

Educación y estrecha colaboración con autoridades y fuerzas del orden 20

Los registros como proveedores de datos autorizados de nombres de dominio 21

Compartir datos de registro con terceros 23

Respondiendo a informes de contenido sospechoso 23

Respuesta a los informes externos 23

Detección de actividades ilegales con medidas adicionales 25

Conclusión 26

Resumen ejecutivo

Los miembros de CENTR son registros de ccTLD, cuya función consiste en administrar los dominios de nivel superior con código de país de Internet (ccTLD). Son responsables de proporcionar y operar la infraestructura técnica del DNS para su TLD, organizar el proceso de registro de los nombres de dominio, y mantener de forma proactiva la base de datos de registro de modo que los nombres de dominio se puedan usar para navegar por Internet.

El contenido abusivo e ilegal disminuye la confianza en Internet como plataforma para la innovación, la creatividad y las oportunidades económicas. Los registros de ccTLD se comprometen a contribuir a un enfoque integral y eficaz contra el contenido ilegal en línea.

Internet es una colección global de redes informáticas interconectadas que permite la comunicación mediante el uso de direcciones IP numéricas únicas. El Sistema de Nombres de Dominio (DNS) funciona como una capa sobre la infraestructura IP. Los nombres de dominio facilitan a los humanos navegar por Internet. Por ejemplo, cuando un usuario escribe el nombre de dominio de un sitio web, el DNS le dirá al dispositivo del usuario cuál es la dirección IP correspondiente donde se puede encontrar el contenido de dicho sitio web.

Para que los contenidos sean accesibles a través de Internet, deben estar almacenados en al menos un computador o servidor que esté conectado a la red. Para eliminar efectivamente los contenidos de Internet, deben ser borrados del dispositivo en el que están alojados, o ese dispositivo debe ser desconectado de Internet.

La calificación del contenido como “ilegal” depende del marco legal local e incluso puede variar según el contexto. Se define localmente quién tiene la autoridad para hacer este juicio.

Eliminar el contenido ilegal de Internet es la única forma efectiva de evitar que se acceda y se consuma dicho contenido. Dos partes tienen acceso directo al contenido o al dispositivo que lo almacena: el editor del contenido y el proveedor de alojamiento. Son los primeros que deben ser contactados.

Cuando se utiliza un nombre de dominio para facilitar el acceso al contenido, el titular del nombre de dominio puede ser el proveedor del contenido y del alojamiento, o ser capaz de identificar a dicho proveedor. La base de datos autorizada del registro, que contiene la información sobre todos los nombres de dominios registrados bajo su TLD, puede ayudar a identificar y contactar al titular del dominio.

Cuando no es posible eliminar el contenido ilegal de Internet —lo que garantiza la única solución efectiva— se puede tratar de dificultar que los usuarios encuentren o accedan a dicho contenido. Existen diferentes métodos para “bloquear” el contenido de Internet, en diferentes niveles e involucrando a diversos actores. Sin embargo, todos tienen en común que el contenido permanece disponible y que la acción puede causar daños colaterales involuntarios. Por lo tanto, estos métodos deben considerarse como una medida provisional que se utilizará en el caso de una emergencia o cuando todo lo demás haya sido probado y haya fallado. Bloquear o eliminar un nombre de dominio es una de esas medidas.

Los marcos legales locales definen qué contenido es ilegal, a quién se le ha otorgado la autoridad para tratar con él y qué procesos están permitidos dentro del estado de derecho. Esto puede variar de un país a otro. Los ccTLD tienen diferentes requisitos respecto a quién puede registrar nombres de dominio y cuáles son sus funciones. La combinación de estos requisitos y el marco legal local influye en las políticas e iniciativas que el registro desarrolla para abordar el contenido ilegal en línea.

Normalmente, estas políticas están arraigadas en la comunidad local, son compatibles con las leyes locales, abordan las necesidades locales y, con frecuencia, se han desarrollado en consulta y cooperación con otras partes interesadas locales. Las políticas y prácticas exitosas para un ccTLD podrían inspirar a otros. Sin embargo, debido a las raíces y particularidades locales, no hay garantía de que la adopción o copia del proyecto o de la política de un ccTLD conduzca al mismo resultado positivo o incluso sea legal en el marco de otro registro:

- En cuanto al contenido ilegal, los registros de ccTLD, entre otros, se centran en:
- La educación y sensibilización a nivel comunitario.
- La educación y la estrecha colaboración con las autoridades y las fuerzas de seguridad.
- El mantenimiento de la base de datos del ccTLD para mejorar la calidad de los datos de registro. Esto puede tener un impacto positivo indirecto, ya que es poco probable que quienes tengan malas intenciones registren un nombre de dominio utilizando información personal correcta.
- Establecer procedimientos para compartir datos de registro con terceros dentro de los límites de las regulaciones de privacidad local.
- Desarrollar procesos para responder a los reportes de contenido sospechoso. Estos procedimientos suelen tener en común que son aplicables a casos limitados y bien definidos, y que en ellos interviene una parte externa con experiencia en la evaluación de ese tipo de contenidos.

Introducción

Los miembros de CENTR administran el registro para uno o más dominios de nivel superior con código de país de Internet (ccTLD). Son responsables de proporcionar y operar la infraestructura técnica del DNS para su TLD, organizar el proceso de registro de los nombres de dominio, y mantener de forma proactiva la base de datos de registro de modo que los nombres de dominio se puedan usar para navegar por Internet.

Los miembros de CENTR creen que la confianza y la seguridad en línea son esenciales para que Internet siga siendo una plataforma para la innovación, la creatividad y la oportunidad económica. El contenido abusivo e ilegal disminuye la confianza. Los registros están comprometidos a contribuir con otros actores en un enfoque integral y efectivo contra el contenido ilegal en Internet.

Objetivos de este documento

El esfuerzo conjunto y la cooperación exitosa requieren que las partes interesadas comprendan y respeten la función, el rol y las limitaciones de los demás. El objetivo de este documento es aclarar el rol de un operador de registro de ccTLD, explicar su relación con el contenido en línea, explorar las posibilidades y limitaciones de las acciones, y establecer expectativas correctas de lo que un registro puede y no puede hacer cuando se trata de contenido ilegal en línea.

Esquema de este documento

La primera sección del documento proporciona una idea de cómo funciona Internet, dónde se encuentra el contenido en línea y cómo se puede acceder a él; además, explica la función facilitadora del Sistema de Nombres de Dominio (DNS).

La segunda parte del documento analiza la cuestión del contenido ilegal en Internet y examina cómo los operadores de registro de ccTLD podrían contribuir a las acciones que conducen a la eliminación de dicho contenido.

Una tercera sección está dedicada a las políticas y prácticas actuales de los registros. A través de una lista no exhaustiva de ejemplos, se expone cómo los diferentes registros de ccTLD desarrollan políticas y toman las medidas que mejor se adaptan a las necesidades de sus comunidades locales, y cómo contribuyen así a la lucha conjunta contra el contenido ilegal en línea.

Internet, el sistema de nombres de dominio y el contenido en línea

El DNS como parte de la infraestructura de Internet

La infraestructura IP y de Internet

Internet es una colección de redes de computadoras que están interconectadas y juntas forman un sistema de comunicación global. El Protocolo de Internet (IP) es el método o conjunto de reglas mediante el cual los datos se envían a través de Internet de un dispositivo a otro. Para tener una transferencia exitosa, es importante que el remitente y el receptor se puedan identificar y ubicar entre los millones de computadoras, teléfonos inteligentes, servidores, IoT y otros dispositivos que están conectados a Internet. Por lo tanto, todos los dispositivos conectados tienen al menos una dirección IP que los identifica de forma única de todos los demás dispositivos. Una dirección IP puede representarse como una etiqueta numérica[1]: por ejemplo, la dirección IP 2001:db8:85a3::8a2e:370:7334[2] podría identificar la interfaz de un servidor donde se almacena el contenido de un sitio web.

El Sistema de Nombres de Dominio

Para los humanos, leer y recordar direcciones IP numéricas es difícil. Para resolver esto, el Sistema de Nombres de Dominio (DNS) permite el uso de nombres de dominio para referirse a las direcciones IP. El DNS funciona como una capa encima de la infraestructura IP. Cuando, por ejemplo, un usuario escribe un nombre de dominio en un navegador o hace click en un enlace con un nombre de dominio, el dispositivo buscará la dirección IP correspondiente en el DNS. Cuando se resuelve el nombre de dominio —"resuelve" significa que el DNS devuelve una dirección IP— el dispositivo del usuario sabe dónde se puede encontrar en Internet el contenido de un sitio web o el buzón conectado a una dirección de correo electrónico.

El DNS se caracteriza por su estructura jerárquica, que consta de diferentes dominios de nivel superior (TLD) bajo una sola raíz. La extensión de un nombre de dominio, esto es la parte después del último punto, indica en qué TLD se registra el nombre (por ejemplo, .de, .com, .fr). La estructura jerárquica es relevante para el funcionamiento del DNS; y la forma iterativa lo es para buscar nombres de dominio.[3]

Un registro de nombres de dominio es responsable de la administración de uno o más TLD. Todos los registros deben respetar las normas técnicas y los requisitos del DNS, pero con respecto a las políticas, cada TLD sigue siendo responsable del establecimiento de sus propias reglas. Mientras que los TLD genéricos (gTLD) tienen que cumplir las políticas y los procesos generales desarrollados por la comunidad de la ICANN, los TLD con códigos de país (ccTLD)

1 Las direcciones IPv6 tienen una longitud de 128 bits y se representan mediante una cadena hexadecimal. La versión anterior de IPv4 tiene una longitud de 32 bits y se indica en grupos de números decimales separados por puntos.

2 Esta dirección IP es solo para fines de documentación y no se enruta a la Internet pública (RFC 3849, prefijo de la documentación IPv6).

3 Para más información sobre el funcionamiento del DNS: https://www.centr.org/about-the-industry/

establecen su propia política de acuerdo con las necesidades de sus comunidades locales de Internet.

El contenido en línea

El contenido debe ser creado, almacenado y puesto a disposición antes de que pueda encontrarse en Internet. La forma en que esto sucede se describe en esta sección identificando los diferentes roles y responsabilidades.[4]

Poner a disposición los contenidos en línea

Proveedor de contenido

El proveedor de contenido suministra a Internet texto, sonido, imágenes, videos, animaciones y otras formas de contenido que son cargadas en un sitio web, publicadas en un blog, puestas a disposición en las plataformas sociales, etc. El proveedor/editor del contenido puede ser, pero no es necesariamente el creador original del contenido.

Para poder acceder a él a través de Internet, el contenido debe almacenarse en al menos una computadora o servidor que esté conectado a Internet. Un proveedor/editor de contenido puede usar su propia computadora o servidor o, más probablemente, hacer uso de los servicios y la infraestructura de un proveedor de alojamiento.

Proveedor de alojamiento

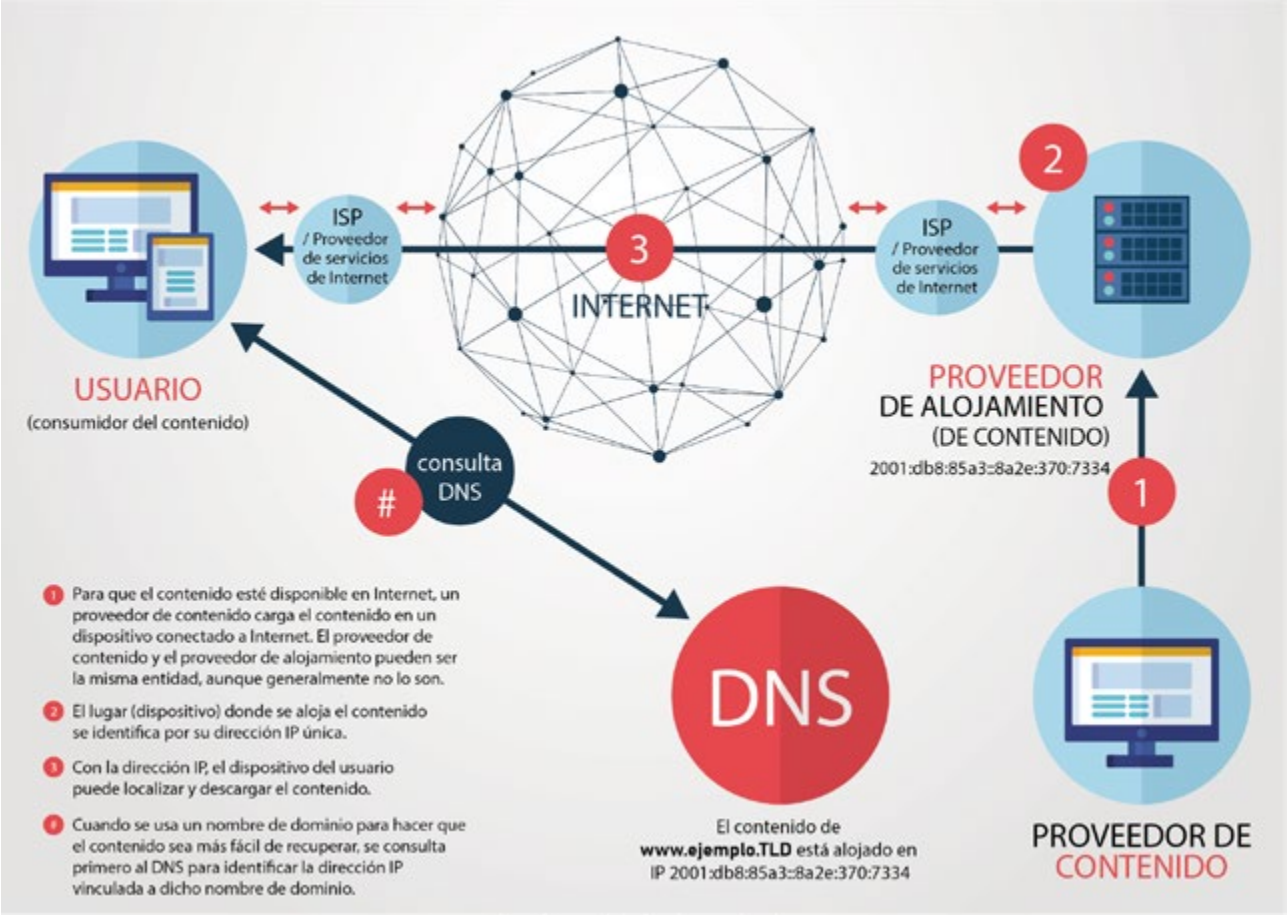
Un proveedor de alojamiento proporciona almacenamiento y conectividad, tiene la experiencia técnica y, lo que es más importante, la infraestructura, la capacidad y el ancho de banda necesarios para hacer frente al tráfico que puede provenir de cualquier parte de Internet en cualquier momento del día. Los proveedores de alojamiento proporcionan la plataforma para que se aloje el contenido, pero no deciden qué se publica o no; esta decisión la toman sus clientes (los proveedores/editores de contenido). Salvo algunas excepciones (generalmente, organizaciones grandes con su propia infraestructura y redes), un proveedor de contenido usará los servicios de un proveedor de alojamiento. Los proveedores de alojamiento tienen grandes centros de datos con servidores que contienen el contenido de sus clientes. Estos servidores están conectados a Internet y pueden identificarse por su dirección IP única. Hay diferentes tipos de alojamiento; los más comunes son web y alojamiento de correo electrónico. El alojamiento de redes sociales (por ejemplo, videos generados por usuarios) podría considerarse un caso especial entre la publicación y el alojamiento.

Proveedor de servicios de Internet / Proveedor de acceso

El proveedor de servicios de Internet (ISP, por sus siglas en inglés) proporciona acceso a Internet. A través de la red y la infraestructura del ISP, sus clientes pueden acceder a Internet. El ISP asignará direcciones IP a los dispositivos conectados a su red, por ejemplo, los servidores del proveedor de alojamiento, el módem del usuario de Internet, etc. El ISP es un proveedor de acceso por lo que no almacena ningún contenido. No obstante, el contenido viaja a través de su infraestructura.

4 Los actores pueden combinar uno o más roles descritos en esta sección, por ejemplo, un ISP también puede proporcionar servicios de alojamiento.

Hay otros participantes que también garantizan el transporte y el intercambio de datos entre redes, como los puntos de intercambio de tráfico (IXP, por sus siglas en inglés) y los operadores de redes (de corta o larga distancia). Además, se identifican las redes de distribución de contenido (CDN[5], por sus siglas en inglés), que alojan copias del contenido de sus clientes en servidores ubicados en diferentes puntos geográficos para optimizar la experiencia del usuario final (por ejemplo, Cloudflare). La relación de estos otros participantes con el contenido no se profundiza en este trabajo.



Utilización del DNS como una herramienta de ayuda para encontrar contenidos

El Sistema de Nombres de Dominio (DNS) proporciona una función que ayuda a "navegar" por Internet y permite recuperar la dirección IP vinculada a un nombre de dominio. Por lo tanto, algunos comparan el DNS con una guía telefónica o un registro de propiedad o compañía.[6]

Titular del nombre de dominio / registrante

Un editor/proveedor de contenido puede registrar un nombre de dominio para facilitar a los usuarios de Internet el acceso al contenido que ha puesto a disposición en línea. El nombre de dominio funciona como una etiqueta sobre la dirección IP; es más fácil de memorizar que la dirección IP numérica y puede contener información útil, como el nombre de una empresa en una dirección de correo electrónico o una referencia al contenido en el nombre de dominio de un sitio web.

5 https://en.wikipedia.org/wiki/Content_delivery_network

6 https://en.wikipedia.org/wiki/Domain_Name_System

El titular del nombre de dominio no es necesariamente el (o el único) proveedor de los contenidos publicados bajo el nombre de dominio. Por ejemplo, los sitios web de grandes universidades, sitios de blogs o sitios de redes sociales permiten que otros publiquen contenido en un sitio identificado por un solo nombre de dominio.

El titular de un nombre de dominio o registrante tiene el derecho de usar un nombre de dominio específico. Para obtener este derecho, una persona o entidad registra el nombre en el registro del TLD, directamente o a través de un registrador. El titular del dominio es responsable de cómo se usa dicho nombre de dominio.

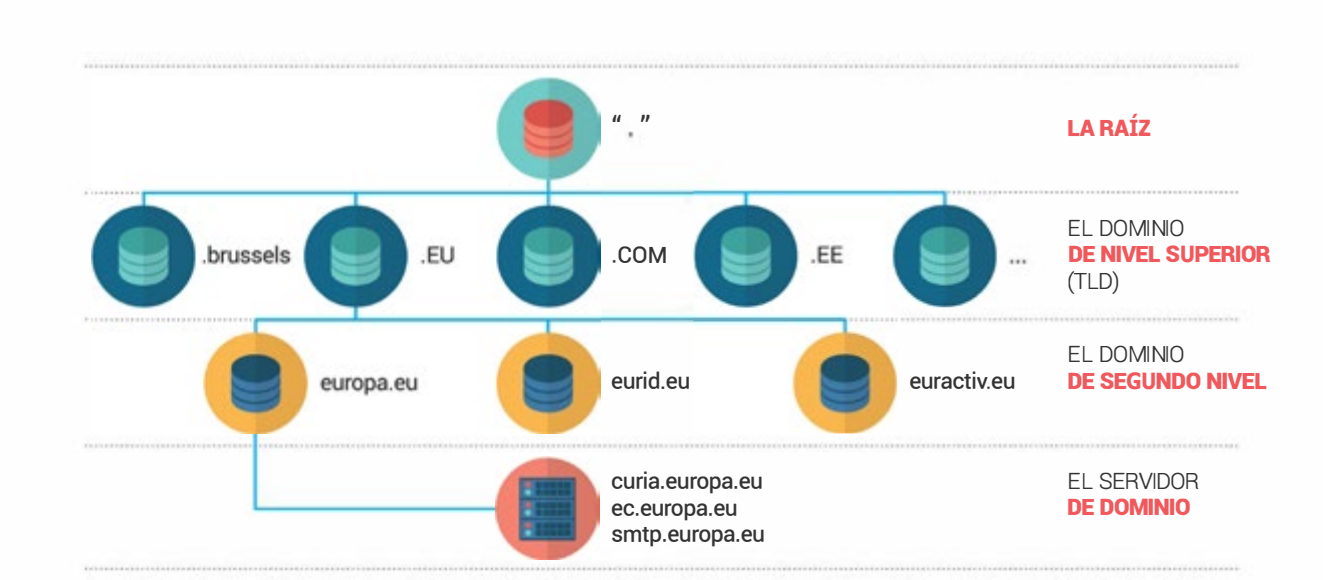
Registrador de nombres de dominio

Un registrador es una empresa que proporciona servicios de registro de dominios a compañías y a personas, directamente o a través de una red de revendedores. El registrador está acreditado por uno o más registros para ofrecer nombres de dominio bajo sus TLD. El registrador verifica la disponibilidad del nombre de dominio y administra el proceso de registro, mientras que el registro gestiona el TLD del nombre solicitado. Como parte del proceso de registro, el registrador enviará la información de contacto del titular del dominio y la información técnica relacionada con el nombre de dominio (por ejemplo, qué servidores de nombres contienen los registros DNS que le indicarán a los navegadores web y a los clientes de correo electrónico dónde encontrar el servidor web con el contenido del sitio web o el servidor de correo que maneja el correo electrónico). Un registrador no aloja contenido, y ningún contenido pasa a través de su infraestructura. Sin embargo, en la práctica, muchos registradores también proporcionarán alojamiento y otros servicios para sus clientes.

Operador del registro de un TLD

El registro administra la única base de datos autorizada de nombres de dominio registrados bajo su TLD y publica esta información en el DNS. Los servidores de un registro de dominios contienen información sobre el titular del dominio, el registro del dominio (por ejemplo, la fecha de caducidad), las direcciones IP vinculadas con el nombre del dominio y otros detalles técnicos. Un registro publicará un archivo de zona actualizado varias veces al día, el cual consiste en un archivo de texto que contiene las asignaciones entre el nombre de dominio y los servidores de nombre propios de cada nombre registrado, así como otros recursos. Este archivo contiene la información sobre cómo ubicar las direcciones IP y otra información necesaria para navegar en Internet. Los registros no almacenan ni optimizan el contenido.

> Nota: La mayoría de los ISP almacenan en caché la información DNS de nombres de dominio consultados recientemente correspondientes a diferentes TLD en los llamados servidores de nombres no autorizados para acelerar la experiencia de navegación de sus clientes. Solo cuando una respuesta reciente no está disponible en el servidor del ISP, se consultará al DNS. Como consecuencia, los cambios realizados en el DNS (como la eliminación de un nombre de dominio del DNS por parte del registro) pueden tomar algún tiempo antes de que entren en vigencia en cualquier parte de Internet.



Actuar contra el contenido ilegal en la red

¿Qué es el contenido ilegal?

El término “ilegal” se usa para describir aquel contenido que está prohibido en un contexto nacional, sin importar el motivo. La Comisión Europea, por ejemplo, define el contenido ilegal como “cualquier información que no cumpla con el Derecho de la Unión o el Derecho de un Estado miembro”.[7] Aparte de los asuntos relacionados con el abuso sexual infantil, existe escaso consenso internacional sobre lo que constituye el contenido apropiado desde una perspectiva de política pública. Lo que está permitido en una jurisdicción puede estar prohibido en otra. La permisibilidad del contenido también puede estar relacionada con el contexto: el contenido que se considera ilegal en un contexto (como una comedia indecente vista por niños) puede ser aceptable en otro (como cuando es vista, por ejemplo, por adultos) incluso dentro de la misma jurisdicción.[8]

Algunos países han establecido un marco legal específico para el contenido en línea, mientras que en otras jurisdicciones los problemas de contenido en línea se abordan según los marcos generales existentes que no son específicos de Internet. Un estudio comparativo en 47 Estados miembros del Consejo de Europa (CoE, por sus siglas en inglés) encontró cuatro categorías amplias de bases legales para juzgar la legalidad del contenido en línea:

- la protección de la salud y la moral (incluido el material de abuso sexual infantil o los juegos de azar ilegales);
- la protección de la seguridad nacional, la integridad territorial o la seguridad pública (incluida la lucha contra el terrorismo);
- la protección de los derechos de propiedad intelectual; y

7 Recomendación de la Comisión de 1.3.2018 sobre las medidas para combatir efectivamente el contenido ilegal en línea, C (2018) 1177, Comisión Europea, marzo de 2018, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX-%3A32018H0334

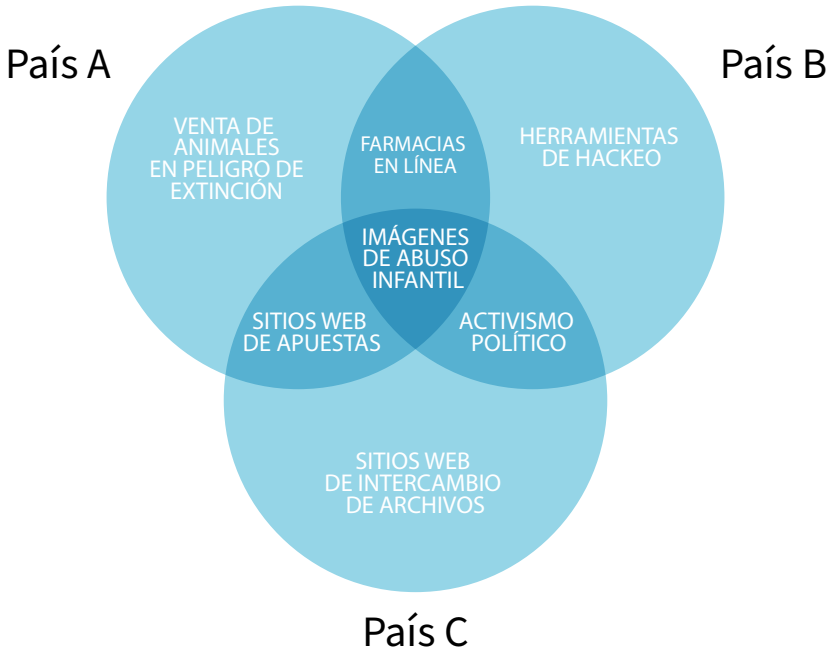
8 Perspectivas de Internet Society sobre el bloqueo de contenido en Internet: Una descripción general, Internet Society, marzo de 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

- la protección contra la difamación y el tratamiento ilegal de datos personales.[9]

¿Quién puede juzgar la legalidad del contenido?

La calificación del contenido como "ilegal" depende del marco legal local e incluso puede variar dependiendo del contexto. Si el contenido es ilegal o no es una decisión para los tribunales locales o las autoridades competentes. Además, el proceso aplicado puede variar incluso dentro de la misma jurisdicción. Algunas autoridades pueden tener el poder de juzgar la legalidad del contenido y actuar directamente a partir de esa sentencia, mientras que otras deben buscar una decisión judicial para tener la facultad de actuar sobre el contenido.

Diagrama de Venn que muestra que lo que es legal en algunos países no lo es en otros.



El editor del contenido es responsable del contenido que se hace accesible a otros usuarios de Internet. Es responsabilidad del titular del dominio que su nombre de dominio no se use para facilitar la búsqueda de contenido ilegal en Internet. Para agregar otra capa de complejidad, el proveedor y el usuario que consumen el contenido podrían no estar en la misma jurisdicción. Además, el contenido en sí podría encontrarse alojado en otra región geográfica con sus propias leyes, morales y definiciones de lo que es legal y lo que no.

Un registro de ccTLD está en la misma posición que cualquier organización o que incluso un individuo con respecto al contenido en línea. Un registro puede hacer una evaluación y formar una opinión de lo que cree que está dentro y fuera de los límites de la ley. No tiene una autoridad especial para juzgar efectivamente la legalidad del contenido que se pone en línea. Cuando un registro accede al contenido en línea, lo hace de la misma manera que cualquier persona que navega por Internet a un sitio web y carga el contenido en su computadora. No hay un acceso directo en el que un registro pueda obtener información sobre qué contenido publican los titulares del dominio. Los registros de ccTLD no alojan ningún contenido y ningún contenido pasa a través de su infraestructura.

9 Estudio comparativo sobre bloqueo, filtrado y eliminación de contenido ilegal de Internet, COE, diciembre de 2015, https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet (consultado el 7 de junio de 2018).

Algunos registros prevén la posibilidad de tomar medidas en casos obvios de contenido ilegal en los que no existen muchas dudas y los riesgos de responsabilidad son mínimos en sus términos y condiciones. En general, los registros no están equipados, no cuentan con personal o no están en una buena posición para proactivamente navegar por Internet en búsqueda de contenido ilegal.

¿Dónde se encuentra el contenido en línea?

Ubicación en Internet

Para poder acceder al contenido a través de Internet, este debe almacenarse en al menos una computadora o servidor que esté conectado a Internet. La ubicación del contenido se especifica mediante las direcciones IP únicas de los dispositivos[10] en los que está almacenado.

Localización física

Geográficamente, el o los dispositivos que contienen el contenido pueden colocarse en cualquier lugar del mundo donde haya energía y una conexión a Internet. Aparte de esto, no hay reglas o requisitos estrictos para la ubicación técnica del contenido, incluso aunque la ubicación física pueda influir en la velocidad y la calidad de la conexión.

El contenido se puede almacenar en un solo servidor o en diferentes servidores (por ejemplo, alojamiento en la nube, alojamiento en clúster). El contenido puede estar en uno o más servidores en el mismo país que el proveedor de contenido y el usuario del contenido. Estos servidores también pueden estar en cualquier parte del mundo y caer bajo las reglas de diferentes jurisdicciones.

Eliminar el contenido ilegal

La eliminación del contenido ilegal de Internet es la única solución efectiva que evita el acceso y el consumo de dicho contenido. Se puede lograr eliminando el contenido del dispositivo en el que está almacenado o desconectando este dispositivo de Internet.[11]

Contactar al editor de contenidos o al proveedor de alojamiento

Dos partes tienen acceso directo al contenido o al dispositivo que almacena el contenido: el editor del contenido y el proveedor de alojamiento. El editor del contenido tiene las herramientas y los códigos de acceso para cambiar o eliminar el contenido que ha colocado en un sitio web, que ha puesto disponible en una plataforma de redes sociales o en cualquier otro lugar. El proveedor de alojamiento puede eliminar el contenido de sus servidores o impedir efectivamente que se acceda al contenido en su infraestructura.

Se debe tener en cuenta que los proveedores de alojamiento generalmente almacenan contenido de diferentes clientes en la misma máquina física, por lo tanto, desconectar o confiscar

10 En términos técnicos, la dirección IP identifica la interfaz a través de la cual el dispositivo intercambia información, no el dispositivo en sí.

11 Se explica en el vídeo de CENTR sobre los ccTLD y los contenidos en línea: https://www.youtube.com/watch?v=kVwK-Dq-qUwY

un servidor puede afectar a diferentes proveedores de contenido y hacer que el contenido legítimo sea inaccesible. Los operadores de redes sociales y sitios de blogs pueden tener la posibilidad de eliminar publicaciones cuestionables o contenido ilegal que se publique en sus plataformas.

Contactar al titular del nombre de dominio

El titular del dominio es la primera entidad a contactar si se usa un nombre de dominio para facilitar el acceso a contenido ilegal. Podría ser que el titular del dominio sea el mismo o esté en contacto cercano con el editor del contenido. El titular del dominio puede no ser la fuente del contenido ilegal o puede no ser consciente de que su nombre de dominio se utiliza para facilitar el acceso a contenido ilegal.[12] Sin embargo, en la mayoría de los casos, el titular del nombre de dominio debe poder ayudar a identificar la fuente del contenido ilegal y a tomar medidas para eliminarlo.

El registro mantiene la base de datos autorizada con las información sobre todos los nombres de dominio registrados bajo su TLD y puede ayudar a identificar y a ponerse en contacto con el registrante. La base de datos del registro contiene, entre otra información, el titular del dominio, el registro del dominio (por ejemplo, la fecha de expiración) y las direcciones del servidor de nombres relacionado con el nombre del dominio.

Los registros de ccTLD ponen mucho esfuerzo en el mantenimiento de su base de datos y aceptan solicitudes legítimas de información. Ponerse en contacto con el registro para obtener información sobre el titular del dominio puede ser un primer paso en el proceso de eliminar efectivamente el contenido ilegal de Internet. Se puede encontrar más información al respecto en la sección III sobre las prácticas de registro actuales.

> Nota: para las autoridades podría valer la pena ponerse en contacto con los registradores ya que pueden proporcionar información útil adicional, como detalles de facturación o tarjeta de crédito, e información sobre qué otros dominios están registrados por el mismo cliente, etc.

Dificultar la localización de contenidos

Otros pasos a seguir cuando la eliminación del contenido ilegal no tiene éxito

Cuando no es posible rastrear o ponerse en contacto con el editor del contenido o el proveedor de alojamiento para eliminar el contenido ilegal de Internet - que es la única solución efectiva - se podría tratar de hacer más difícil para los usuarios encontrar o acceder al contenido. Existen diferentes métodos para bloquear el contenido de Internet, en diferentes niveles e involucrando a diferentes actores. Un informe de 2017 de Internet Society[13] describe los

12 Por ejemplo, en el caso de grandes redes universitarias o plataformas de redes sociales en las que muchos usuarios publican contenido, etc., o cuando un servidor es comprometido y es usado por criminales para alojar contenido.

13 Perspectivas de Internet Society sobre el bloqueo de contenido en Internet: Una descripción general, Internet Society, marzo de 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

métodos más actuales y evalúa qué tan bien funcionan. El documento analiza el bloqueo basado en el protocolo e IP, el bloqueo basado en inspección profunda de paquetes (deep packet inspection), el bloqueo basado en la URL, el bloqueo basado en la plataforma y el bloqueo basado en el DNS a nivel de red o ISP. El informe concluye que, independientemente del nivel y el método, "el uso del bloqueo de Internet para abordar el contenido ilegal es generalmente ineficiente, a menudo ineficaz y propenso a causar daños colaterales no intencionales a los usuarios de Internet". El bloqueo de contenido no resuelve el problema: el contenido permanece disponible y, por lo tanto, el bloqueo debe considerarse como una medida provisional en el caso de una emergencia o cuando todo lo demás haya sido probado y haya fallado.

Este documento se centra en las acciones que se toman en el registro de dominios, como cuando un registro impide que un nombre de dominio resuelva una dirección IP válida al bloquear temporalmente el nombre de dominio o al eliminarlo de la zona.

Riesgos e inconvenientes al eliminar un nombre de dominio en el registro

Bloquear o eliminar un nombre de dominio y así removerlo del DNS significa que un usuario ya no obtendrá una dirección IP válida cuando busque dicho nombre de dominio. El usuario recibirá un mensaje de error informándole que el nombre de dominio no existe en lugar de cargar el sitio web esperado.[14]

Eliminar o bloquear un nombre de dominio es una operación técnica bastante simple, pero una intervención drástica en el DNS, con el efecto de que el nombre de dominio ya no se puede usar para navegar hacia el contenido (tanto ilegal como legal) que se publica bajo dicho nombre de dominio y sus diferentes subdominios. Esta intervención también hace que todos los servicios vinculados con el nombre de dominio en cuestión, como por ejemplo el correo electrónico, dejen de funcionar. Esto suele ocurrir en un plazo de horas, pero también puede demorar algunos días debido al almacenamiento en caché.

Cualquier decisión de eliminar o bloquear debe tener en cuenta todas las consecuencias y equilibrar la prudencia con la proporcionalidad. El Reglamento de la Unión Europea sobre Cooperación para la Protección del Consumidor (en vigencia a partir de enero de 2020), por ejemplo, establece claramente que ordenar a los registros eliminar nombres de dominio solo debe considerarse "cuando no haya otros medios efectivos disponibles para lograr la cesación o la prohibición de la infracción cubierta por este Reglamento y para evitar el riesgo de daños graves a los intereses colectivos de los consumidores".[15]

Algunos ccTLD, en función de su legislación y jurisdicción local, han establecido relaciones con sus organismos nacionales de aplicación de la ley y/o empresas de seguridad acreditadas o CERT nacionales para mejorar la confianza y la seguridad en su ccTLD mediante la eliminación o desactivación expedita de los nombres de dominio que se utilizan para fines

14 Conflictos de dominio en el sistema legal, Norid, septiembre de 2017, https://www.norid.no/en/om-domenenavn/veiledere/domenekonflikter-i-rettssystemet/

15 Reglamento (UE) 2017/2394 del 12 de diciembre de 2017, que entró en vigor el 17 de enero de 2020. Art.9, 4, (g) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2394&from=EN

delictivos. Dichas relaciones generalmente se caracterizan por un entendimiento mutuo del procesamiento y los controles para garantizar que las decisiones sean justas y responsables. Las acciones que se pueden tomar dependen del marco de la política nacional de un ccTLD y de los problemas legales y de responsabilidad en torno a las notificaciones de terceros.

Los siguientes párrafos abordan algunos de los riesgos y problemas relacionados con el bloqueo o la eliminación de nombres de dominio.

Bloquear o eliminar un nombre de dominio puede dificultar la búsqueda de contenido ilegal en Internet, pero no resuelve el problema ni el delito, ya que el contenido permanece disponible para aquellos que desean encontrarlo. Además de esto, hay una serie de riesgos e inconvenientes que se tratan a continuación.

Eficacia dudosa y falsa sensación de seguridad, ya que el contenido sigue estando disponible

El bloqueo o la eliminación de un nombre de dominio no remueve el contenido ilegal de Internet. El contenido permanece disponible y se puede acceder a él directamente usando la dirección IP en lugar del nombre de dominio. Este tipo de acceso no es muy difícil; una simple búsqueda en Google devuelve amplias explicaciones y videos que describen cómo acceder a un sitio por su dirección IP. Eliminar el nombre de dominio reducirá la posibilidad de que los usuarios se enfrenten accidentalmente con el contenido ilegal, pero no detendrá a aquellos que buscan ese tipo de contenido de forma activa. “Debido a la arquitectura de Internet, los usuarios finales pueden evitar fácilmente el bloqueo por nombre de dominio y, por lo tanto, es probable que sea en gran medida ineficaz a largo plazo y cargado de consecuencias imprevistas en el corto plazo”.[16]

Además, los proveedores de contenido ilegal pueden anticipar el bloqueo y pueden tomar medidas de precaución para reducir aún más el efecto de la medida. Un proveedor de contenido, por ejemplo, puede registrar varios nombres de dominio bajo el mismo TLD o bajo diferentes TLD en diferentes jurisdicciones y permitir que todos se resuelvan en la misma dirección IP y, por lo tanto, mostrar el mismo contenido. Los hipervínculos utilizados en correos electrónicos o ubicados en plataformas o sitios web pueden vincularse directamente a la dirección IP, sin usar el DNS.

Riesgo del bloqueo masivo (overblocking) y daños colaterales.

Cuando se elimina o bloquea un nombre de dominio, se afecta a todo el contenido al que se puede acceder bajo dicho nombre de dominio y sus subdominios, incluido el contenido ilegal previsto, pero también todo el resto de los contenidos. Eliminar el nombre de dominio de una red social o sitio de blogs donde los usuarios individuales pueden publicar su propio contenido o crear su blog personal impactará a todos los usuarios, no solo aquellos que publicaron contenido ilegal, sino también a todos los que publicaron sus fotos familiares, expresaron una opinión política, a las empresas que utilizan el sitio para promoción y comercio electrónico, etc. Al bloquear un nombre de dominio, todos los servicios vinculados con dicho nombre de dominio, por ejemplo el correo electrónico, dejan de funcionar inmediatamente.

16 ‘SAC 056 - Asesoramiento del SSAC sobre los impactos del bloqueo de contenido a través del Sistema de Nombres de Dominio’, SSAC, 9 de octubre de 2012.

En un caso de estudio ficticio en “Conflictos de dominios en el sistema legal”, el registro de nombres de dominios de Noruega describe el impacto y las consecuencias del bloqueo del nombre de dominio de la Universidad de Oslo, después de que un estudiante publicara contenido ilegal en una página web bajo el dominio de la universidad17.

Riesgo de aplicación excesiva y errores fáciles de cometer

La facilidad técnica con la que se pueden bloquear los nombres de dominio aumenta el riesgo de una aplicación excesiva18. Los costos de error son bajos en el lado del ejecutor, pero, en contraste, podrían tener un impacto dramático en el lado del registrante que ve su dominio bloqueado erróneamente19, por ejemplo, una empresa que tiene bloqueado su sitio de comercio electrónico o una institución a la que ya no se puede acceder por correo electrónico.

Nota: existen otras formas de bloqueo o intervención en el DNS, por ejemplo, a nivel de ISP o del registrador. La mayoría de ellas conllevan advertencias similares y pueden ser eludidas. Ninguna medida de bloqueo es una solución integral, ya que ninguna elimina el contenido.

17 Véase Conflictos de dominio en el sistema legal, Norid, septiembre de 2017, https://www.norid.no/en/domenekonflikter/rettslig-behandling/veileder/

18 Aviso y eliminación en el Sistema de Nombres de Dominio: Tendencia ambivalente de la ICANN hacia la regulación del contenido en línea: (págs. 1379 - 1383).

19 En la siguiente publicación, se describe un ejemplo: “Orange, el principal proveedor de Internet francés, bloquea el tráfico a Google”, Alix Guillard, 27.10.2016, https://en.blog.nic.cz/2016/10/27/french-orange-blocks-traffic-to-google/

Prácticas actuales de los ccTLD

Como se mencionó anteriormente, los marcos legales locales definen qué contenido es ilegal, a quién se le ha dado la autoridad para tratar con él y qué procesos están permitidos dentro del estado de derecho. Esto puede variar de un país a otro. Además, los registros de ccTLD tienen diferentes requisitos con respecto a quién puede registrar nombres de dominio y cuáles son sus deberes. La combinación de estos requisitos y el marco legal local influye en las políticas e iniciativas que el registro desarrolla para abordar el contenido ilegal en línea.

Normalmente, estas políticas están arraigadas en la comunidad local, son compatibles con las leyes locales, abordan las necesidades locales y, con frecuencia, se han desarrollado en consulta y cooperación con otras partes interesadas locales. Las políticas y prácticas exitosas para un ccTLD podrían inspirar a otros. Sin embargo, debido a las raíces y particularidades locales, no hay garantía de que copiar el proyecto o la política conduzca al mismo resultado positivo, o que sea legal dentro de otro ccTLD.

Educación y sensibilización, con especial atención al diálogo abierto y a la cooperación con las autoridades y Agentes del cumplimiento de la ley (LEA)

Hay diferentes tipos de riesgos y peligros que enfrentan los usuarios cuando se conectan en línea (técnico, privacidad, etc.); reconocer y tratar con el contenido ilegal es uno de ellos. Varios registros de ccTLD consideran que es su deber advertir a sus comunidades sobre los peligros de Internet. Educan y proporcionan orientación sobre cómo los usuarios pueden protegerse mejor a sí mismos, cómo mitigar los riesgos o resolver problemas.

Educación y sensibilización a nivel comunitario

Los registros de ccTLD se dedican a la sensibilización y educación de sus comunidades locales de Internet para que la red sea un lugar más seguro. Los registros toman iniciativas para advertir y educar a los titulares de dominios y a la comunidad local más amplia de usuarios sobre el contenido no deseado, y para proporcionar orientación sobre cómo reaccionar. Hay una variedad de formas en que los registros informan a sus comunidades, por ejemplo, organizando reuniones o participando en talleres, dando presentaciones, discutiendo contenido ilegal en sus publicaciones, etc.

Muchos sitios web de registros contienen una página o sección sobre contenido ilegal. En ellas, se describen los problemas y peligros potenciales, se explica la política del registro, se aclara la función del registro y lo que (técnicamente) puede y no puede hacer en el caso de contenido ilegal.

El registro guiará a cualquier usuario que quiera quejarse sobre contenido en línea potencialmente ilegal a organizaciones y agencias gubernamentales especializadas en evaluar y tratar con tipos específicos de contenido en línea (por ejemplo, juegos ilegales, material de abuso sexual infantil, productos falsificados, etc.).

Ejemplos

Nic.at (.at): el sitio web del registro austríaco ofrece consejos a los usuarios sobre cómo lidiar con las actividades ilegales en Internet, así como enlaces a Stopline, la oficina nacional de denuncia contra el material de abuso sexual infantil y el nacionalsocialismo en Internet. Véase aquí y aquí.

Nominet (.uk): el registro británico ha publicado un documento sobre prácticas delictivas para explicar cómo el registro aborda la actividad criminal. Además, proporciona enlaces a una serie de autoridades con sede en el Reino Unido que pueden ayudarlo. En lugar de eliminar los nombres de dominio del archivo de zona, Nominet redirige a los usuarios de Internet a una página web educativa. Ver aquí.

Afnic (.fr): el registro francés proporciona un enlace a la plataforma dedicada a la presentación de informes del Ministerio de Asuntos Internos en donde los "contenidos de sitios web o conductas ilícitas o contrarias a la ley y al orden público" pueden ser informadas. El sitio web de Afnic también contiene un formulario que los usuarios pueden rellenar para notificar al registro los nombres de dominio ilegales.

Norid (.no): el sitio web del registro noruego proporciona un enlace al sitio web de la policía con consejos sobre cómo informar actividades ilegales en línea y el servicio de orientación slettmeg.no que ofrece consejos sobre cómo eliminar información de Internet.

DNS.PT (.pt): el registro portugués, en cooperación con otras organizaciones que se ocupan de la difusión no autorizada de contenido protegido por derechos de autor, ha desarrollado y aloja un sitio web que proporciona acceso rápido y fácil a sitios que ofrecen contenido digital que respeta los derechos de propiedad intelectual de autores y creadores. DNS.PT también publica una revista trimestral dedicada exclusivamente a la ciberseguridad con el fin de concienciar sobre las amenazas en línea.

SWITCH (.ch): el registro suizo apoya a la comunidad de Internet mediante plataformas de sensibilización sobre la seguridad y ofreciendo servicios para educar y formar a los usuarios en materia de seguridad. Ver aquí.

Los registros a veces usan sus canales de comunicación para advertir sobre los criminales que usan sitios web falsos (por ejemplo, para obtener las credenciales de un usuario para la banca o el comercio electrónico) y para demostrar cómo los usuarios pueden verificar la legitimidad de un sitio web. Por lo general, el sitio web falso se registrará bajo un TLD de un país extranjero, y el registro en sí no tiene acceso ni influencia en el nombre de dominio utilizado.

SIDN (.nl): consejos para reconocer las tiendas web falsas

Norid (.no): consejos para identificar las estafas por correo electrónico.

TRAFICOM (.fi): sitio web titulado "Proyecto de disciplina de los estafadores", que propone paquetes para identificar y reconocer las estafas digitales.

Educación y estrecha colaboración con autoridades y fuerzas del orden

Muchos registros ponen especial énfasis en sensibilizar y establecer buenas relaciones con las distintas autoridades (como las agencias de protección al consumidor o las comisiones de juego). Es importante que estas agencias y autoridades, que en muchos casos tienen la autoridad para evaluar la legalidad del contenido, entiendan cuál es la función de un registro y lo que este puede hacer para ayudarlos en casos de contenido ilegal, y a establecer buenos canales de comunicación. Esto evitará que se pierda un tiempo importante cuando le soliciten al registro que realice acciones que no están dentro de su capacidad, o cuando no dirigen sus solicitudes a la persona o al servicio que puede reaccionar adecuadamente. Las entidades de aplicación de la ley juegan un papel importante en la lucha contra el contenido ilegal en línea y, en la mayoría de los casos, deben considerarse como un primer punto de contacto para las quejas.

Es importante que las personas que trabajan en las fuerzas del orden y las autoridades relevantes tengan una buena comprensión de cómo funciona Internet y el DNS, incluida la función del registro así como las posibilidades y limitaciones de la acción al nivel del ccTLD. Algunos registros también desarrollan pautas o procedimientos para una comunicación rápida y sin complicaciones entre las agencias o autoridades específicas y el registro.

Ejemplos

NORID (.no) es el autor de una guía informativa para las fuerzas del orden, la policía y las personas que trabajan en el sistema judicial: "Conflictos de dominio en el sistema legal". El registro también, en colaboración con la autoridad de procesamiento, ha desarrollado pautas específicas sobre cómo deben proceder las fuerzas del orden al tratar el registro de un nombre de dominio. Ver aquí y aquí.

CZ.NIC (.cz) ha firmado un Memorando de Cooperación con el Departamento Checo de Actividades Especiales del Servicio de Policía Criminal e Investigación. El Memorándum tiene como objetivo aumentar la colaboración entre CZ.NIC y las autoridades policiales en lo que respecta a la prevención y localización de actividades delictivas y a la persecución de delitos, reduciendo al mismo tiempo las cargas administrativas. CZ.NIC también ha realizado una declaración conjunta con el Servicio de Policía e Investigación de la Jefatura Nacional de Lucha contra el Crimen Organizado para abordar mejor el material de abuso sexual infantil en línea, y recientemente ha firmado un Memorando de Cooperación con la Autoridad de Inspección Comercial Checa para facilitar la detección de tiendas electrónicas de riesgo.

SWITCH (.ch): En casos de procedimientos penales o administrativos, las autoridades pueden acercarse al registro con solicitudes para revocar o bloquear nombres de dominio. En colaboración con el regulador, el registro ha desarrollado pautas sobre cómo debería proceder una autoridad en tales casos y qué ámbito de acción está disponible para SWITCH cuando responde a las instrucciones de las autoridades.

Nominet (.uk), en consulta con su comunidad local de Internet, ha desarrollado un proceso de colaboración con las agencias de cumplimiento de la ley del Reino Unido. Bajo este proceso, las agencias del orden público del Reino Unido pueden presentar a Nominet

certificados formales de uso o contenido delictivo en relación con los dominios .uk, lo que llevará a su suspensión dentro de las 48 horas posteriores a la notificación al registrador y al titular del dominio. Cada año se publica un informe de criminalidad.

El registro irlandés (.ie) está trabajando en la aplicación de un acuerdo de cooperación con la autoridad policial local.

La política de DK Hostmaster (.dk) permite al registro facilitar datos sobre los registrantes a una serie de autoridades, entre las que se encuentran la policía y las autoridades judiciales, el Ministerio de Cultura, la Junta de Quejas de Nombres de Dominio, las autoridades fiscales y la inspección de datos. Ver aquí.

Los registros como proveedores de datos autorizados de nombres de dominio

Como se mencionó anteriormente, la única solución efectiva para el contenido ilegal es eliminar dicho contenido de Internet. Si un usuario u organización descubre contenido ilegal en un sitio web, una de las primeras acciones es ponerse en contacto con el titular del dominio quién puede eliminar o adaptar el contenido en cuestión.

El registro recopila datos porque debe poder identificar quién es el titular del dominio (su cliente) y poder comunicarse con él en caso de disputa, problemas técnicos, cambios en los Términos y Condiciones, pagos faltantes, etc. Los Términos y Condiciones de un registro generalmente requieren explícitamente que el titular del dominio proporcione los datos y detalles de contacto correctos al momento del registro y mantenga esta información actualizada. Proporcionar datos falsos o incorrectos es una violación de los Términos y Condiciones y puede llevar a la eliminación de un nombre de dominio.

Los registros destinan mucho tiempo y esfuerzo al mantenimiento de la base de datos. Esto no solo mejora la calidad de los datos de registro de WHOIS, sino que también puede tener un impacto positivo indirecto, ya que es poco probable que las personas con malas intenciones registren un nombre de dominio con su información personal correcta. Las acciones y prácticas para mantener una base de datos de alta calidad dependen de factores específicos del registro, como la legislación local, el tamaño del registro, la cantidad de registros procesados, etc. Algunas de estas prácticas podrían consistir en:[20]

- Evaluación de alto nivel de los datos proporcionados al registrarse para filtrar entradas obviamente falsas (por ejemplo, los solicitantes de registro llamados 'Mickey Mouse');
- Verificaciones automáticas del formato de los datos proporcionados (por ejemplo, dirección de correo electrónico, número de teléfono);
- Verificación de la documentación legal proporcionada por el solicitante del registro en países donde existe tal requisito de documentación legal;
- Verificación aleatoria de los datos de registro de nombres de dominio ya registrados (por ejemplo, el registro selecciona y verifica aleatoriamente un número de dominios por día, mes o año);

20 Estos ejemplos se basan en una encuesta de miembros de CENTR de 2017.

- Verificación de los datos en caso de reclamos;
- Verificaciones cruzadas de los datos proporcionados con las bases de datos oficiales (por ejemplo, código postal válido, número de teléfono existente, número de la compañía/organización o número de identificación nacional si se requiere dicha información al momento del registro).

Es importante tener en cuenta que muchos registros de ccTLD no tienen contacto directo con el registrante de un nombre de dominio. En este caso, todos los contactos, incluida la provisión y actualización de los datos de registro, pasan por el registrador.

Ejemplos de esfuerzos de registros para obtener y mantener datos de registro correctos:

Norid (.no) requiere que todos los titulares de dominios estén registrados en el Registro Coordinador Central Noruego para Entidades Jurídicas o en el Registro Nacional. El operador del registro .no luego verifica regularmente que los titulares del dominio aún existan de acuerdo con el Registro de Coordinación Central para Entidades Legales. Los dominios mantenidos por entidades legales que hayan sido disueltas están automáticamente programados para su eliminación.

DK Hostmaster (.dk) requiere que los registrantes de dominios daneses se identifiquen utilizando MitID, una solución de inicio de sesión utilizada por bancos daneses, sitios web gubernamentales y otras compañías privadas. Los solicitantes de registro extranjeros están sujetos a una evaluación de riesgos, que determinará si recibirán una solicitud de prueba de identidad antes del registro —riesgo alto— o dentro de los 30 días posteriores al registro —riesgo bajo— (los clientes sin riesgo no están obligados a proporcionar pruebas de identidad). Si el titular del dominio no puede o no proporciona prueba de su identidad, se eliminará su nombre de dominio. DK Hostmaster también ha introducido un formulario de contacto que permite a los usuarios informar de datos de registro incorrectos, tras lo cual el registro tiene la obligación legal de seguir examinando el caso para garantizar la exactitud de los datos. Ver aquí y aquí.

SIDN (.nl) considera que las tiendas web falsas dañan la reputación de .nl como un dominio de nivel superior sólido y seguro. Ha desplegado un sistema de detección temprana de los dominios utilizados para tiendas web falsas y examina las denuncias de las víctimas de estafas y la información recibida de la Oficina Nacional de Información sobre el Fraude en Internet. Si los datos de registro de los nombres de dominio involucrados son falsos, el registro puede desactivarlos.

SWITCH (.ch): El registro de un nombre de dominio .ch no requiere la verificación de la identidad del registrante. Sin embargo, si hay razones para creer que el registrante (a) proporciona datos de identificación falsos o utiliza ilegalmente la identidad de un tercero y (b) empleará el nombre de dominio solicitado para un fin ilícito o de manera ilícita, el registro del dominio .ch puede no activar un nombre de dominio hasta la verificación de la identidad del registrante. Este nuevo instrumento está previsto en la Ordenanza sobre Dominios de Internet y se basa en la obligación de los registrantes de nombres de dominio de identificarse correctamente. Si un registrante no se identifica correctamente en un plazo de 30 días, el nombre de dominio será revocado. Ver aquí.

Algunos registros cuentan con procedimientos especiales para informar o presentar quejas sobre datos de registro falsos:

Nominet (.uk): quejas por datos WHOIS incorrectos.

Afnic (.fr): Solicitud de verificación de la información del registrante, que conduce al bloqueo de los nombres de dominio en un plazo de 7 días.

DNSBelgium (.be): Revoke/Revoke+

Compartir datos de registro con terceros

Los registros deben respetar las regulaciones locales de privacidad cuando se comparte información sobre los titulares de dominios con terceros. La política y el procedimiento para obtener información de contacto se pueden encontrar en el sitio web del registro. Existen diferentes prácticas: algunos registros requieren solicitar la información manualmente a través de un formulario en línea, otros registros proporcionan un acceso (limitado después del GDPR) a su base de datos (a través del protocolo WHOIS), y otros registros han creado una herramienta que permite enviar un mensaje directamente al solicitante.

Ejemplos

Afnic (.fr) dispone de un formulario para solicitar la revelación de los datos personales de un particular que tenga un nombre de dominio y proporciona una interfaz que permite al tercero enviar un mensaje al registrante sin conocer su dirección de correo electrónico.

DomReg (.lt) proporciona un formulario que permite a los usuarios ponerse en contacto con los registrantes de nombres de dominio.

Norid (.no) ofrece una búsqueda limitada de dominios donde el público puede encontrar la dirección de correo electrónico de un registrante y puede encontrar información adicional sobre quién es el registrante, si se trata de una persona jurídica. Ver aquí.

DENIC (.de) admite tanto una solicitud general como un contacto de abuso por dominio para el contacto por correo electrónico con el registrante o el registrador responsable sin necesidad de compartir los datos del titular del dominio. Además, DENIC ofrece varios formularios para las agencias de aplicación de la ley y los portadores de interés legítimo con el objetivo de guiar la presentación eficiente de documentos de apoyo para la revelación de datos en pleno cumplimiento del GDPR.

Respondiendo a informes de contenido sospechoso

Respuesta a los informes externos

Algunos registros han establecido procedimientos para responder a informes de contenido sospechoso mediante el bloqueo o la suspensión de un nombre de dominio en casos específicos. Estos procedimientos generalmente tienen en común que son aplicables a casos limitados y bien definidos, y que un actor externo con experiencia en evaluación de contenido ilegal suele estar involucrado.

Un procedimiento de este tipo puede ser útil cuando la decisión de un tribunal de revocar un nombre de dominio toma un tiempo considerable. Uno de los peligros es que los reclamantes no toman conciencia del impacto limitado de la medida adoptada por el registro y dejan de emprender acciones para eliminar el contenido de Internet.

Ejemplos

SIDN (.nl) estableció un procedimiento voluntario de notificación y eliminación basado en el código de conducta nacional holandés. El procedimiento de notificación y eliminación solo puede invocarse si el reclamante puede probar que se han tomado las medidas necesarias para contactar al proveedor del contenido, al administrador del sitio web, al registrante y al registrador del nombre de dominio (teniendo en cuenta que estos terceros tienen la capacidad de resolver efectivamente el problema y eliminar el contenido). Solo en casos inequívocos e ilegales, SIDN puede decidir (temporalmente) eliminar los servidores de nombres para un dominio.

SWITCH (.ch): La Ordenanza sobre Dominios de Internet (OID) prevé el bloqueo de un nombre de dominio si hay razones para creer que el nombre de dominio en cuestión se está utilizando para (a) acceder a datos críticos por métodos ilegales (b) distribuir o utilizar software malicioso; o (c) apoyar uno de los actos mencionados. Si se cumplen los criterios de la OID, los organismos reconocidos por la Oficina Federal de Comunicaciones (OFCOM) pueden solicitar la suspensión del nombre de dominio por un periodo limitado de 30 días. Si no se toman medidas adicionales después de 30 días, la suspensión debe ser levantada. Ver aquí.

DNS Belgium (.be) ha puesto en marcha un procedimiento de Aviso y Acción en colaboración con FPS Economy. Esto implica que, tras los informes de infracciones graves de FPS Economy, DNS Belgium hace que los dominios .be correspondientes sean inaccesibles anulando los servidores de nombres y redirigiendo a los usuarios a una página de advertencia. Si los titulares de los nombres de dominio no pueden demostrar que son de buena fe, los nombres de dominio se eliminan. Ver aquí y aquí.

EURid (.eu, .ею, .ευ) colabora con diversas organizaciones e instituciones cuyo objetivo es luchar contra la ciberdelincuencia (falsificación de productos, piratería, phishing, etc.). Estas colaboraciones ayudan a depurar la base de datos de registro de EURid de nombres de dominio fraudulentos y a establecer un espacio de dominio más seguro para los usuarios de Internet.

TRAFICOM (.fi): el artículo 172 de la Ley de Servicios de Comunicación Electrónica otorga a TRAFICOM el derecho de tomar las medidas necesarias para detectar, prevenir, investigar y comprometerse a realizar investigaciones preliminares de cualquier violación significativa de la seguridad de la información dirigida a las redes o servicios públicos de comunicaciones que utilicen nombres de dominio de código .fi o a sus titulares. Las medidas necesarias pueden ser acciones dirigidas a los datos del servidor raíz de nombres .fi y pueden incluir lo siguiente: 1) prevenir y restringir el tráfico al nombre de dominio; 2) redireccionar el tráfico al nombre de dominio hacia otra dirección de nombre de dominio; y 3) cualquier otra medida técnica comparable en el sentido de las subsecciones 1-2. El

registro puede eliminar un dominio si la información del titular del nombre de dominio no es correcta, no está actualizada y no es identificable, y el titular del nombre de dominio no ha corregido o complementado los datos, a pesar de una solicitud, si un tribunal de justicia ha prohibido el uso del dominio o si la Autoridad Finlandesa de Competencia y Consumo o las Autoridades de Vigilancia del Mercado han tomado la decisión de eliminar el dominio.

Detección de actividades ilegales con medidas adicionales

Para apoyar una mayor protección y seguridad de los consumidores en línea, algunos registros han desarrollado herramientas y/o procesos automatizados para ayudar a identificar actividades ilegales o abusos en línea. Estas prácticas van desde el escaneo regular de los nombres de dominio para identificar fraude, hasta algoritmos técnicos destinados a detectar intentos de phishing.

Ejemplos

SIDN Labs (.nl) ha desarrollado DMAP, un rastreador que escanea mensualmente todos los dominios .nl, entre otros, en busca de características asociadas al fraude para identificar actividades ilegales (por ejemplo, tiendas web falsas). Ver aquí y aquí.

EURid (.eu, .ею, .ευ) ha desarrollado un mecanismo de prevención de abusos denominado APEWS que predice los registros maliciosos, es decir, si un nombre de dominio podría utilizarse potencialmente con fines abusivos. Si APEWS detecta que un nombre de dominio registrado podría estar relacionado con un abuso, retrasará su delegación en el archivo de la zona .eu. A continuación, EURid revisará estos nombres de dominio y posiblemente pedirá a los titulares que confirmen sus datos de registro antes de decidir si el nombre de dominio debe ser delegado al archivo de zona .eu o suspendido. Ver aquí.

Nominet (.uk) ha desarrollado un sistema antiphishing denominado Domain Watch que identifica y suspende los dominios que realizan intentos de phishing mediante algoritmos técnicos e intervención manual. Si se suspende un dominio, se informa a los registradores y a los titulares por correo electrónico. El dominio se desbloquea si el registrante puede confirmar el uso legítimo del nombre de dominio.

Conclusión

El contenido abusivo e ilegal disminuye la confianza en Internet. Los marcos legales locales definen qué contenido es ilegal y quién tiene la autoridad para tratar con él dentro del estado de derecho. Esto puede variar de un país a otro.

Eliminar contenido ilegal de Internet es la única solución efectiva que evita que se acceda y se consuma. El editor de contenido y el proveedor de alojamiento tienen acceso directo al contenido o al dispositivo que lo almacena. Los registros de ccTLD no tienen acceso al contenido y tampoco alojan o transfieren contenido a través de su infraestructura.

Los registros de ccTLD se comprometen a contribuir a un enfoque integral y eficaz contra el contenido ilegal en línea y desarrollarán políticas e iniciativas en este sentido, como por ejemplo:

- sensibilizar y educar a sus comunidades sobre los peligros de Internet,
- facilitar la cooperación con las agencias del orden y autoridades,
- proporcionar datos de registro sobre nombres de dominio sospechosos,
- responder a los informes de nombres de dominio utilizados para facilitar el acceso a contenido sospechoso en el marco de la jurisdicción local;
- o ayudar a identificar actividades ilegales de forma voluntaria.

Las políticas y prácticas exitosas presentadas en el documento podrían inspirar a otros ccTLD. Sin embargo, debido a las particularidades locales, no hay garantía de que copiar un proyecto o una política conduzca al mismo resultado positivo o, de hecho, sea legal dentro de otro ccTLD.

Council of European National
Top-Level Domain Registries

Sobre CENTR

CENTR es la asociación de registros de dominio de nivel superior con código de país europeo (ccTLD), como .de para Alemania o .si para Eslovenia. Actualmente, CENTR cuenta con 52 miembros plenos y 9 miembros asociados; juntos, son responsables de más del 80% de todos los nombres de dominio registrados en todo el mundo.

Los objetivos de CENTR son promover y participar en el desarrollo de altos estándares y mejores prácticas entre los registros de ccTLD.

CONTACTO

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

SÍGANOS

Para mantenerse informado de las actividades y de las publicaciones de CENTR, síganos en Twitter y LinkedIn.

Publicado el 13 de mayo de 2022