Privacidad y anonimato para un manejo seguro de mi información en redes.

Imparten:

Ma. de Lourdes Reséndiz Martínez
Diego Alberto Barriga Martínez
Marco Antonio Ruano Muñoz
Oscar Emilio Cabrera López

Coordina:

Gunnar Eyal Wolf Iszaevich

Proyecto UNAM/DGAPA/PAPIME PE102718
Desarrollo de materiales didácticos para los mecanismos de privacidad y anonimato en redes

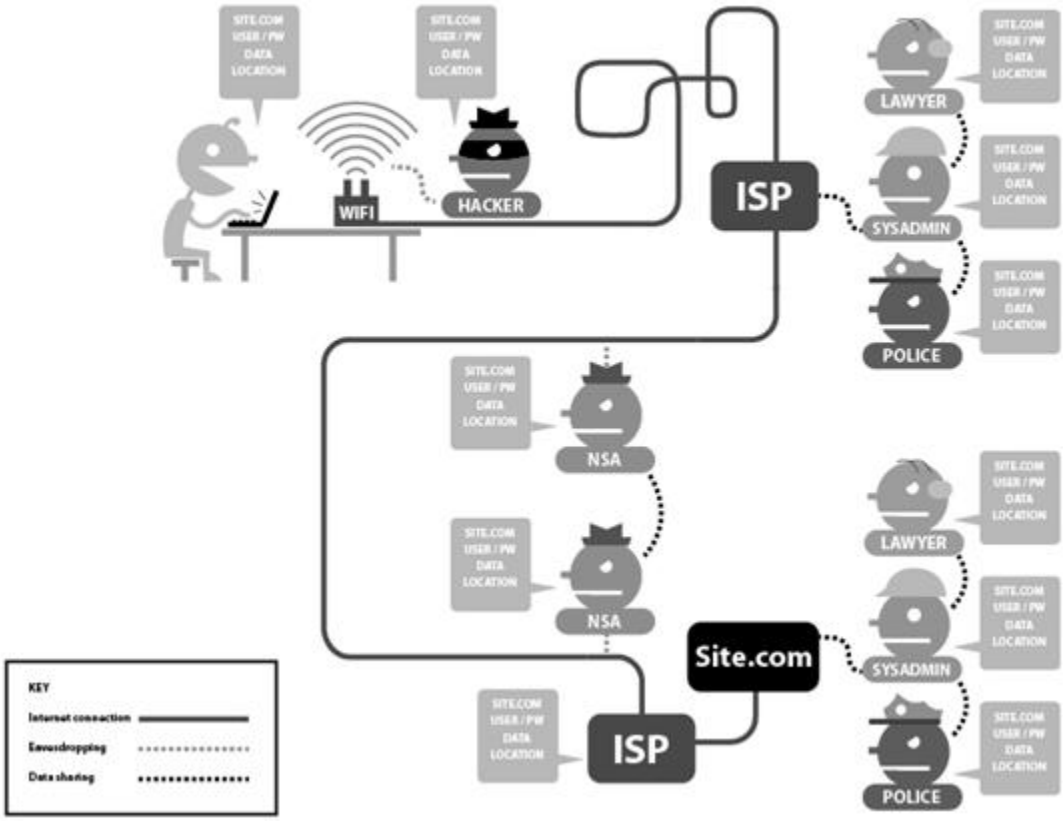
Contenido esquemático general del curso

1. Introducción al curso.
    1. Buenas prácticas en el uso de recursos digitales para la investigación científica.
    2. Demostración: ¿Qué información nuestra podemos encontrar en línea?
    3. Casos de uso para profesionales de las ciencias políticas y sociales.
2. Descubriendo errores, malas prácticas y situación en México
    1. Privacidad y Anonimato
    2. ¿Qué es internet?
    3. Internet en México
    4. Vigilancia y censura.
3. Corrigiendo los errores y buenas prácticas
    1. Buenas prácticas.
    2. Herramientas y utilidades.
4. The Onion Router
    1. ¿Qué es Tor?
    2. Instalación
    3. Configuración
    4. Demostración
5. Conclusión.
    1. Desarrollo tecnológico de Tor.
    2. Involúcrate.
    3. Presentación de material multimedia “Internet, la vida privada y otras historias de paquetes”

Internet

¿Sabes cómo funciona? ¿Qué personas y entidades se encargan de que nos podamos comunicar en línea y a qué tipo de información tienen acceso?

En el siguiente gráfico, puedes observar el proceso simplificado que sigue tu información (así como quiénes podrían mirarla) cuando visitas páginas web cuyas direcciones no comienzan con las letras 'https'.[1]



El diagrama que aquí reproducimos fue ideado por la *Electronic Frontier Foundation* para ilustrar la forma en que distintas formas de acceso a la

1 https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto

red ayudan a proteger diferentes detalles de nuestra conexión; para ver el diagrama de forma interactiva, sugerimos visitar su sitio Web.[2]

Muchos sitios recolectan información de distintas formas, aún cuando estos sean “gratuitos”. Por ejemplo, cuando inicias sesión en tu cuenta tras haber proporcionado datos –como podrían ser, tu nombre real, domicilio, email, género, edad, etc.– formas parte de una serie de estadísticas que, después de ser analizadas, revelan tus patrones de actividad. Con lo anterior, los sitios buscan ofrecerte productos y servicios basándose en tu actividad y la de personas con hábitos similares.

Sin embargo, aún cuando navegamos por ciertas páginas sin habernos identificado, es posible ser rastreados por terceros –una práctica común en sitios donde hay secciones de publicidad– ya que estos suelen emplear *cookies*, las cuales almacenan cierta información en tu dispositivo y esta es utilizada para recordar la actividad de una persona, por ejemplo: desplegar anuncios relacionados con productos que hayas visitado, los clics que hayas hecho en ciertos botones e incluso páginas anteriores que hayas visitado.[3]

Al igual que otros elementos, las cookies tienen como objetivo ‘simplificar’ tu experiencia al navegar –por ejemplo, *recordando* lo que hayas ingresado en campos de texto donde se solicita tu nombre, contraseñas, números de tarjetas de crédito, etc– pero también es posible desactivarlas o limitarlas en algunos casos si tu no deseas que tu información sea utilizada por terceros.

Para una explicación más elaborada sobre cómo funciona internet te recomendamos el documento *«¿Cómo funciona Internet?»*, editado por Mozilla.[4]

2 https://www.eff.org/es/pages/tor-and-https

3 https://en.wikipedia.org/wiki/HTTP_cookie

4 https://developer.mozilla.org/en-US/docs/Learn/Common_questions/How_does_the_Internet_work

Internet en México

México fue un país de vanguardia en temas de Internet y tecnologías de la información. Recordemos que en 1958 la Universidad Nacional Autónoma de México adquirió e instaló, en la Facultad de Ciencias, la computadora IBM-650. Esta computadora fue la primera en América Latina colocando a la UNAM como un eje importante para el desarrollo de la computación en México.[5] Para 1989, el primer nodo de Internet de nuestro país (en el Instituto de Astronomía de la UNAM) inició operaciones.[6]

Sin embargo, tener una computadora en nuestro país desde hace poco más de 60 años no nos hace una potencia tecnológica. Muchos actores que toman decisiones en este país se ven maravillados y tienden a creer que existe cierta magia en los dispositivos tecnológicos. Como menciona Claudio Ruiz, director ejecutivo de Derechos Digitales: “Es como si ciertas características ocultas permitieran de manera automática la mejora de las condiciones materiales de nuestra sociedad y su sola adopción nos acelerara en el camino del desarrollo”.[7]

Actualmente, las plataformas digitales nos permiten organizarnos mejor que nunca, amplificar nuestra voz y tener impacto significativo en una mayor audiencia. Esto supone condiciones únicas para el desarrollo de la libertad de expresión, información, asociación, auto-aprendizaje, democratización del conocimiento y más. Pero, a la vez estas tecnologías propician el espionaje gubernamental, la censura a gran escala, la enajenación de masas, discriminación y violencias de género a escalas sin precedentes.

La complejidad política, la seria crisis de derechos humanos y los constantes cuestionamientos institucionales por parte de la sociedad civil ameritan un análisis serio, que abone al debate democrático, pensando en las oportunidades que entrega internet para el ejercicio de los derechos humanos desde el contexto local, menciona Ruiz.

5 http://www.fundacionunam.org.mx/donde-paso/festeja-unam-60-anos-de-la-primera-computadora-en-mexico-y-en-america-latina/

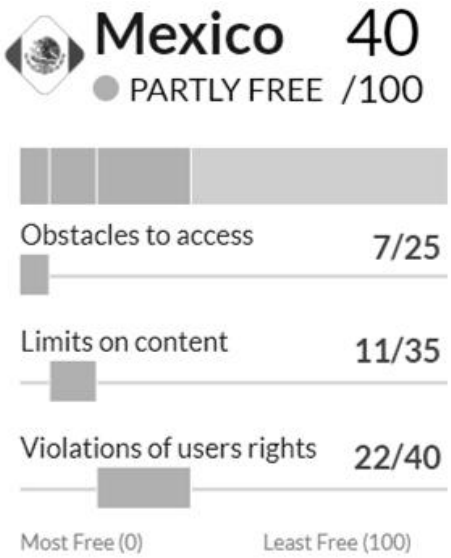
6 https://www.fis.unam.mx/~gloria/g.koenigsberger_inicios_internet_libro.pdf

7 https://www.derechosdigitales.org/wp-content/uploads/Internet-en-Mx-2016.pdf

Por estas razones y otras, que se abordarán en este curso, es importante ser plenamente conscientes del papel que desempeñamos en Internet. Es necesario tener ciertas nociones de cómo funciona Internet dado que ha permeado en nuestras vidas cotidianas de formas inimaginable. Por último, conviene esclarecer ¿Qué es nuestra huella digital en Internet?, ¿Qué datos entregamos?, ¿A quienes se los entregamos?, ¿Cómo esta práctica nos hace vulnerables? y ¿Qué alternativas libres existen y están a nuestro alcance para disminuir dicha vulnerabilidad?

Libertad en la red de México.

De acuerdo con el reporte de la “Freedom House” de 2018, México es catalogado como un país parcialmente libre en la red de acuerdo con puntajes establecidos en las categorías de obstáculos de acceso, limitación de contenido y violación de los derechos de usuarios y usuarias.[8]



El puntaje de 40/100 (menor puntaje representa mayor libertad) asignado a México es consistente con respecto a años anteriores ya que se ha reducido la brecha digital y promocionado la competición en el sector de Tecnologías de Información y Comunicaciones (ICT por sus siglas en inglés); grupos de derechos digitales alertaron acerca de cambios en la Ley Federal de Derechos de Autor que permitirían a las cortes censurar

8 https://freedomhouse.org/report/freedom-net/2018/mexico

contenido en línea e incautar equipamiento sin la necesidad de pruebas de que una violación de derechos de autor se haya llevado a cabo; y por otro lado un gran uso de *bots* y cuentas falsas estuvo presente durante el periodo de elecciones de 2018 impactando la desinformación en redes sociales; además de las revelaciones sobre tecnologías digitales para espiar a periodistas, abogados de derechos humanos, activistas y figuras políticas.[9]

¿Por qué resulta de interés para los participantes objetivo de este curso, miembros de la Facultad de Ciencias Políticas y Sociales?

Porque personas que ejercen el periodismo en México han sufrido agresiones tales como la “intimidación y el hostigamiento, la amenaza, el bloqueo o remoción de información, el ataque físico o material, y la privación de la libertad del comunicador”. No es secreto que nuestro país es uno de los lugares más peligrosos para desempeñar dicha profesión; particularmente durante el sexenio del expresidente Enrique Peña Nieto, México encabezó la lista, no únicamente con respecto a Latinoamérica, sino que a escala mundial.[10]

Y, por supuesto, la violencia de género también se hace presente: “En una encuesta hecha en 2017 por la Federación Internacional de Periodistas (FIP) entre casi 400 periodistas de 50 países, 48 % de mujeres dijeron haber sufrido alguna forma de violencia de género en su trabajo.”[11] México ha visto también un alarmante aumento en las agresiones de género de toda naturaleza.

De ninguna manera intentamos desalentar el ejercicio de sus profesiones infundiendo miedo, sin embargo, es muy importante entender el contexto en el que nos encontramos para darle la importancia necesaria a proteger nuestra información y tratar con sumo cuidado nuestra identidad digital. Cada uno de nosotros representa un perfil muy específico de usuario, y debe realizar una evaluación de riesgos relacionados con éste — Con sus características ocupacionales, personales, y demás.

9 https://freedomhouse.org/article/libertad-en-la-red-2018-el-auge-del-autoritarismo-digital

10 https://www.animalpolitico.com/2019/04/periodistas-asesinados-mexico/

11 https://www.animalpolitico.com/2019/03/violencia-mujeres-periodistas-cidh/

En junio de 2019 se anunció que Estados Unidos solicitará información relativa a las cuentas en redes sociales, inclusive respecto a actividad no-pública (mensajes privados, contactos, etc.) a quien solicite visa de ingreso, así sea como turista, lo cual potencialmente se convierte en un gran problema, pues "los usuarios podrán preocuparse de forma justificada de que su voz en línea pueda afectar el resultado de sus solicitudes para una visa, lo cual les puede llevar a la autocensura".[12]

Herramientas

Presentamos a continuación algunas herramientas que pueden ayudar a mantener un mejor control de la información personal en las actividades en línea. La lista que presentamos no es definitiva ni exhaustiva, y no presenta soluciones "mágicas" — No deja de ser responsabilidad de cada usuario comprender los principios del funcionamiento, alcances y limitaciones de las herramientas que emplea.

Las herramientas y prácticas aquí mostradas y durante el curso, son algunas de las que recomendamos, conocemos y hemos usado, sin embargo, un compromiso que debemos seguir al usar navegadores, aplicaciones, y todo tipo de *software* es mantenernos al día, ya que constantemente hay nuevas versiones o alternativas de programas a utilizar, al igual que sistemas que dejan de actualizarse y representan un riesgo potencial a tu seguridad.

Navegación "privada" (o Modo *incógnito*)

Seguramente has escuchado estos términos en uno u otro navegador, pero ¿Sabes exactamente qué es lo que hacen? ¿Cuándo es conveniente usarlos, y cuándo no?

El modo incógnito forma parte de los navegadores más populares como Chrome, Firefox, Edge, Safari, Opera, entre

12 https://freedomhouse.org/article/united-states-monitoring-social-media-accounts-visa-applicants-sets-dangerous-precedent

otros y tiene como objetivo permitir al usuario navegar sin que se guarde cierta información como búsquedas, contraseñas, historial y *cookies*.

Sin embargo, la navegación privada **no otorga privacidad en Internet en absoluto.** Lo único hace es *limitar* los datos que se almacenan en *nuestra* computadora. Las interacciones que tengamos con los sitios web seguirán habilitadas.

En conclusión, La navegación privada protege contra personas que esten espiando en el historial de tu navegador y, en algunos casos, evita que sitios web te rastreen a través de *cookies* almacenadas en tu PC. En otras palabras, este modo ayuda a protegerse contra personas que husmean en tu navegación web **después** de que ocurrió, pero no te protege de personas, o empresas, que estén espiando **mientras** navegas, esto es, no protege a tu identidad (o fragmentos de ella) de ser revelados a los sitios que estás utilizando, directa o indirectamente.

DuckDuckGo — https://duckduckgo.com/

Es probable que al navegar por internet utilices el motor de búsqueda *Google*, a pesar de que existen alternativas que se preocupan por no recolectar información tuya o “aprender” de tus búsquedas. Uno de ellos es *Duckduckgo*, el cual brinda la capacidad de hacer búsquedas anónimas, sin almacenamiento de tus datos personales y sin rastreo a través de los sitios que visitas.

Data Detox — https://datadetoxkit.org/en/home

En algunos países se han implementado algunas leyes para intentar proteger la información de usuarios y usuarias, por lo que muchos servicios ahora están obligados a actualizar sus políticas de privacidad y retención de información. En consecuencia, algunas de las prácticas que utilizan para recabar tus datos son opcionales para ti. Así que, otra buena práctica es revisar la configuración ‘de fábrica’ que incluyen los programas que utilizas tanto en computadoras como dispositivos móviles.

En ese sentido, una buena guía para revisar y seguir es *Data Detox*. En esta página se nos muestran diferentes recomendaciones, test, información útil y pasos a seguir para desintoxicar nuestra huella digital.

Privacy Badger — https://www.eff.org/privacybadger

Privacy Badger es una extensión que se instala en los navegadores web, y detiene anunciantes y rastreadores de terceros que de **forma secreta rastrean** a que páginas vas y qué páginas miras en la web. Si algún anunciante te rastrea a través de múltiples *websites* sin tu consentimiento, *Privacy Badger* automáticamente bloqueará dichos anunciantes evitando que carguen cualquier contenido en tu navegador. Para el anunciante, es como si desaparecieras.

uBlock Origin — https://github.com/gorhill/uBlock

uBlock Origin es una extensión de navegadores web. *uBlock Origin* no es sólo un "*ad blocker*" (bloqueador de anuncios), sino que es un bloqueador de *amplio espectro*. El comportamiento básico de la extensión cuando es instalada en un navegador es la de bloquear anuncios, rastreadores y sitios maliciosos.

Ghostery — https://www.ghostery.com/

Ghostery es una extensión de navegador que permite gestionar los rastreadores de los sitios web para disfrutar de una experiencia en Internet más transparente, rápida y segura.

HTTPS Everywhere — https://www.eff.org/https-everywhere/faq

HTTPS Everywhere es una extensión de navegadores que cifra las comunicaciones de la mayor parte de los sitios web, haciendo la navegación más segura. La extensión habilita la protección HTTPS de los sitios en las que no está habilitado por omisión,

pero que sí la soportan. Idealmente, esto proporciona cierta protección contra ataques maliciosos.

Sobre el anonimato

El anonimato es, en esencia, la condición de una persona o grupo de personas que ocultan su identidad, o aspectos de ella. En el contexto actual, donde proliferan las redes sociales y la posibilidad de expresar una opinión, se manifiestan cuestionamientos y preocupaciones respecto a esta condición. Se ha alegado que el anonimato fomenta actividades criminales, que suaviza la responsabilidad sobre los discursos emitidos, que vulnera la seguridad del resto de las usuarias, entre otras.

Para empezar, conviene ver a lo que llamamos Internet con dos perspectivas. Por una parte, está la infraestructura que es el conjunto de cables, routers, switches, protocolos y servidores, que son la parte estrictamente física y tangible de Internet. Por otra, las interacciones entre personas que se sucita empleando dicha infraestructura.

Las diferentes personas usuarias de las redes envían información codificada en *paquetes de datos* de un punto a otro sin que se conozca la naturaleza de los mismos, sea estos correos, fotos, videos o canciones, a lo largo de la red. Esta forma de transmitir información define al protocolo de Internet (*Internet Protocol, IP*) y es lo que ha permitido su crecimiento como vía para la comunicación. La no discriminación de datos por su tipo es lo que se conoce como *neutralidad de la red*. En consecuencia, puede comprenderse que los datos transmitidos sobre una red neutra son anónimos.

Después, se debe tomar en cuenta que, además de las personas usuarias y los medios físicos, también están presentes como actores los Estados y las empresas privadas, cada cual con sus propios intereses. Todos estos elementos, físicos, humanos, legales, sociales y políticos, generan tensión respecto al anonimato en la red.

El derecho a ser anónimo es una consecuencia del desarrollo de la libertad de expresión. Las personas tienen derecho a la plena voluntad de expresar y revelar su identidad para establecer contacto con su entorno y, así,

comunicar ideas o acceder a información. El anonimato es una protección contra posibles abusos y la revelación de identidad en la red puede afecta a grupos vulnerables o que ejercen opiniones incómodas hacia individuos con poder. Por ejemplo activistas, periodistas, defensores de derechos humanos, entre otros.

En ese sentido, existe un desequilibrio de poder, se equilibra cuando está del lado de los vulnerables y se acentúa cuando es empleado por las figuras de poder. El anonimato es especialmente importante a la hora de asegurar la voz de los excluidos. La demanda por parte de empresas y estados de nuestras identidades reales es un abuso de poder, dado que, vulneran los derechos de las minorías de expresarse libremente y el derecho a la privacidad de los datos de las personas. Entre más expuestos estamos, más probable serán las prácticas de vigilancia masiva — prácticas en que México ha demostrado interés y desarrollo.

Las desigualdades de acceso a voz pública por cuestiones políticas, raciales, de clase o género, se replican y magnifican en la red. Es hora de dejar de pensar que el anonimato es la capa que cubre lo ilícito y considerarlo como el escudo que protege y garantiza el ejercicio de la libertad de expresión.

Tor

Es una tecnología conformada por una serie de herramientas que buscan promover libertades y derechos humanos creando y desplegando tecnologías para el anonimato y privacidad de código abierto y gratuito, soportando su uso y disponibilidad sin restricciones y fomentar su comprensión científica y popular.

Particularmente el navegador Tor –que funciona usando la red Tor– permite a cualquier usuario navegar de forma anónima al redirigir los datos de forma cifrada[13] a través de 3 nodos aleatorios en todo el mundo para que el sitio a donde se intente acceder, el gobierno u otras entidades no vigilen tu actividad.

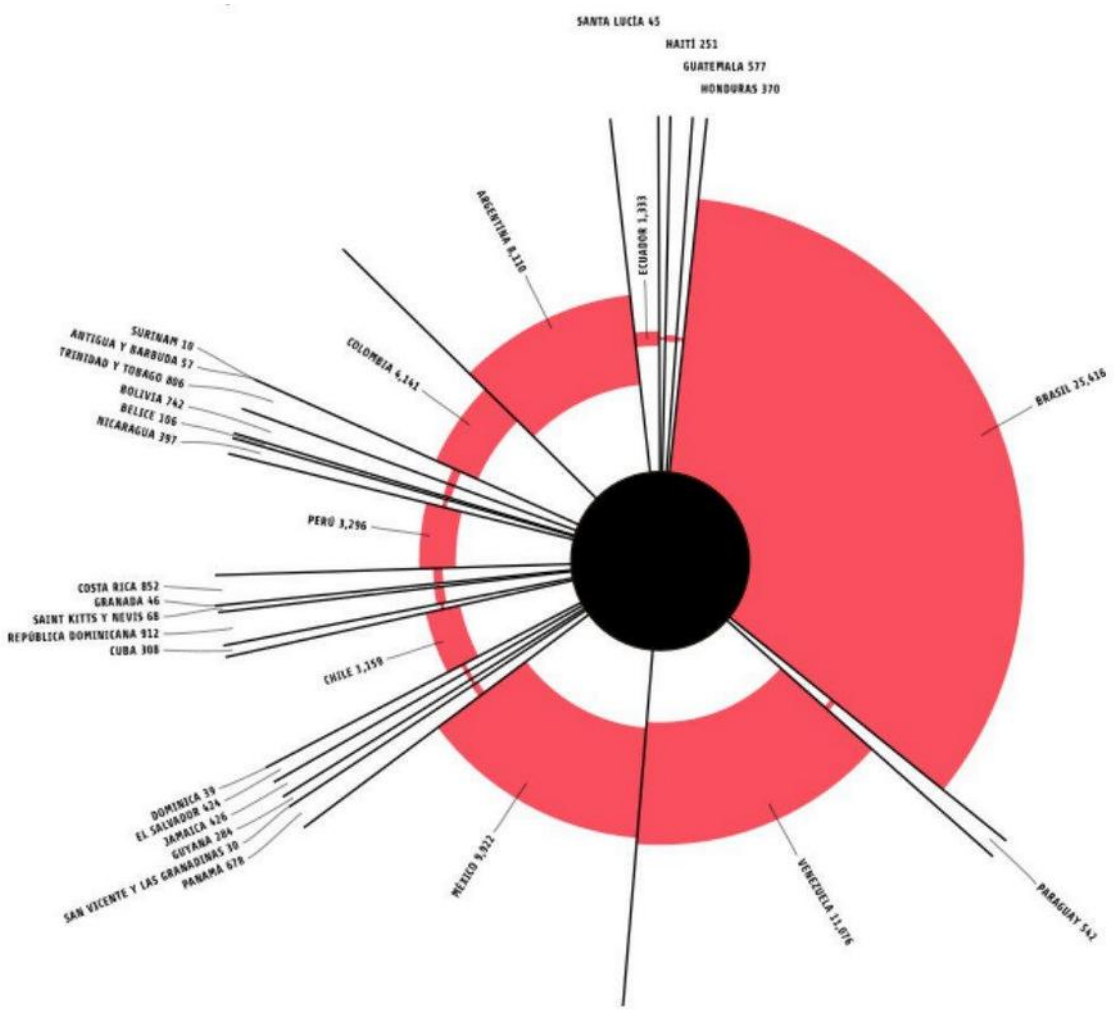
13 https://es.wikipedia.org/wiki/Cifrado_(criptografiía)

Muchas personas en el mundo utilizan y dependen de Tor, por ejemplo defensores de derechos humanos, activistas, periodistas o personas que son vigiladas.[14]

El uso de Tor es, relativamente, de gran importancia en México: Como lo muestra la figura a continuación, elaborada por Enjambre Digital[15], el nuestro es el tercer país con mayor número de usuarios diarios en Latinoamérica. Menciona el reporte referido, “las personas somos constantemente vulneradas ya que nuestro gobierno trabaja con empresas que promueven el uso de tecnologías de vigilancia masiva y las acciones directas de amedrentamiento y censura hacia periodistas y activistas. El anonimato y la navegación privada que ofrece la red Tor son alternativas valiosas para salvaguardar nuestros derechos a la libertad de expresión, acceso a la información y a la privacidad; mismos que permiten que la democracia exista dentro y fuera de las plataformas digitales.”

14 https://trac.torproject.org/projects/tor/raw-attachment/ticket/30430/02-tor-personas.pdf

15 https://tor.enjambre.net/



21

Sin embargo, a pesar de la importancia en números respecto a la región latinoamericana, hay un gran camino por recorrer para normalizar y fomentar el uso de Tor en la región — Considerando la estimación de usuarios diarios de Tor en dos millones[16], se revela que la cantidad de usuarios en la región latinoamericana no alcanza con mucho la media internacional.

16 https://metrics.torproject.org/userstats-relay-country.html

Obstáculos que enfrenta el uso de Tor

Debido a que algunos particulares, empresas o gobiernos desean tener un estado de vigilancia activo, realizan algunas acciones para evitar que la gente forme parte o haga uso de Tor. Por ejemplo, a pesar de que se puede usar Tor con los proveedores Telmex o Izzi, no es posible formar parte de los voluntarios que operan los nodos.
Por el contrario, si es posible ser voluntario si utilizas el proveedor Axtel.

Si te interesa ser parte de este proyecto o conocer más al respecto puedes visitar el sitio oficial de Tor o visitar el Laboratorio de Investigación y Desarrollo de Software Libre en el anexo de Ingeniería en el segundo piso del edificio P, donde con gusto te podremos orientar.[22]