



GUÍA

ASPECTOS LEGALES PRÁCTICOS DE LA UTILIZACIÓN DE TOR Y OPERACIÓN Y USO DE HERRAMIENTAS DE PRIVACIDAD Y ANONIMATO

ARGENTINA

DRA. JOHANNA CATERINA FALIERO
DR. RODRIGO SEBASTIAN IGLESIAS

GUÍA

ASPECTOS LEGALES PRÁCTICOS DE LA UTILIZACIÓN DE TOR Y OPERACIÓN Y USO DE HERRAMIENTAS DE PRIVACIDAD Y ANONIMATO

DRA. JOHANNA CATERINA FALIERO
DR. RODRIGO SEBASTIAN IGLESIAS



Esta publicación está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY 4.0):
<https://creativecommons.org/licenses/by/4.0/deed.e>

Portada y diagramación: Javiera Méndez
Correcciones por Sebastian Alburquerque
Noviembre de 2018.

Esta publicación fue posible gracias al apoyo de Open Technology Fund



Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción de la libertad de expresión, el acceso a la cultura y la privacidad.

Índice

Guía de aspectos legales prácticos de la operación y uso de tor y herramientas de privacidad y anonimato en argentina	3
Estado de la regulación legal a nivel local: ¿qué nos ampara para el uso de tor y otras herramientas de privacidad y anonimato?	3
¿Qué utilidades tienen las herramientas de privacidad y anonimato como tor?	3
Frente a la operación y utilización de herramientas de privacidad y anonimato tales como tor, ¿qué posibles implicancias y respuestas enfrentamos ante solicitudes legales?	4
¿Qué límites en materia de investigación judicial existen cuando se cuestiona el uso de herramientas tales como tor?	5

Guía de aspectos legales prácticos de la operación y uso de tor y herramientas de privacidad y anonimato en argentina

Estado de la regulación legal a nivel local: ¿qué nos ampara para el uso de Tor y otras herramientas de privacidad y anonimato?

En nuestro país podemos afirmar con certeza que resulta legal la utilización de herramientas de privacidad y anonimato, ya que estas cuentan con la protección de leyes de varios tipos (desde la Constitución Nacional, Tratados de Derechos Humanos, y Leyes).

En Argentina son reconocidos a nivel constitucional y legal extendido los derechos humanos y fundamentales a la intimidad, privacidad, protección de datos, autodeterminación informativa, confidencialidad, reserva, entre otros.

Esto nos permite reflexionar respecto de la enorme utilidad que representan las herramientas de privacidad y anonimato, tales como Tor, respecto de la defensa de estos derechos y el empoderamiento ciudadano a través de su ejercicio práctico.

Los referentes más salientes doctrinarios en Delitos Informáticos han establecido que la utilización de herramientas de privacidad y anonimato como Tor son lícitas y se encuentran incluidas en el marco jurídico argentino que hemos mencionado.

Como no hay una prohibición legal específica, y todo aquello que no se encuentra expresamente prohibido está permitido, la utilización de técnicas de anonimato, privacidad, seudonimia o cifrado, se encuentra permitida y es legal.

¿Qué utilidades tienen las herramientas de privacidad y anonimato como Tor?

La utilización de herramientas de privacidad y anonimato, tales como Tor, permiten el robustecimiento y empoderamiento ciudadano a través del fortalecimiento democrático que permiten. Contribuyen a la libre circulación de las ideas, y como metodología, permite evitar las maniobras de censura previa que atentan contra los derechos que debemos gozar todos los ciudadanos.

En la actualidad, el uso de estas herramientas está en franco crecimiento, tanto en entornos de privacidad (por necesidad operativa), como por aquellos usuarios conscientes y rigurosos respecto de su privacidad y la protección de sus datos.

Las herramientas de privacidad y anonimato son una muy efectiva barrera técnica natural de defensa frente a los abusos característicos de la industria moderna privativa empresarial en materia de propiedad intelectual, respecto de la libre circulación del conocimiento y la cultura, y lo que ello significa para la educación y capacitación de las personas.

Tanto estas como otras utilidades caracterizan el uso de Tor y demás herramientas de privacidad y anonimato, por lo que resulta necesario capacitarnos responsablemente en todos los niveles de participación y organización social, no sólo para saber cómo responder ante un requerimiento legal, sino para saber cómo defender el derecho de utilizarlas como genuinas herramientas de la democracia y la protección de nuestras libertades.

Frente a la operación y utilización de herramientas de privacidad y anonimato tales como Tor, ¿qué posibles implicancias y respuestas enfrentamos ante solicitudes legales?

La jurisprudencia estableció que ser Tor Exit Node no implica delito alguno, por más que la dirección IP sea la misma desde la cual se realizó un hecho ilícito, ni penal o civilmente.

Esto, dicho en otros términos más simples, implica afirmar que ser un nodo de salida de Tor no es ilícito en nuestro ordenamiento, más allá de que en el marco de un proceso judicial pueda verse sometida su utilización al escrutinio legal.

Entonces, si no tiene responsabilidad alguna un Tor Exit Node, cabe repreguntarnos por qué se los imputa de delitos, realiza allanamientos y se le secuestran equipos.

Esto es así porque el formato habitual de investigación en procesos penales es, en términos generales, identificar una dirección IP como si fuera una dirección de domicilio físico y se interpreta por lo tanto este hecho de forma errónea.

Así mismo, otros defectos forenses y de investigación tales como no utilizar los mismos servicios de Tor como Exonerator, que permite saber si se encuentra en funcionamiento o no el nodo, conlleva aún más confusiones innecesarias en torno a la temática. Esto genera gastos innecesarios, procesos judiciales absurdos y por sobre todo, la consecuencia fatal de la falta de investigación de delitos graves de forma efectiva y coherente.

¿Qué recomendamos? Para ser Tor Exit Node, y a los fines de evitar estos inconvenientes ante solicitudes legales, es preferible disponer para ello de una dirección IP distinta del resto de los equipos de trabajo o del hogar. En lo posible, bajo un domicilio físico distinto, para evitar la identificación y analogía que explicábamos de domicilio físico con IP, e identificar de forma correcta a los equipos utilizados para brindar una adecuada colaboración a la hora de responder a estos requerimientos procesales.

¿Qué límites en materia de investigación judicial existen cuando se cuestiona el uso de herramientas tales como Tor?

En lo que respecta a la investigación forense a nivel local, el monitoreo de Tor Exit Nodes solo puede efectuarse sujeto a orden judicial de autoridad competente, como máximo por el plazo de 45 días, mientras que, por el contrario, su obtención fuera de estos parámetros deviene ilícita.

Asimismo hay que destacar que la prueba obtenida bajo la figura de un agente encubierto anonimizado puede ser realizada bajo la utilización de Tor bajo las condiciones de legalidad descritas, dentro un proceso judicial que lo solicite particularmente.

A nivel jurisdiccional se observa de manera generalizada una falta grave de preparación para la contemplación de casos en los que estas herramientas hayan sido utilizadas, lo que compromete el servicio de justicia.

Es por eso que resulta sumamente importante que se preserve el respeto de estos límites de legalidad en investigación y se fomente la capacitación institucional, a nivel nacional, en estas temáticas, para que en materia de investigación los cuestionamientos judiciales no terminen por afectar injustamente a los usuarios de estas herramientas, ni someterlos a riesgos innecesarios e injustificados.

