Libro electrónico

MECANISMOS DE PRIVACIDAD Y ANONIMATO EN REDES

Una visión transdisciplinaria

Gunnar Wolf
coordinador

UNAM
La Universidad de la Nación
dgapa

MECANISMOS DE PRIVACIDAD Y ANONIMATO EN REDES. UNA VISIÓN TRANSDISCIPLINARIA

MECANISMOS DE PRIVACIDAD Y ANONIMATO EN REDES. UNA VISIÓN TRANSDISCIPLINARIA

Gunnar Wolf
coordinador

Primera edición digital en pdf, septiembre de 2021

Ciudad Universitaria, Coyoacán,
04510, Ciudad de México.
INSTITUTO DE INVESTIGACIONES ECONÓMICAS
Circuito Mario de la Cueva s/n
Ciudad de la Investigación en Humanidades
04510, Ciudad de México.

ISBN: 978-607-30-5073-9
DOI: https://doi.org/10.22201/iiec.9786073050739e.2021

Proyecto: "Desarrollo de materiales didácticos para los mecanísmos de privacidad y anonimato en redes"(UNAM/DGAPA/PAPIME PE102718)

Diseño de portada: Juan Carlos Burgoa
Corrección, cuidado de la edición y diseño de interiores: Marisol Simón

Hecho en México.

¡Copia este libro!

ÍNDICE

INTRODUCCIÓN

Gunnar Wolf

Todas nuestras actividades dejan un rastro digital. Ya en 1999 Scott McNealy, entonces presidente ejecutivo de Sun Microsystems, decía "Tienen nula privacidad, de todos modos. ¡Acéptenlo!" (Sprenger, 1999), Más que aceptarlo, tecnólogos y activistas han luchado por mantener un espacio mínimo de privacidad personal, ya sea, mediante soluciones tecnológicas que dificultan el monitoreo e identificación, impulsando regulaciones que dificulten la invasión de la esfera personal o educando con las mejores prácticas para el manejo seguro de la información.

Esta antología se desprende del proyecto "Desarrollo de materiales didácticos para los mecanismos de privacidad y anonimato en redes" (UNAM/DGAPA/PAPIME PE102718), donde buscamos comprender y analizar los riesgos a la privacidad y los mecanismos que podemos emplear para evadirlos, a nivel individual y como organizaciones. Queríamos abordarlo de una forma transdisciplinar y llevarlo a los usuarios que más riesgos corren por la invasión a su privacidad: periodistas, defensores de derechos humanos, activistas, personas sin una sólida formación tecnoló-

gica. Para escuchar la experiencia de cada uno de estos perfiles y programadores muy cercanos al desarrollo de herramientas especializadas, convocamos en 2018 al coloquio Mecanismos de Privacidad y Anonimato en Redes (el 4 y 5 de octubre, Auditorio Sotero Prieto, Facultad de Ingeniería, UNAM). Este libro es el resultado de transcribir esas charlas y tratar de recopilar lo dicho e intercambio de ideas y traerlos a un formato de capítulos. Antes de presentar los trabajos se agregan un par de ideas en esta introducción.

Es un hecho irrefutable que las redes de cómputo son la espina dorsal de las comunicaciones en escala mundial. Esto puede, además, leerse desde muy distintos ángulos: las telecomunicaciones son la base sobre la que se construyen relaciones interpersonales, transacciones comerciales, integración de grupos de trabajo. La mayor parte del entretenimiento entregado al usuario final viaja ya sobre internet. Incluso para salir de casa, cada vez más gente, verifica el estado del tránsito sobre internet. La telefonía tradicional dejó hace tiempo de ser el vehículo sobre del cual nuestros módems nos hacían llegar internet, para convertirse en pasajera de ésta. En el transcurso de la pandemia de Covid-19, durante la cual realizamos la revisión del presente texto, esto no ha hecho más que exacerbarse: las telecomunicaciones vía internet, se han convertido en necesarias hasta para realizar nuestro trabajo diario, comunicarnos con nuestros amigos y familiares.

Por la naturaleza de sus protocolos, nuestras comunicaciones hoy son altamente monitoreables, fáciles de espiar, y analizables en individual y de forma agregada para la creación de perfiles detallados por parte de diferentes tipos de actores:

- Los *sospechosos habituales*, actores que han formado parte del monitoreo de comunicaciones desde sus inicios, como los proveedores del servicio de internet (ISPs) y los distintos niveles de gobierno en todas las jurisdicciones que nuestras comunicaciones atraviesen.
- Los *ineludibles*, las grandes empresas de naturaleza monopólica sobre las cuales llevamos a cabo nuestras transacciones, así sea de forma directa y expresa (al estilo de Google, Facebook o Amazon), o que son meros facilitadores transparentes de infraestructura —nombres menos comunes para los *no iniciados*, como *Cloudflare*, *Akamai*, *Azure*, *Rackspace*, e incluso los mismos mencionados en la primera parte de este párrrafo.
- Los *invisibles*, pero no por ello menos peligrosos: grupos de empresas dedicados expresamente al monitoreo y análisis. Típicamente estos se dedican a la venta de publicidad, pero (como en el ampliamente conocido caso de *Cambridge Analytica*) frecuentemente crean detallados perfiles de comportamiento para su aplicación política, o se enfocan al seguimiento personalizado de un grupo claramente definido por su perfil (como lo han hecho en México *Pegasus* o *Hacking Team*, muchas veces bajo las órdenes del gobierno mismo). Para este apartado, dar nombres de compañías resulta menos claro; éstos aparecen y desaparecen constantemente (aunque se mantienen bajo el control de amplios grupos).
- A mucho menor grado, pero no por ello dejan de ser importantes: los *individuos cercanos*. La concentración de las comunicaciones sobre internet ha facilitado el monitoreo de individuos cercanos —pareja, familiares, amigos, potenciales rivales. No hace falta ya *pinchar* un cable, una acti-

vidad bastante notoria y de riesgo, cuando hay tantas vías para obtener información personal de quien nos interese.

CONCEPTOS PRINCIPALES

Comenzamos esta obra partiendo de que se reconoce la *privacidad* como un derecho humano y un concepto inherentemente positivo, y al *anonimato* como un prerrequisito natural para la existencia de ésta. Sin embargo, resulta necesario aprovechar este espacio para una breve definición de estos términos y por qué consideramos necesaria su interrelación.

Partamos de definiciones de diccionario del término *privacidad*. Es común encontrar definiciones lacónicas como la siguiente (Larousse, 2016), "Carácter de lo privado o íntimo. Sinónimo: intimidad". Obtenemos definiciones más acertadas a lo que esta obra presenta buscando, entonces, *privado*: "(...) 2. Que es particular y personal de cada uno. 3. Que se ejecuta a vista de pocos, sin formalidad ni ceremonia. Que está reservado a una sola persona o a un grupo selecto y escogido. 5. Que pertenece a un particular y no al Estado (...)." Dado que queremos comprender el término desde un tratamiento de derechos humanos, presentamos también una definición proveniente de un diccionario especializado en términos jurídicos (DPEJ, 2020): "1. Facultad de una persona de prevenir la difusión de datos pertenecientes a su vida privada que, sin ser difamatorios ni perjudiciales, esta desea que no sean divulgados. 2. Derecho de la persona a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, su domicilio o su correspondencia, ni ataques ilegales a su honra o reputación".

La privacidad como derecho no es un concepto nuevo; encontramos como interesante antecedente un trabajo publicado hace ya 130 años (Warren y Brandeis, 1890), que presenta la evo-

lución de los derechos individuales a partir del derecho a la propiedad privada y los que, poco a poco, se le fueron agregando —derecho a la vida, a la integridad, a la vida plena, avanzando de forma orgánica hasta llegar al derecho a la privacidad. Y —ya en 1890— cita como ejemplos de invasión a la privacidad las fotografías no deseadas, las publicaciones periodísticas carentes de ética y rigor, y "numerosos dispositivos mecánicos que llevarán a la predicción de que lo que se susurra en el armario sea proclamado desde las azoteas".

Si ya en 1890 se tenía esta visión acerca de cómo una invasión a la privacidad puede resultar tan claramente nociva a la calidad de vida y al desarrollo de la persona, el cada vez mayor flujo de la información debe alertar a cada uno de nosotros a que la tendencia de acopio de datos pueda resultar en una tremenda pérdida del espacio de privacidad. Y sí, hace 50 años esto se tenía ya bien claro. Westin (1968) presenta la organización de su libro *Privacidad y libertad* en cuatro partes. En traducción propia:

> (1) La función de la privacidad en la sociedad; (2) una descripción de los avances en tecnologías de vigilancia; (3) la respuesta de la sociedad americana a la introducción de dichas tecnologías, y (4) una evaluación del papel pasado y futuro de la ley americana en esta área.

Westin presenta su contribución de una forma que parece muy actual, a partir de establecer su valor social, que dice que está ausente en todos los otros trabajos sobre vigilancia en la época. Se continúa citando:

> Desde la Segunda Guerra Mundial, avances en los dispositivos electrónicos de espionaje presenta crecientes riesgos

> a la privacidad en la sociedad. Este aumento en la vigilancia puede atribuirse al bajo precio y facilidad con los que se pueden conseguir dichos dispositivos de vigilancia. Un factor adicional es el cambio en la moral de la sociedad, evidenciando una mayor disposición a divulgar más información acerca de hábitos de vida (...) sin limitar el concepto de vigilancia a la observación física o escuchas telefónicas. Esto incluye vigilancia psicológica (el uso de pruebas de personalidad y detectores de mentiras como medios para la selección de personal) y vigilancia de datos (recolección centralizada de información sobre individuos en bancos de cómputo).

La privacidad, pues, se nos presenta como un derecho ampliamente reconocido, pero bajo amenaza y al acecho del efecto de la tecnología —incluso utilizada con fines positivos, como el de tener una sociedad informada o reducir el alcance de conductas antisociales— sobre sí. Paulatinamente, se han ido aprobando leyes que formalmente la reconocen de esta manera, tanto a nivel nacional como internacional, podemos constatar que esta protección ha evolucionado como también ha ido cambiando la realidad; en diversos países se han aprobado leyes para tal fin en la última década. Por citar como ejemplo, en México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LFPDPPP 2010, y LGPDPPSO 2017), y en la Unión Europea, la Regulación General de Protección de Datos (GDPR 2016).

Respecto a la relación entre los dos ejes de esta obra, la privacidad y el anonimato, para ciertos análisis podrían no resultar obvios —incluso podrían verse como contrapuestos. Citando a Skopek (2014), en traducción propia,

> Bajo la condición de privacidad, podemos obtener la identidad de una persona, pero no la de hechos personales relacionados, en tanto bajo la condición de anonimato, obtenemos los hechos relacionados, pero no la identidad de la persona. Bajo este concepto, privacidad y anonimato son términos opuestos, y por esta razón pueden funcionar de forma opuesta: en tanto la privacidad oculta los hechos de alguien cuya identidad es conocida, removiendo de éstos información asociada con la persona de la circulación pública, el anonimato oculta la identidad de alguien cuyos hechos son conocidos para fines de su puesta en circulación pública.

Esto aplica, sin embargo, para conjuntos de datos en manos de terceros. Cuando nos referimos a las acciones que un individuo puede emprender, la principal herramienta para mantener la privacidad respecto a sus acciones es realizarlas de forma anónima.

El estándar ISO sobre Criterios Comunes para la Evaluación de Seguridad en Tecnologías de la Información (ISO/IEC 2005) lo reconoce, definiendo como los cuatro requisitos para garantizar la privacidad: "a) anonimato; b) pseudonimato; c) no vinculabilidad; d) inobservabilidad", e indica que el anonimato "asegura que un usuario pueda utilizar un recurso o servicio sin divulgar su identidad. El anonimato no necesariamente debe verse como una protección para la identidad del sujeto (...) el anonimato requiere que otros usuarios o sujetos sean capaces de determinar la identidad de un usuario dado."

La necesidad del anonimato para mantener la privacidad parece estar ya claramente comprendido por los usuarios de internet en general —86% de los usuarios estadounidenses han intentado tener un uso de la red de forma que se minimice la

visibilidad de sus *huellas digitales* utilizando distintas estrategias (Rainie *et al*., 2013). Las estrategias que ponen en práctica para tal fin, sin embargo, no siempre son tan efectivas, y pueden llevar a conjuntos de datos fácilmente *desanonimizables*, o a la generación de perfiles detallados alrededor de su actividad que, sin requerir tener la totalidad de datos considerados como personalmente identificadores, brinden a un adversario suficiente información para ubicar a cada individuo de forma no ambigua. Esta fue una de las principales motivaciones para dar inicio al proyecto que se presenta en esta obra.

El anonimato puede significar y puede lograrse de diferentes maneras dependiendo del modelo de riesgos que se maneje; la información que nuestras comunicaciones presentan ante distintos actores (con distintos niveles de disponibilidad de recursos) dependen del medio que empleemos, y de la naturaleza específica de la información que estemos generando. Si bien, como se presentará a lo largo de la obra, la principal herramienta utilizada hoy en día por usuarios que buscan mantener su anonimato es la red Tor, ninguna herramienta cubre 100% de los casos de uso. Y, como los desarrolladores de Tor lo fueron descubriendo al paso de los años (lo cual motivó una transformación importante al corazón de su proyecto), no basta con *soltar al mundo* una herramienta: para que quien esté interesado pueda ejercer su derecho a la privacidad utilizando al anonimato como estrategia, es necesario que las herramientas sigan un diseño de interacción que ponga al usuario final en primer lugar.

MAPA DE CAMINOS

El recorrido que daremos, pues, sigue tres líneas discursivas principales. La primera parte, titulada **Complejizar los conceptos**,

presenta las diferentes explicaciones provenientes de lo social, de lo humano, del *por qué* de la privacidad y el anonimato. ¿Qué perseguimos al impulsar este proyecto? Esta primera parte se compone por el capítulo de Alejandro Miranda en que explica cómo la sociedad humana se ha estructurado psicológicamente ante el *panóptico digital*. Juan Carlos Pérez escribe sobre el significado de los conceptos de lo público y lo privado en un entorno digital; presenta criterios para entender el tema, y lo complementa con ejemplos de cómo lo tocan los usos comunes de las redes. Raúl Ornelas, uno de los primeros usuarios frecuentes de redes de anonimato no provenientes del ámbito duro tecnológico de que tenemos conocimiento nos relata cómo y por qué incorporó a Tor a su vida y práctica académica desde hace largos años.

La segunda parte, **Profundizando en las herramientas**, se enfoca en el desarrollo y diseño técnico de las herramientas. Iniciamos con la participación de Roger Dingledine, iniciador y líder de desarrollo del proyecto Tor, principal sistema a nivel mundial de red superpuesta anonimizadora, hablando de *la privacidad en internet en la era de la gran vigilancia*. Cynthia Solís y Alfredo Reyes Krafft (de Lex Informática) continúan, presentando un análisis centrado en el uso de Tor, analizado su viabilidad desde una perspectiva legal.

La experiencia del usuario es fundamental, entonces, para lograr una adopción a mayor escala de las *PETs* (Tecnologías que Aumentan la Privacidad, del inglés, *PETs*, *Privacy Enhancing Tecnologies*). Antonela Debiasi comparte su experiencia acercando a Tor a los usuarios menos técnicos —quienes probablemente más requieran de Tor en la realidad— y se enfoca en el qué y el por qué de los cambios en la usabilidad realizados al navegador *Tor Browser*, logrando importantes resultados. *Sajolida*, del proyecto Tails, aborda también el tema de la usabilidad, presentando una

serie de tensiones que encuentra entre el desarrollo tradicional de software libre y la adopción de criterios y prácticas de usabilidad. Por último, la segunda parte cuenta con la participación de Daniel Kahn Gillmor. Si bien al hablar de comunicaciones en internet pensamos en primer término en un uso interactivo, Daniel aborda un interesante problema: cómo asegurar la privacidad en el correo electrónico. Si bien desde 1990 existe PGP (por las siglas *Muy Buena Privacidad*, en inglés *Pretty Good Privacy*), un programa diseñado por Phil Zimmerman y ampliamente utilizado en círculos tecnófilos, hoy en día incluso convertido en estándar formal, su usabilidad imposibilita su adopción a gran escala. Autocrypt presenta un nuevo modo de interacción para el manejo del cifrado en el correo electrónico, rompiendo con muchas prácticas firmemente asentadas en la comunidad técnica.

Para la tercera parte, **Territorios/contextos**, presentamos ejemplos dela aplicación o necesidad del anonimato ante problematizaciones específicas en entornos nacionales o legales particulares. Inicia con el panorama que brinda Juan Jacobo Nájera acerca del uso y de problemas derivados de buscar la participación activa para ampliar la red de Tor en México. Norman García presenta su experiencia desde Nicaragua, donde enfrenta y ayuda a combatir los aspectos de monitoreo, censura gubernamental, cibervigilancia y acoso digital. La obra cierra con la participación de Jesús Robles (Enjambre Digital), quien abordó los aspectos legales del anonimato en las comunicaciones.

AGRADECIMIENTOS

Llevar a cabo un proyecto como el que este libro corona no es una tarea para una sola persona, ni siquiera para el grupo que conjunta sus participaciones en los capítulos de este libro. Que-

da patente la gratitud al gran equipo que conforma el Laboratorio de Investigación y Desarrollo de Software Libre (LIDSOL) de la Facultad de Ingeniería.

Una buena parte de este libro consta de transcripciones de las charlas impartidas en el coloquio. Los alumnos participantes del LIDSOL ayudaron a realizar ese pesado trabajo. Sin mayor orden que el alfabético, queda el agradecimiento al trabajo y tiempo que invirtieron en este proyecto a Diego Barriga, Emilio Cabrera, Juan Flores y Cinthya Tamayo.

El buen Hacklib, habitante de la esfera de la pseudonímia desde hace muchos años, hizo una primera lectura del libro para homogeneizar estilos y que en lo global resulte más *digerible* para el lector. Esta tarea, especializada e intensiva en tiempo, merece todo agradecimiento.

BIBLIOGRAFÍA

GDPR (2016). General Data Protection Regulation. *Official Journal of the European Union.* Consultado en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (2021-02-04).

ISO/IEC 15408 (2020). Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de TI. Parte 1: Introducción y modelo general.

LFPDPPP (2010). Ley Federal de Protección de Datos Personales en Posesión de Particulares. *Cámara de Diputados del H. Congreso de la Unión*. Consultado en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (2021-02-04).

LGPDPPSO (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Cámara de Diputados del H. Congreso de la Unión*. Consultado en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf (2021-02-04).

Privacidad, Privado (2016). *Diccionario Larousse de la Lengua Española*. Consultado en: https://www.diccionarios.com/diccionario (2020-08-18).

Privacidad (2020). *Diccionario Panhispánico del Español Jurídico (DPEJ).* Consultado en: https://dpej.rae.es/lema/privacidad (2020-08-18).

Rainie, L. (2013). Anonymity, Privacy and Security Online. *Pew Research Center.* https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf (2020-10-05).

Skopek, J. M. (2014). Anonymity, the production of goods, and institutional design. *Fordham Law Review* vol. 82, issue 4, 1751-1809.

Sprenger, Polly (1999). Sun on Privacy: 'Get over it' *Wired News, 26, 1-4.* Consultado en: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ (2020-08-18).

Warren, S. D., y L. D. Brandeis (1890). The right to privacy. *Harvard law review*, 193-220. Consultado en: https://www.jstor.org/stable/1321160 (2020-08-18).

Westin, A. (1968). Privacy and Freedom. *Washington and Lee Law Review,* vol. 25, núm. 1. Consultado en: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/ (2020-08-18).

PRIMERA PARTE

COMPLEJIZAR LOS CONCEPTOS

1

MECANISMOS PSICOLÓGICOS DE LA PRIVACIDAD Y ANONIMATO EN EL PANÓPTICO DIGITAL

Alejandro Miranda

TECNOLOGÍA, PSIQUE Y HUMANIDAD

Me gusta viajar en tren; además de ir menos lleno que el metro o los autobuses, gran parte de los pasajeros se dedican a leer más que a escuchar música. Claro, de 10 años para acá la gente dejó de comprar impresos y van leyendo en su celular, en donde probablemente regalarán algunos "me gusta", y estarán conversando en las redes sociodigitales. Una escena que ha llevado a cierta generación a lamentarse por el visible aislamiento que las tecnologías digitales hacen al tejido social, no importando que somos las personas, al final, quienes llenamos el espacio sociodigital.

El presente texto es una continuación de "Intimidad y privacidad mediada por entornos digitales", parte de la compilación del libro *Ética hacker, seguridad y vigilancia* publicada por la Universidad del Claustro de Sor Juana en 2016 y en el que se amplía el planteamiento de nuestros mecanismos evolutivos frente a la tecnología y de cómo la propensión a interiorizarnos y hacerlos parte de la integración del YO nos vulnera frente a la vigilancia electrónica en el uso de los dispositivos mediacionales digitales.

Lo que ha pasado en el tren es que se ha reemplazado una tecnología (el libro) por otra (el celular). Pero ¿de dónde viene nuestra propensión por la tecnología? La respuesta no se encuentra en lo que nos rodea, si no en lo que nos *integra*. Probablemente, los casos más analizados en psicología sobre la relación simbiótica entre tecnología y actividad humana son los estudios sobre pensamiento y lenguaje de las décadas de 1980 y 1990, centrados en encontrar si el lenguaje dominaba sobre el pensamiento, o al revés. Piaget y su teoría de la generatividad cognitiva en la infancia estaba contrapuesto con Vygotsky y su teoría de interiorización del mundo social. Las evidencias aportadas por ambos grupos teóricos, hoy, nos permiten sostener que la generatividad cognitiva y el pensamiento se desarrollan a partir de las disposiciones biológicas y la interacción con el medio ambiente, pero que, gracias a la interiorización del lenguaje es que el pensamiento potencia las capacidades de cálculo y abstracción.

Esta discusión clásica en los estudios evolutivos del desarrollo humano terminó por evidenciar la importancia de los dispositivos tecnológicos, entre ellos el lenguaje. Es decir, los seres humanos integramos y somos tecnología: al nacer nos encontramos rodeados de personas con un lenguaje específico, así como costumbres y prácticas culturales, que han de conformar nuestro desarrollo y personalidad, moldeando nuestras emociones y pensamiento.

Parafraseando a Wertsch (1998) en su libro *La formación social de la mente*, este hecho lo conocemos como la superposición de las relaciones sociales y los dispositivos tecnológicos y que son asimiladas y adaptadas por el individuo, dando como resultado el moldeamiento de la psique. Entonces, no hay un estado natural del ser humano, porque estamos estrechamente vinculados a la tecnología del grupo.

Cuando hablamos de tecnología la referimos como el conjunto de artefactos desarrollados por la acción humana que posibilita la transformación del ambiente concreto o simbólico.

La tecnología y sus artefactos representan la cristalización del intelecto, dispositivos que posibilitan, restringen y potencian la actividad humana, creando contextos partiendo de nuestra capacidad biológica, cognitiva y emocional. La psique humana se vincula con los dispositivos y los usa para su desarrollo, no hay individualidad sin colectividad y ambos constructos se encuentran sujetos a las mediaciones existentes en el entorno.

La estructuración del YO comienza con la diferenciación del individuo con el entorno por medio de los límites corporales y cognitivos entre el yo, nosotros y ellos y con ello se moldean la noción de intimidad y espacios socioemocionales compartidos.

Hasta hace poco tiempo (al menos 30 años) existía un claro límite entre la esfera pública y la esfera privada, pero esto cambió drásticamente desde que los dispositivos digitales y la conectividad irrumpieron en nuestra vida cotidiana. Los dispositivos digitales nos han permitido generar nuevas simbiosis en las que hemos extendido nuestras capacidades cognitivas, emocionales y de comunicación, posibilitándonos la ubicuidad simbólica, al documentar nuestra acción, abstraerla del espacio vital para proyectarla en el espacio virtual.

Esta capacidad de habitar el espacio virtual y de comunicarnos y "estar" en dos o más partes simultáneamente ha roto las fronteras de lo que conocíamos como lo público y lo privado.

INTIMIDAD Y ACTITUD LUDITA EN LO DIGITAL

Lo privado, referido como la intimidad es la "zona reservada por una persona para sí misma o un grupo específico de personas", y

con ello surge la privacidad que puede ser entendida como aquello "que se ejecuta a la vista de pocos" (DRAE, 2014), y de esta acepción se deriva la protección de cualquier intromisión externa. Entonces, los conceptos nos son equivalentes, la intimidad refiere a la acción de reserva de un apartado de la vida, mientras la privacidad es una acción social que protege la intimidad.

Desde los modelos de desarrollo, como el ecológico de Bronfenbrenner (1986), en la infancia temprana la intimidad se ejerce sólo a la vista del círculo de pertenencia (familia) y conforme el individuo se desarrolla se incluyen otros sistemas sociales como los pares, la escuela, el trabajo y la comunidad, esto crea una serie de intersecciones circulares en los que el individuo ejercerá un papel público e íntimo en el que actúa diferencialmente.

Ya en la etapa adolescente se ha interiorizado el papel y los comportamientos de lo íntimo y lo público en los diversos círculos de interacción como la familia, los amigos, la pareja, y los colegas de escuela o trabajo.

Son diversos los ejes de lo íntimo en las teorías del desarrollo pero podemos observarlo fácilmente en la reserva de algunas zonas del desarrollo emocional, sexual y de identidad de género frente a los adultos, mientras se abre un espacio de confianza para algunos de sus pares.

Un ejemplo más se observa en el comportamiento moral (Navas, 2010), desde la postulación de la teoría del desarrollo moral de Kolberg hemos aprendido que en la infancia temprana (primera etapa de Kolberg) hay un comportamiento heterónomo al premio o el castigo derivado de nuestros compartimentos morales, mientras que para la adolescencia ya se observa un comportamiento moral concordante con el deber ser (tercera etapa de Kolberg) que implican actitudes prosociales hacia nuestros grupos; pero también sabemos que estos comportamientos pro-

sociales se rompen cuando sabemos que no somos observados o que no habrá castigo por romperlos.

También en la teoría del desarrollo psicosocial de Erikson (Papalia, Wendkos y Duskin, 2010) al término de la adolescencia y comenzando la adultez temprana las personas daremos prioridad al establecimiento de relaciones recíprocas que le brinden seguridad, acompañamiento y confianza.

En el ciclo del desarrollo humano vamos aprendido la construcción de estos espacios de intimidad aprendiendo a reservarnos fragmentos del YO para nosotros o bien nuestro circulo de confianza.

¿Cuál de todos los énfasis conductuales son nuestra verdadera personalidad? La suma de todos esos rasgos que permanecen constantes aún cuando las variables ambientales cambien son nuestra personalidad. Entonces la vida se pasa en el ejercicio de distintas esferas públicas e íntima en las que conscientemente nos reservamos o mostramos características emocionales, cognitivas y comportamentales.

De la intimidad se desprenden al menos tres áreas de reserva (Vacarezza, 2000): Respecto al espacio propio o *intimidad territorial*. Refiere a la reserva topológica en que se protege el territorio y la posición, se entiende que el acceso al territorio implica una violación a la intimidad, los dormitorios son un buen ejemplo de las reservas territoriales, pero también pueden incluir objetos personales como un diario o un dispositivo electrónico.

La *intimidad corporal*. La vestimenta protege sobre otras intromisiones territoriales, las del propio cuerpo, esta intimidad se vincula con el concepto de sexualidad y erotismo desarrollado ampliamente por Giddens (1995).

Por último (Vacarezza, 2000), existe *intimidad psicológica*. Que es la reserva de todo individuo a mantener en lo privado sus

afectos, pensamientos, creencias, valores y acciones y en la que se entiende se aleja del escrutinio de terceros.

Sin embargo, estos tres planteamientos de lo íntimo son insuficientes para explicar la intimidad contemporánea: la intimidad territorial, corporal y psicológica no están considerando la ubicuidad de los medios digitales, omnipresentes a todas las esferas. Es decir, hay una cuarta esfera, la *intimidad digital*, y que constituye en la aparente reserva territorial, corporal y psicológica mediada por un dispositivo digital.

En el campo del estudio del desarrollo humano existe la creencia de que las interacciones digitales compensan las carencias de interacciones en lo vital (Bazán y Boveda, 2005), se sostiene que una persona poco participativa en los entornos vitales no lo será en los entornos en línea en tanto este compensará sus carencias con la protección del aislamiento físico y el control de la ansiedad generada; pero la realidad es que existen múltiples voces con diversos posicionamientos de los efectos de la intimidad en la esfera digital.

Ghalioun (1998) sostiene que internet promueve una dinámica integradora de valores universales que desdibujando el rastro de lo local, resultando una fractura de la identidad al interior de la sociedad.

Baladrón (2003) plantea que los medios moldean las conciencias al ofrecer una visión selectiva de los fenómenos y que desvirtúa las relaciones humanas en tanto el humano de esos mundos virtuales a pesar de parecer reales son menos reales, es decir, son falsos en algún sentido (así se rescata la acepción original de lo virtual, lo que aparenta ser).

Zegers (2011) indica que internet es un laboratorio identitario en el que se puede experimentar entre la unicidad y la multiplicidad, concluyendo que internet es capaz de cooptar el

desarrollo de la psique al cambiar los propósitos y motivaciones de la persona.

Tal parece que en opinión de todos estos autores hay un ruta para el desarrollo de la personalidad y los medios digitales la trastornan; pero como ya lo hemos establecido en el apartado inicial del texto, lo natural en el ser humano es un ciclo de uso de la tecnología que cambia su psique y al ambiente.

En otra rama de los estudios de la intimidad digital, Birnie y Horvath (2002) evaluaron el comportamiento social tradicional (sociabilidad y timidez) frente al comportamiento social en línea de 115 estudiantes universitarios (52 hombres, 63 mujeres) encontrando que la sociabilidad e intimidad complementaban el compartimento presencial, aunque sí exisistía un ligero repunte del habla por canales íntimos en el caso de las personas tímidas, estos hallazgos nos dicen que las redes sociales se convierten en una extensión de la conducta social tradicional.

En otra investigación, Linne (2014) le da seguimiento en dos años de observaciones diarias al comportamiento de 200 adolescentes de la ciudad de Buenos Aires con actividad en Facebook, en donde por medio de una técnica de análisis de contenido identificó que los tipos de contenidos más populares eran la autopresentación, el intercambio entre conocidos, las relaciones socio afectivas, encontrando en este sentido ejecuciones íntimas que aumentan la socialización entre los integrantes de su clica.

Además, Linne reporta un análisis cualitativo del acceso de población en desventaja social en cibercafés, con 40 entrevistas a profundidad en población similar. Los cibercafés funcionaban como espacios lúdicos para los preadolescentes (11 y 12 años) y para los adolescentes como espacios de práctica comunicativa y de socialización entre pares, aunque ambos casos también se usan como sistema de búsqueda para la información de tareas escolares.

Un caso más de cómo internet potencializa la comunicación y la intimidad es el reporte de Kang (2012) que analiza las transformaciones de la comunicación íntima entre familias dispersas entre Londres y China y en el que se observan transformaciones importantes en las funciones tradicionales del cuidado emocional pasando de ser una función netamente femenina a una actividad cada vez más difundida entre el papel masculino.

Así pues, el uso de las redes sociales se ejerce entre los más jóvenes como un espacio de oportunidad para cultivar amistades y llevar a cabo actividades de socialización desde una óptica narcisista en la que simultáneamente se cultiva la presencia individual, pero también hay diálogo continuo con el grupo de pertenencia virtual en el que con una sensación de privacidad favorecen la comunicación y se desarrolla identidad y el cultivo de amistades verdaderas (Livingstone, 2008).

Las investigaciones de Linne (2014) y Livingstone (2008), permiten sostener que los espacios de confianza e intimidad que se observan a partir de la adolescencia en los estudios del desarrollo también ocurren en la comunicación mediada por internet, y esto puede enterderse solo si la persona lo considera un espacio seguro.

McKenna, Green y Gleason (2002) realizaron un estudio bajo el supuesto de que, como internet brinda una oportunidad de expresión abierta, es muy probable que fomente vínculos emocionales francos en las relaciones en línea, aumentando la probabilidad de que estas se lleven al espacio de la vida presencial, para cumplir con la meta los investigadores levantaron un par de sondeos sobre los motivos y tiempo de duración de las relaciones que surgen en internet y cómo estas amistades se perpetúan en los espacios no presenciales. Entre algunos de los hallazgos relevantes tenemos que las relaciones que surgen en

internet y se migran al espacio presencial era altamente probable encontrarlas vigentes dos años más tarde; también encontraron que aquellas parejas que habían comenzado intercambios dialógicos por internet se gustaban más en comparación con los que habían comenzado cara a cara.

En los tres estudios de McKenna, Green y Gleason (2002), Livingstone (2008) y Linne (2014), se tipifican perfiles psicológicos relacionados con la ansiedad o facilidad para entablar relaciones sociales observando que aquellos que generan ansiedad en el establecimiento de la relaciones sociales presenciales encuentran en el establecimiento de relaciones en línea un medio en el que se les facilita la tarea para expresar su "verdadero YO" y como en el caso de los que no tienen problema en el establecimiento de relaciones presenciales cuando generan una relación emocionalmente alta en internet tienden al contacto fuera de línea en una relación larga y duradera.

No importando la facilidad o dificultad para el establecimiento de relaciones, se observa que la comunicación mediada facilita la eficacia en la transmisión de expresiones socioemocionales, por lo tanto, la tecnología desempeña un papel importante en la construcción y mantenimiento de una relación con grado emocional. Estos mismos autores reportan que aquellos que establecen relaciones emocionalmente ricas en internet también tienden a la colaboración y participación activa en comunidades virtuales; esto quiere decir que con independencia del perfil introvertido o extrovertido hay beneficios directos en el uso de internet en el establecimiento de relaciones ampliando en ambos casos la comunicación e integrantes de la familia y amigos.

En un estudio de escala similar, Gross, Juvonen y Gable (2002) dieron seguimiento en tres noches sucesivas al intercambio de

sus mensajes instantáneo por internet de 130 estudiantes de séptimo grado de una ciudad de California, buscando esta actividad con el bienestar social entre adolescentes. Entre los hallazgos relevantes encontraron que el tiempo de uso de internet e intensidad de mensajes no reporta ninguna correlación con el bienestar social, aunque sí hay un efecto en la sensación de acompañamiento entre quienes lo usan.

En investigaciones más recientes con adultos en contexto laboral Broadbent (2009 y 2015) nos propone que internet está posibilitando el establecimiento de relaciones íntimas a pesar de los confinamientos a los que nos encontramos sometidos en los contextos contemporáneos. Tan solo hace tres décadas cualquier persona laborando en alguna institución estaba sometida a los controles de las llamadas telefónicas alámbricas, pero con la irrupción de internet y las telecomunicaciones personales se comunican con hasta siete personas de su primer círculo por medio de llamadas de celular, correo electrónico o mensajería.

En este mismo sentido nos muestran que en Facebook se tiene contacto con hasta 120 personas, y que se interactúa frecuentemente con hasta cuatro contactos, en el caso de las llamadas de voz también se ha observado que 80% se dirige hasta cuatro usuarios.

Los hallazgos de Broadbent son importantes, porque en una época en la se ha puesto énfasis en las posibilidades de contactar y conversar con múltiples personas, los individuos usan las telecomunicaciones para darse un pequeño respiro de sus actividades laborales y contactar al círculo de personas que emocionalmente encuentran cercano.

En opinión de Ponce (2014) esta condición de ubicuidad de grupo en nuestro primer círculo va trastocando los estilos culturales de la interacción en el hogar y espacio físico, creando nue-

vas condiciones topológicas físicas y virtuales que dibujan nuevos espacios de apropiación donde se reedita la noción del humano nómada pero manteniendo un contacto estrecho con las personas emocionalmente cercanas.

Sin embargo, no todo son opiniones positivas respecto a las posibilidades de la comunicación mediada digitalmente, por ejemplo, Saramago (2002:3) lamenta la pérdida de espacios de "la comunicación real, directa, de persona a persona", con ello el riesgo de la deshumanización aumenta; en tanto el ser humano dejó de ser crítico a los cambios mediacionales para dejarse llevar por las mediciones tecnológicas que se originan en empresarios de dudosas motivaciones.

Saramago es representativo de una línea de pensamiento que tiene una versión catastrofista de las nuevas mediaciones digitales humanas, pareciera que toda construcción física y dialógica pasada fue mejor, e inclusive nos hace recordar las protestas del movimiento ludita en el siglo XIX ante la emergencia de la máquina industrial; pero aunque no sea evidente como si lo humano se encuentra definido por una sucesión de mediaciones tecnológicas que van cambiado el sentido mismo del YO.

Considerando que el desarrollo de la psique humana se encuentra asociado al estado del desarrollo tecnológico, ¿en un futuro leeremos las anteriores argumentaciones como un movimiento neoludita?, como defensores de un estado tecnológico y de conciencia humana que convivirá con nosotros pero que ya no será dominante.

Pero no todas las mediaciones digitales tienen un lado oscuro o implicaciones catastrofistas, la idea del gran empresario que decide el destino de todos nosotros por medio de la arquitectura de lo digital va encontrando oposición en los usos no planificados de la tecnología.

Rheingold (2004) en su libro *Multitudes inteligentes,* describe ampliamente el fenómeno de la inteligencia colectiva potenciada por los usos no planificados de los dispositivos y tecnologías digitales a pesar de la oposición de la industria y los gobiernos empecinados en el control de la tecnología.

La socialización por internet rompió el eje temporal del ser y estar para extender las interacciones de conversación. Cuando interactuamos, actuamos sobre lo digital, se cristaliza y perpetúa la acción permitiendo acciones dialógicas de otros agentes, que anteriormente eran posibles pero con un efecto limitado; como el diálogo entre escritores de libros.

Con la internet, la propiedad de cristalizar la acción humana en objetos digitales se convierte en una gran virtud por su velocidad de propagación y es la cimentación sobre la que descansa muchos de los arreglos colaborativos contemporáneos como el caso del Software Libre o Wikipedia.

Es esta misma virtud la propiedad que condena a las personas cuando se ejerce sobre su intimidad al posibilitar una diseminación que potencia el acoso y la explotación de eventos íntimos, al permitir la distribución amplia, y por largo tiempo, de un acto cristalizado que vulnera y expone emocionalmente a la persona.

En el contexto de libre circulación de los objetos digitales pueden existir eventos con más repercusión que el acoso como puede ser la exposición sexual por internet, uno de los eventos más íntimos. En lo general, la mayor parte de las personas toman sus precauciones para reservar ese espacio, sin embargo, cuando se combina con el uso de dispositivos digitales la delimitación, lo íntimo puede salirse de lo previsto.

Cuando una pareja (sin importar su edad) decide incluir alguna clase de dispositivo digital para aumentar o extender el erotismo se parte de un supuesto de confianza en que ninguna

de las dos partes han de divulgar los intercambios textuales y gráficos.

¿Qué pasa con estos objetos cuando hay un rompimiento de la pareja?, ¿se borran?, ¿se conservan?, ¿se comparten?

En las dos primeras opciones no hay problema alguno, aquellos registros eróticos se han de quedar en la intimidad y en la esfera de lo privado, pero en el caso que alguno de los dos decida la exposición pública de los objetos el daño moral, emocional y cognitivo puede ser amplio.

Aunque el fenómeno sucede en la virtualidad, su efecto no lo es; aunque las repercusiones sean mayúsculas en lo individual, no quiere decir que sean extremadamente frecuentes.

Del Rey, Sánchez y Ortega (2012) realizan una revisión contemporánea del concepto de las actitudes prosociales e intimidad de los adolescentes en internet en contraposición de los usos negativos de internet, como el acoso escolar, con la idea de balancear los reportes académicos que giran alrededor de los usos de la tecnología específicamente entre los adolescentes españoles concluyendo que éstos usan mayormente internet y la telefonía celular para la comunicación y el esparcimiento (como los juegos) y las menos comunes son las actividades prosociales. En opinión de estos autores es necesario replantear el enfoque de los esfuerzos de autoridades e investigadores, indicando que en vez de resaltar los usos negativos de internet y telefonía celular, es necesario modelar y hacer visibles las actividades prosociales que suceden en internet, en su opinión de esta forma se podrá incidir directamente en un desarrollo psicosocial óptimo entre los adolescentes.

Las recomendaciones de Del Rey, Sánchez y Ortega resaltan un componente importante de internet, la conducta prosocial; de hecho muchos de los objetos con mayor éxito en internet sí

tienen este énfasis. Estos objetos son producto de la cooperación y acción colectiva aparentemente desinteresada, en donde la ganancia individual es cognitiva, emocional o social.

Estos grandes objetos colectivos han creado espacios donde se modelan las actitudes y acciones prosociales, aunque no sean aparentemente relevantes para la producción del objeto mismo. Así, aunque hay ganancia individual, en lo colectivo los objetos existen gracias al acuerdo de consideración al otro y actitudes prosociales guiadas por el bien común.

Debemos de resaltar, aunque algunos de los argumentos advierten de los peligros de alienarse por la exposición a los dispositivos electrónicos, en tanto que son deshumanizantes, también se observan argumentos en el sentido contrario, agrupamientos humanos que han encontrado mecanismos de cooperación orientados al bien común.

Pero ambas corrientes de pensamiento hablan de los efectos e importancia de la tecnología digital en la acción humana, pero no como un agente externo, sino como un artefacto que inicialmente complementa las acciones, y que por su efecto mediador termina por cambiar la acción visibilizando su efecto mediador.

PRIVACIDAD DIGITAL

Las tecnologías digitales son mecanismos mediacionales de la acción humana, que va desde los actos íntimos, hasta la comunicación pública y el ejercicio del ocio en ambas esferas.

No hay que perder de vista que algunos usos implican la decisión consciente de la persona de vivir en una caja de cristal, como en Twitter donde la conversación es pública, y puede ser observado por terceros sin necesidad de reciprocidad, pero en la mayoría de los usos se busca sólo la extensión de la conversión

y proyección de las emociones sin depender del espacio físico manteniendo la comunicación con un grupo delimitado de personas. La mediación transforma las acciones (antes efímeras) en eventos con registro que pueden ser consultados, almacenados y compartidos, lo que pone en riesgo el acto de compartirlos solo con un grupo delimitado de personas porque la empresa que gestiona el almacenamiento de los datos siempre se encuentra en posibilidad de observarlos, usarlos y hasta compartirlos.

La filtración sobre la vigilancia global, que hasta hace poco parecía de ciencia ficción, hoy se confirma mediante programas de vigilancia como Echelon, Carnivore y PRISM, diseñados para la extracción de datos de las telecomunicaciones en puntos estratégicos. Según su implementación histórica, por ejemplo, en el caso de Echelon fueron los proveedores de ISP, en tanto que para PRISM las fuentes fueron empresas que se han convertido en nodos de información dominantes como Google o Apple. Estos programas de vigilancia tenían una coordinación global que permitía tener patrones a largo plazo de comportamiento sobre metadatos de diversos servicios como videos, correo, conversaciones de texto y video, complementando con programas globales de seguimiento de conversaciones telefónicas bajo el programa MYSTIC (Muñoz, 2014).

En opinión de Wolf (2013), lo sorpresivo del anuncio de PRISM no fue la vigilancia sobre el tráfico de internet, sino la escala de este programa y esto provocó un resurgimiento de la discusión sobre el seguimiento de nuestras actividades en internet. También permitió discutir si hay otros actores de diferente escala observando nuestros rastros, no se trata de tener información sensible, dedicarse a actividades ilegales, las filtraciones subrayaron un tema que todos intuían pero no se reconocía, la vigilancia electrónica en distintas escalas.

De hecho, el tema de la vigilancia electrónica se encuentra a la vista de todos, desde hace algunos años vimos emerger el tema con la inteligencia de negocios a partir de grandes conjuntos de datos, en 2012 se hablaba de 2.5 exabytes de información creados cada día y con un estimado que estaría duplicándose cada 40 meses, es decir, la marca de nuestros tiempos son los registros y cómo procesarlos (McAfee, *et al*., 2012). El *Big Data* se basa en la analítica de datos, una serie de técnicas existentes que usan minería de datos y algoritmos de inteligencia artificial que tienen un amplio espectro de aplicación en los negocios y en el seguimiento educativo (Chen, Chiang y Storey, 2012). La minería de datos es una técnica de extracción y procesamiento de datos para transformar datos crudos en una matriz interpretativa, para ello se seleccionan los datos, se procesan, transforman, se organizan según los focos de interés y, finalmente, se interpretan y evalúan (Fayyad, Piatetsky-Shapiro y Smyth, 1996).

Lo nuevo en el *Big Data* es el volumen de los datos, desde la década de 1950 hemos dado pasos en la digitalización de los servicios, al punto que hoy todo centro humano gira alrededor de los servicios digitales; aun cuando las personas no usen directamente esos servicios, la informática se encuentra omnipresente. En cierta medida, se han cumplido los imaginarios de Asimov cuando apostaba a la existencia de computadoras omnipresentes y con una enorme capacidad de procesamiento, y que se abstraería de su sustrato físico para convertirse en un ente pensante y autónomo.

El problema de la omnipresencia de los sistemas informáticos es que a diferencia de los entes divinos e informáticos de Asimov éstos aún no cuentan con límites morales para regularse, no se preocupan por el buen resguardo de los datos o protegerán

al usuario aún cuando su propia existencia digital esté de por medio. Como lo menciona Wolf (2013), el problema del estado actual de las bases de datos que recogen información sobre los metadatos y actividades realizadas por la mediación digital es que están sujetas a la toma de decisiones de personas con intereses diversos que en algunas ocasiones actúan en el sentido contrario o sin su consentimiento.

Estas decisiones van, desde actos dolosamente intencionales para invadir el espacio privado de los usuarios, hasta el análisis de registros para propósitos específicos como la analítica escolar o el uso de una interfaz.

En el primer caso encontramos las acciones de la NSA (Agencia de Seguridad Nacional de los Estados Unidos, por sus siglas en inglés) para hacerse de información por medios ilegales que incluían acciones de espionaje electrónico en gran escala en discos duros de marcas como Western Digital, Seagate y Toshiba desde 2001 y hasta el 2015, los países mayormente infectados fueron Rusia, Pakistán, Afganistán, China, Malí, Siria, Yemen y Argelia, pero se sabía de la existencia de la puerta trasera en México y Brasil en un nivel medio (Reuters, 2015).

En temas de gran escala, en julio del 2015, se publicaron las filtraciones de Wikileaks que daban cuenta de diferentes entidades de gobierno mexicano que contrataron servicios de troyanos y software espía de la empresa Hacking Team (Sánchez, 2015), entre ellos, el Centro de Investigación y Seguridad Nacional (Cisen), los gobiernos del Estado de México, Querétaro, Puebla, Campeche, Tamaulipas, Yucatán, Durango y Jalisco. Este tipo de casos, por su magnitud, hacen pensar en un espionaje masivo, permanente y necesario, del que sólo debe preocuparse quienes tengan algo que ocultar, el resto no debe temer ni desconfiar de este escrutinio no consensuado.

También hay espionaje en pequeña escala, por ejemplo, el colegio Lower Merion de Pennsylvania usó el software de rastreo antirrobo de las laptops *Apple* para espiar a sus 2 300 estudiantes, de los que recabó 56 000 imágenes en diferentes contextos, como su casa o la escuela. Esto fue de conocimiento público hasta que una foto, tomada fuera de la escuela, fue usada como argumento para expulsar a un estudiante, del que tenían unas 400 fotografías (AP, 2010).

La invasión a la intimidad no sólo busca la vigilancia e identificación de patrones que se ajusten al elemento deseado, también tienen un efecto disuasivo. Penney (2016), en un estudio preliminar sobre los efectos de la vigilancia masiva en la actividad de artículos sobre gobierno y privacidad observa una disminución estadísticamente significativa posterior a las revelaciones de PRISM, manteniéndose la tendencia de la reducción de tráfico en temas sensibles como lo pueden ser la vigilancia en línea, los conflictos bélicos, los litigios constitucionales y el estado de la democracia en Estados Unidos.

La desaceleración en la edición de temas sensibles puede ser interpretada como un efecto de indefensión aprendida, entendido como el aprendizaje de una persona de no hacer nada ante un evento de carácter inminente por la razón de que sabe que no podrá evitarlo, la falta de esperanza se desarrolla históricamente cuando la persona cae en cuenta de su incapacidad de control ambiental. Este efecto psicológico es esperable si consideramos que la vigilancia global y local atenta con uno de los espacios más preciados, la reserva de lo íntimo y el usuario asume que no podrá evitarlo.

Emparentado con este efecto de desbalance psicológico la periodista Naomi Klein (2007) en su libro, *La doctrina del shock* propone la tesis de que el auge de las teorías económicas libe-

rales se extendieron no porque fueron populares si no por medio de efectos psicológicos aprovechando la conmoción emocional de eventos naturales o planificados, si bien esta propuesta sociológica puede ser catalogada de teoría de la conspiración, es una tesis aceptable considerando los esfuerzos coordinados de la vigilancia global. Las diversas filtraciones de los alcances de vigilancia ayudan a la visibilidad del tema también crean un contexto de autocensura extendida por la aparente imposibilidad de no tener control sobre el hecho.

Si bien las personas en general han decido retraerse de estos temas, no ha sucedido así con las organizaciones y personas dedicadas al tema de la intimidad en internet y la vigilancia electrónica que han aprovechado las filtraciones para promover una agenda global, nacional y local sobre la importancia de poner límites al seguimiento electrónico sin importar su finalidad.

PANÓPTICO DIGITAL. LA FALSA PERCEPCIÓN DE PRIVACIDAD

En el derecho internacional se usa "privacidad" como equivalente al derecho de la intimidad digital, pero en realidad hay dos acepciones (Moreno y Abril, 2014). La primera refiere a la premisa clásica de la "privacidad como dignidad", que presupone el principio de "inviolabilidad de la personalidad", donde la intimidad es el espacio reservado al escrutinio público. Sin embargo, en los nuevos espacios socioemocionales digitales hay una falsa percepción de intimidad, por diseño estas mediaciones emocionales están pasando por el canal tecnológico de un tercero.

Esto es un cambio paradigmático, por *defecto* hemos cedido la intimidad. Si bien en el caso de los marcos regulatorios de las conductas en internet hay un principio extendido referente

a que si ya se encuentra regulado en lo presencial, sólo hay que extender esa protección a lo digital, esto no aplica a los nuevos escenarios dialógicos.

No sólo se trata de la posibilidad de ser vigilado en la intimidad digital, también al existir un registro y almacenamiento de nuestras interacciones son susceptibles de ser extraídas y exhibidas sin el consentimiento de los usuarios. Un ejemplo de la falsa percepción de seguridad en la que nos movemos como usuarios con mediaciones digitales fueron las filtraciones del 2014 en el foro 4Chan de artistas que se habían sacado fotos con desnudos o en poses provocadoras y almacenadas en el servicio iCloud de Apple (AP, 2014).

Ante estos nuevos escenarios de mediación de la intimidad toma fuerza una segunda acepción que refiere a la privacidad como el control que se tiene sobre la información personal, en la que el usuario decide qué tipo de información desea divulgar y además de contar con las herramientas para que configure de manera informada el tipo de información que se puede colectar sobre él; bajo este esquema el usuario puede decidir qué información será colectada por las distintas instancias del servicio y cuál publicada y exhibida (Moreno y Abril, 2014).

En tanto la mediación tecnológica y el registro de la actividad es una condición del servicio, este enfoque requiere de la autorregulación del intermediario, quien deberá abstenerse de dar seguimiento a la actividad no solicitada por parte de su cliente. El problema es que el prestador de servicios no tiene los incentivos económicos suficientes para garantizar su neutralidad en el mismo, en tanto muchas de estas empresas se financian con el trazado de patrones de consumo de sus usuarios y la identificación de perfiles económicos para el ofrecimiento de publicidad adecuada al usuario.

El problema de origen no son las motivaciones éticas y económicas de los empresarios que ofrecen servicios de comunicación mediacionales, el origen es la decisión del usuario de hacer uso de estos servicios, somos nosotros los que voluntariamente cedemos nuestro espacio íntimo, por servicios de una intimidad digital aparente.

Presuponiendo que el usuario se encuentra informado sobre las condiciones en las que sucederá esa mediación parecería absurda esa alienación a cambio de la pérdida de intimidad, sin embargo, desde la óptica del usuario la ganancia de los entornos socioemocionales ubicuos bien valen el costo de sumarse al panóptico digital.

La participación de las personas en los contextos mediacionales contemporáneos implican el uso del medio y su exposición al medio, es decir, no hay medio digital neutral. Sobre estos medios, las personas ven oportunidades para el ejercicio de su identidad, intimidad y sociabilidad, partiendo de una falsa premisa, falsa apariencia de privacidad. Los usuarios no somos conscientes del uso que se hace de su información y de la vulnerabilidad de sus datos ante sus pares y ante las empresas que ofrecen el servicio.

En la actualidad tenemos tan normalizadas la mediación de los espacios socioemocionales (anteriormente de reserva exclusiva, hoy de reserva aparente), que la mayoría de los usuarios aportan datos voluntariamente, como fotos, comentarios, geolocalización. Hoy en las redes sociodigitales se encuentra gran parte de la vida reservada de las personas.

Aunque párrafos arriba se ha dicho que una parte del problema es la cesión voluntaria de datos por parte de las personas, en realidad los dispositivos mediacionales se aprovechan de los mecanismos de la psique humana.

Nuestros mecanismos evolutivos se apropian de la tecnología para extender nuestras capacidades, en este caso las socioemocionales. Estos mecanismos naturalizan la mediación y la transforman en parte de la definición del YO, como en su momento sucedió con el lenguaje o la escritura.

Esto nos regresa al estado inicial de nuestro argumento, lo natural en el ser humano es su estado en constante evolución, en la que hace uso de herramientas y artefactos para catalizar su actividad.

La interiorización de estos dispositivos y su efecto socioemocional puede llegar al punto extremo de que algunas personas se exhiban voluntariamente, aun cuando sea altamente probable que esto acarree consecuencias negativas.

Al respecto, podemos encontrar algunos casos. Por citar dos ejemplos: una chica en una reunión en Ohio transmitió la violación que sufría otra joven por parte de uno de los asistentes (BBC, 2016); en otro caso, una mujer ebria se grabó mientras conducía, y fue reportada por sus propios seguidores (*Las Américas*, 2015).

Estas decisiones vinculadas con la posibilidad de la exhibición pública, de carácter voluntario, accidental o por dolo de un tercero sobre los espacios de reserva aparente de la vida privada, más la capacidad de la creación de registros históricos intangibles de la virtualidad han creado las condiciones necesarias para considerar con seriedad el "derecho al olvido", que enfatiza la libre autodeterminación que tiene la persona de borrar o bloquear información sobre su persona considerada no relevante o que hace algún daño a sus derechos fundamentales (Terwange, 2012).

Internet representa una gran oportunidad en la forma que creamos y conservamos el conocimiento humano, pero también implica una serie de cambios importantes (en mi opinión difícilmente reversibles) sobre la forma en la que establecemos relaciones.

En el pasado el panóptico se encontraban reservado al diseño arquitectónico, específicamente al diseño de las prisiones. Estos arreglos permiten observar al recluso en todo momento, el que gracias a la experiencia fenoménica interioriza que no tendría un sólo momento de privacidad como consecuencia de un acto indebido. En contraste, para el panóptico digital el observador está ahí, no se oculta, pero tampoco se ve, es parte del arreglo y sólo se hace evidente cuando somos parte de una filtración que nos vulnera, sujetos de la venta de publicidad *ad hoc* o enemigos públicos.

RESISTENCIA, MODELAMIENTO Y CIBERPUNKS

¿Estamos en la antesala de un panóptico digital generalizado y permanente?

Cuando surgió esta pregunta, en 2016, no se tenía tan claro el panorama. Hoy en día podemos decir que vivimos en un panóptico digital generalizado y permanente.

Muchos de los argumentos contemporáneos son reactivos al escenario de las filtraciones globales de vigilancia electrónica, lo que estamos atestiguando es el inicio de un nuevo capítulo en la carrera de largo aliento de una tensión entre la seguridad e intereses de las naciones, frente al derecho de la reserva de la intimidad, esta tensión es históricamente larga, pero lo que ha cambiado es la posibilidad y facilidad para hacerlo, parafraseando a Richard Stallman (EFE, 2016), se trata del sueño de cualquier Estado totalitario.

Y como en todo Estado totalitario emergen asociaciones, colectivos y personajes ciberpunk que modelan un estilo de resistencia y argumentación política, que haciendo uso de la informática y criptografía dan una batalla pública, pero teniendo

como escenario los entornos digitales. La propuesta de resistencia de estos ciberpunks es el cifrado, permitiendo que sólo el emisor y el receptor sean quienes puedan decodificar el mensaje. Como todo desarrollo tecnológico podrá ser roto, pero para el gran conjunto de las personas será suficiente para no ser espiados por sus proveedores de servicios.

En la lucha por la salvaguarda de los espacios reservados de las personas con la mediación digital el software libre ayuda en la creación de herramientas de fácil uso que van explorando alternativas, modelando usos y permitiendo que la industria de las telecomunicaciones gire e implemente tecnología en la que originalmente no se encontraba en su área de interés.

Sin embargo, hay otras aristas del panóptico que hay considerar, por citar una, el uso de las cámaras de vigilancia con propósitos policiales, hoy tan populares en las ciudades. Se tiene documentado que estos sistemas son usados de forma discrecional por los sistemas policiacos de forma que cuando las grabaciones son favorables a los cuerpos policiacos hay facilidad para obtenerlas o son filtradas, en contraste cuando se trata de fundamentar una denuncia que podría atentar contra la integridad policiaca, se encuentran una gran dificultad para acceder a estos documentos digitales (R3D, 2019).

En un grado más de la evaluación del video orientado a la vigilancia, encontramos el reconocimiento facial y en la misma magnitud van ventilándose reportes de falsos positivos en los algoritmos de que reconocen el rostro de un posible criminal, por ejemplo, en 2018 la policía de Gales del sur compartió un reporte sobre su uso en la final de una liga de futbol en 2017 y en el que se alertaba sobre las fallas masivas de este tipo de sistemas, en tanto al usarlo en un estudio detectó 2 297 falsos positivos y 173 alertas reales (Omicrono, 2018). En este caso, se trata de siste-

mas de vigilancia con algún tipo de algoritmo para el reconocimiento facial y en la que su finalidad es localizar a personas con algún señalamiento policial, sin embargo esta misma tecnología puede vulnerar el ejercicio de las libertades civiles.

Para nadie es un secreto el grado de vigilancia digital que China ejerce sobre sus ciudadanos, y esto se ha hecho evidente en las protestas de Hong Kong. Las protestas iniciaron en febrero del 2019 cuando China propuso una reforma que permitiría la extradición de ciudadanos a China continental, desde entonces (y hasta octubre del 2019), las tensiones entre ciudadanos y gobierno han escalado.

Los ciudadanos de Hong Kong encontraron formas muy creativas para hacer frente a la vigilancia del gobierno como el derribo de los postes de vigilancia y el uso de punteros láser y linternas intermitentes para cegar las cámaras (*La Izquierda*, 2019), uso de guantes ignífugos y máscaras de gas y conos de señalización de tránsito para recoger y neutralizar los cartuchos de gas lacrimógeno (*El tiempo,* 2019), el uso de inhibidores de RFID (Identificación por radiofrecuencia, nombre que recibe la tecnología, por sus siglas en inglés), tecnología común en tarjetas de transporte y pasaportes y que son capaces de almacenar información que puede vulnerar la identidad de quien la porta (*La Vanguardia*, 2019) y el uso de tarjetas de prepago para el servicio de datos y mensajería cifrada como Telegram, Threema o Wickr o mensajería de proximidad por Bluetooth (*The Objective*, 2019; *La Vanguardia*, 2019), así como la reimplementación de los servicios como Pokemon Go, Tinder o Twitch para difundir información, videos, compartir imágenes o darse cita sin levantar las sospechas del gobierno (*La Vanguardia*, 2019).

Las protestas de Hong Kong han dado muestra de lo que ya sabíamos, la vigilancia electrónica es un hecho y puede ser usada

para vulnerar poblaciones completas, pero también observamos las capacidades de los ciudadanos para hacer frente a un escenario de vigilancia digital muy adverso usando las tecnologías que tienen a su alcance, en lo que Rheingold describe como los usos no planificados de la tecnología por las multitudes inteligentes.

En conclusión, para ayudar a las personas a mantener control sobre las áreas de reserva de su vida en ambientes digitales, se debería actuar en tres vías: fortalecimiento de las regulaciones de protección de la vida privada en entornos digitales, desarrollo de aplicaciones intuitivas que usen por defecto el cifrado en las comunicaciones personales y, finalmente, educar a las personas en la importancia de la protección de sus espacios de intimidad digital y las situaciones límite (como las protestas de Hong Kong) son una buena oportunidad para establecerlas.

BIBLIOGRAFÍA

Abril, Patricia y Eugenio Moreno (2014), "La intimidad europea frente a la privacidad americana", *Indret. Revista para el análisis del Derecho*, 1:4-62.

Associated Press (2010), "Lower Merion School District Settles Webcam Spying Lawsuits For $610,000", *The Huffington Post,* <http://www.huffingtonpost.com/2010/10/11/lower-merion-school-distr_n_758882.html >.

____ (2014), "Roban fotos comprometidas a Jennifer Lawrence, Kirsten Dunst, Kate Upton", *El Confidencial*, <http://www.elconfidencial.com/tecnologia/2014-09-01/roban-fotos-comprometidas-a-jennifer-lawrence-kirsten-dunst-kate-upton_183721/>.

Baladrón, Antonio (2003), "Nuevos modos de construcción de la identidad en la sociedad informacional". *Revista latina de comunicación social*, 6(53).

Bazán, Claudia y Fernando Boveda (2005), "La comunicación vía Internet. Dioses o demonios", *Subjetividad y procesos cognitivos*, 7:72-89.

BBC News Mundo (2016), "La joven acusada de transmitir por Periscope la violación de una amiga", *BBC News Mundo*, <http://www.bbc.com/mundo/noticias/2016/04/160414_periscope_streaming_acusados_violacion_ps>.

Birnie, Sarah y Peter Horvath (2002) Psychological predictors of Internet social communication. *Journal of computer-mediated communication*, 2002, 7 (4): JCMC743, <https://doi.org/10.1111/j.1083-6101.2002.tb00154.x>.

Broadbent, Stefana (2009), How the Internet enables intimacy, *TEDGlobal 2009*, <https://www.ted.com/talks/stefana_broadbent_how_the_internet_enables_intimacy>.

_____ (2015), *Intimacy at Work: How Digital Media Bring Private Life to the Workplace*, Routledge.

Bronfenbrenner, Urie (1986), "Ecology of the family as a context for human development: Research perspectives", *Developmental psychology*, 22(6):723.

Chen, Hsinchun; Roger Chiang y Veda Storey (2012), "Business intelligence and analytics: From big data to big impact", *MIS quarterly*, 36(4):1165-1188.

De Terwangne, Cécile (2012), "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *IDP. Revista de Internet, Derecho y Política*, (13):53-66.

Del Rey, Rosario; Virginia Sánchez y Rosario Ortega (2012), "Prosocial use of the internet in adolescence", *The impact of technology on relationships in educational settings*, Routledge Nueva York, 66-76.

EFE (2016), "Los celulares habrían sido el sueño de Stalin, afirma el fundador del software libre", *Pulso*, <http://pulsoslp.com.mx/2016/05/16/los-celulares-habrian-sido-el-sueno-de-stalin-afirma-el-fundador-del-software-libre>.

El Tiempo (2019), "Las ingeniosas tácticas de manifestantes contra policía en Hong Kong", *El Tiempo*, <https://www.eltiempo.com/mundo/

asia/las-ingeniosas-tacticas-de-los-manifestantes-contra-la-policia-en-hong-400724>.

Fayyad, Usama; Gregory Piatetsky-Shapiro, y Padhraic Smyth (1996), From data mining to knowledge discovery in databases, *AI magazine*, 17(3):37-37.

Ghalioun, Burhan (1998), "Globalización, deculturación y crisis de identidad", *Revista CIDOB d'Afers Internacionals*, CIDOB, 123(43/44):107-118.

Giddens, Anthony (1995), *La transformación de la intimidad*, Madrid, Ediciones Cátedra, 124 pp.

Gross, Elisheva; Jaana Juvonen y Shelly Gable (2002), "Internet use and well-being in adolescence", *Journal of Social Issues*, 58(1):75-90.

Kang, Tingyu (2012), "Gendered media, changing intimacy: Internet-mediated transnational communication in the family sphere", *Media, Culture y Society*, 34(2):146-161.

Klein, Naomi (2007), *The shock doctrine: The rise of disaster capitalism,* New York, Picador, 720 pp.

La Izquierda (2019), "Manifestantes destruyen cámaras de reconocimiento facial en Hong Kong", *La Izquierda*, <https://www.laizquierdadiario.com/Manifestantes-destruyen-camaras-de-reconocimiento-facial-en-Hong-Kong>.

Las Américas (2015), "Mujer ebria se graba con Periscope y termina en la cárcel. Diario *Las Américas*, <http://www.diariolasamericas.com/4842_locales/3396155_mujer-ebria-graba-periscope-carcel-florida.html>.

La Vanguardia (2019), "Así usan el camuflaje digital los manifestantes de Hong Kong", *La Vanguardia*, <https://www.lavanguardia.com/tecnologia/20190919/47465599843/hong-kong-tecnologia-camuflaje-vigilancia-mensajeria-telegram-criptografia.html>.

Linne, Joaquín (2014), "Después de la ampliación de la internet hogareña: los adolescentes de sectores populares y los cibers en la Ciudad de Buenos Aires", *Signo y Pensamiento* 33(65):70-83, julio-diciembre.

Livingstone, Sonia (2008), "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression", *New media & society*, 10(3):393-411.

McAfee, Andrew *et al.* (2012) "Big data: the management revolution", *Harvard Business Review,* 90(10):60-68.

McKenna, Katelyn; Amie Green y Marci Gleason (2002), "Relationship formation on the Internet: What's the big attraction?", *Journal of Social Issues*, 58(1):9-31.

Muñoz, Miguel (2014), "La tensión entre privacidad y seguridad en el desarrollo de internet", *Dilemata*, (15):181-193.

Navas, Antonio (2010), "Síntesis y valoración de la teoría sobre el desarrollo moral de Lawrence Kohlberg", *Agora*, 29(2):31-54.

Omicrono (2019), "2 300 inocentes marcados como criminales en una noche, el problema del reconocimiento facial", *omicrono*, <https://www.elespanol.com/omicrono/tecnologia/20180507/inocentes-marcados-criminales-noche-problema-reconocimiento-facial/305470658_0.html>

Papalia, Diane; Sally Wendkos y Ruth Duskin (2010), *Desarrollo humano. De la infancia a la adolescencia*. México: Mc Graw Hill.

Penney, Jonathon (2016), "Chilling Effects: Online Surveillance and Wikipedia Use", *Berkeley Technology Law Journal*, 31(1):117:182.

Ponce, Frida (2014), "Remote Homes: Towards a Nomadic Urbanism?", *The Mediated City Conferece,* London: 01, 03 April, 2014.

R3D (2019), "Las cámaras corporales no son una solución mágica contra los abusos de la policía, *R3D*, https://r3d.mx/2019/10/02/las-camaras-corporales-no-son-una-solucion-magica-contra-los-abusos-de-la-policia/.

Real Academia Española (2014), intimidad, *Diccionario de la lengua española*, Madrid, Real Academia Española, <https://dle.rae.es/intimidad>.

Reuters (2015), "La NSA infectó discos duros de marcas famosas para espiar a países claves", *ABC*, http://www.abc.es/tecnologia/redes/20150217/abci-hackers-espionaje-ordenadores-201502171314.html.

Rheingold, Howard (2004), *Multitudes inteligentes*, Barcelona, Gedisa, 286 pp.

Sánchez, Julio (2015), "Vulneración a Hacking Team confirma abuso de espionaje en México", *El Economista*, <https://www.eleconomista.com.mx/tecnologia/Vulneracion-a-Hacking-Team-confirma-abuso-de-espionaje-en-Mexico-20150706-0055.html>.

Saramago, José (2002), "¿ Para qué sirve la comunicación", *José Saramago, (comp.), El Mito Internet, Selección de artículos de Le Monde Diplomatique, Santiago de Chile: Aún Creemos en los Sueños*, 9-12.

The Objective (2019), "Protestas del futuro: así burlan en Hong Kong a la policía tecnológica"*, The Objective*, <https://theobjective.com/further/protestas-del-futuro-asi-burlan-en-hong-kong-a-la-policia-tecnologica>.

Vacarezza, Ricardo (2000), "De los derechos del paciente", *Revista médica de Chile*, 128(12):1380-1384.

Wertsch, James (1988), *La formación social de la mente*, Barcelona, Paidós, 264 pp.

Wolf, Gunnar (2013), "Privacidad, vigilancia, filtraciones, y el resto de nosotros", *Software Gurú* (42):46-47.

Zegers, Beatriz y María Larraín (2011), "El impacto de la Internet en la definición de la identidad juvenil: una revisión", *PSYKHE,* 11(1):203-216.

2

RIESGOS INHERENTES EN LA PRIVACIDAD DE LAS PERSONAS POR EL USO DE LAS TIC

Juan Carlos Pérez

Hoy en día las tecnologías de la información y comunicación (TIC) forman parte integral de nuestra vida diaria. Facilitando tareas mediante el uso de computadoras, dispositivos inteligentes, teléfonos, tabletas, *weareables* y tecnologías emergentes como el Internet de las Cosas (IoT, por sus siglas en inglés). Esto nos ha conducido a llevar una vida digital con el uso de estos dispositivos que cuenta con software y sensores que recopilan información personal de cada usuario destinada a alimentar sus expedientes digitales con la finalidad declarada de brindar una mejor experiencia de usuario en productos y servicios consumidos por medio de estos dispositivos.

Sin embargo, el progreso tecnológico también acarrea riesgos inherentes. En el caso de las TIC, abren una puerta trasera de nuestra vida privada, no solo a las empresas que comercian con nuestra información, sino a la vigilancia por parte del Estado o husmeadores de nuestra vida íntima. Estas intrusiones pueden desencadenar perjuicios de distintas dimensiones a los usuarios. Se propone un análisis de este tipo de riesgos, partiendo

del significado de privacidad, características de la información y comportamientos de la sociedad.

Debido a que hemos comenzado a vivir una vida dual; una vida física y otra digital en línea, donde existimos como una entidad virtual (Chauhan y Panda, 2015) que posee nuestros datos personales, financieros, geolocalización, gustos y preferencias. El comportamiento de dicha entidad en el ciberespacio o algún mundo virtual, en gran medida depende de nosotros ya que al encontrarnos inmersos en ese entorno vamos perdiendo la capacidad de distinguir entre lo público y lo privado. Ámbito que nos es tan importante en la vida real (Albornoz, 2016).

Por lo cual, es importante conocer la diferencia entre lo público y lo privado, Rabotnikof (1998) plantea tres criterios para distinguir entre lo público y lo privado.

- *Colectividad*. Donde lo público es plural y lo privado singular. De este modo lo público puede ser de interés de una comunidad, un pueblo, un país e incluso global. En el mundo de internet existen comunidades de diversos tipos con individuos que físicamente se encuentran en distintos puntos geográficos del mundo, pero que aun así mantienen un interés común. Lo privado es de interés individual, referido al uso de las tecnologías podemos limitarlo a dispositivos de uso personal como la computadora personal, el teléfono inteligente u otro dispositivo capaz de almacenar información que solo es relevante para el individuo.
- *Visibilidad.* Con este criterio lo público es visible, volviendo a la analogía con el mundo de internet, lo público es aquello que pone a la vista, ya sea en perfiles de redes sociales, sitios de internet, pantallas con anuncios, etc. También podríamos referirnos no solo a lo visible si no a

lo que es audible, aquello que escuchamos en nuestros dispositivos. Para Rabotnikof (1998) con este criterio define lo público como aquellas actividades que realizamos a la mirada de otros. Lo privado se mantiene oculto, en secreto, es aquello que mantenemos almacenado en nuestros dispositivos para que no pueda ser visualizado o escuchado en dispositivos de terceros. Pudiendo también ocultar accesos o información en sitios de internet o aplicaciones, por distintos motivos, con el principal criterio de colectividad que hace referencia a lo privado como algo de interés individual o de unos cuantos.

- *Accesibilidad.* Hace referencia a la apertura y la clausura. En el caso de lo público, lo que es accesible para todos, puede referirse a lugares públicos. En internet, las redes sociales son un ejemplo claro en donde los usuarios pueden abrir al público sus perfiles y sus contenidos para ser visualizados sin restricción por cualquier persona.

Esta autora (Rabotnikof, 1998) también expone que a partir del criterio de accesibilidad se deriva el sustantivo "el público", que hace referencia a todos aquellos que se benefician de la accesibilidad, que con las TIC se puede ver potenciada en número de personas y lugares. Estos tres criterios regularmente son congruentes entre sí y pueden ayudar a delimitar la línea entre lo público y lo privado. Está en una línea delgada que varía en el tiempo, los principios éticos y morales de cada individuo o sociedad.

Es aquí donde toma relevancia lo mencionado por Albornoz (2016), con el uso de las TIC como internet, redes sociales y videojuegos en línea que proveen mundos virtuales, vamos perdiendo la capacidad de distinguir entre lo público y lo privado.

Por su parte Solove (2002) conceptualiza la privacidad con base en seis criterios, que se complementan con los tres anteriores, para diferenciar entre lo público y lo privado.

1. El derecho a estar solo: el llamado *Right to be alone,* formulado en el ensayo "The Right to Privacy" (Warren y Brandeis, 1890), donde el aislarse de los demás está sustentado en dos criterios, uno espacial y otro de visibilidad planteado por Rabotnikof (1998), en el que es posible apartar sus actividades de la mirada de otros y se considera un derecho.
2. Acceso limitado al YO: en este caso el criterio de accesibilidad es específico al YO. Solove (2002) lo plantea como la capacidad de protegerse del acceso no deseado por parte de otros. En este caso es una combinación del criterio de colectividad y accesibilidad donde para la privacidad aplica el interés individual y la clausura.
3. Secreto: este criterio de visibilidad también planteado por Rabotnikof, se refiere a la ocultación de actividades y asuntos a terceros.
4, Control sobre la información personal: la capacidad de ejercer control sobre la información propia. En nuestra opinión, este criterio es interesante ya que trata directamente sobre el control de los datos personales, aplicando mecanismos que permitan la combinación de los criterios de colectividad, visibilidad y accesibilidad de Rabotnikof en su cualidad de lo privado, es decir, manteniendo el interés individual, el secreto y la clausura sobre la información personal para restringir la accesibilidad y visualización de su información.
5. Personalidad: este criterio plantea la protección de la per-

sonalidad, la individualidad y la dignidad. De acuerdo con Garzón Valdés (2012), el desvelamiento de la propia intimidad significa la eliminación o la reducción de lo secreto, de sentimientos y pensamientos muchas veces confusos o transitorios, difíciles de ser aprehendidos cabalmente por otro. El criterio de visibilidad, en este caso, no es suficiente para explicar la protección de la personalidad ya que lo mostrado de la propia intimidad puede ser información no integral y difícil de interpretar, lo cual de acuerdo con Garzón puede ofrecer una versión distorsionada de nuestra propia personalidad.

6. Control sobre la intimidad: para Solove (2002), implica el control sobre, o acceso limitado a, aspectos de la vida o relaciones íntimas del individuo. Lo que implica la administración de accesibilidad a la intimidad.

En la tabla 1 se vinculan los criterios de Solove (2002) para conceptualizar y concebir la privacidad, y los criterios de colectividad, visibilidad y accesibilidad en su carácter de privado planteados por Rabotnikof (1998) donde se identifica qué criterios son necesarios para cumplir cada una de las concepciones de privacidad.

Aquí vemos una correspondencia entre los criterios de privacidad de Solove y los criterios de interés individual (colectividad), secreto (visibilidad) y clausura (accesibilidad). Donde destaca el "Control sobre la información personal", que no solo corresponde con uno o dos de los criterios, sino que se vincula con los tres criterios para poder concebir un adecuado control de dicha información.

Debido a que la información no escapa de estos criterios de público y privado, ya que siempre ha sido un activo esencial

Tabla 1
Concepción de privacidad y sus criterios

Concepción de privacidad	*Concepción de privacidad*
Derecho a estar solo	Visibilidad (secreto)
Acceso limitado al YO	Accesibilidad (clausura)
Secreto	Visibilidad (secreto)
Control sobre la información personal	Colectividad (interés individual), Visibilidad (secreto) y accesibilidad (clausura)
Personalidad	Visibilidad (secreto) y accesibilidad (clausura)
Control sobre la intimidad	Accesibilidad (clausura)

Fuente: Elaborada con datos de Rabotnikof (1998) y Solove (2002).

para los seres humanos, les ha brindado ventajas sobre otros en varios ámbitos de la vida, que van desde lo personal hasta lo organizacional. Siempre se ha buscado proteger la información valiosa y mantenerla secreta para unos cuantos.

Datos ordenados generan información, la cual es base del conocimiento. Datos personales agrupados y analizados generan información personal. La confidencialidad, integridad y disponibilidad son características de la información y forman la triada CIA, por sus siglas en inglés (Confidentiality, Integrity, Avaliability), y son definidas por Krustz y Vines como:

1. *Confidencialidad*, es la prevención de la divulgación no autorizada o no intencional de contenidos.
2. *Integridad*, es la garantía de que la información no se altera intencional o no intencionalmente.
3. *Disponibilidad*, refiere a que pueda ser utilizado cuando sea necesario, por personas autorizadas. Refiere a elementos que crean confiabilidad y estabilidad en redes y sistemas.

Características alcanzadas mediante la seguridad de la información, que es el conjunto de medidas para la protección de la información y sistemas de información contra el acceso, uso, revelación, interrupción, modificación o destrucción no autorizados a fin de proporcionar confidencialidad, integridad y disponibilidad (Kissel, 2013).

De acuerdo con el glosario de los principales términos de seguridad de la información del Instituto Nacional de Normas y Tecnología, Departamento de Comercio de Estados Unidos (2013), mantener la integridad de la información implica protección contra información inadecuada, modificación o destrucción, e incluye el no rechazo y la autenticidad.

La tabla 2 vincula las características de la información, con los criterios de lo privado planteados por Rabotnikof (1998). Para determinar la importancia de dichos criterios en el control sobre la información personal y privada, donde la confidencialidad pasa a ser la característica más relevante al corresponder con los criterios de interés individual, la secrecía y la clausura de la accesibilidad a dicha información.

La integridad depende de la accesibilidad para mantenerse y evitar su modificación o destrucción. Mientras la disponibilidad

Tabla 2
Características de la información y criterios privados

Concepción de privacidad	*Concepción de privacidad*
Confidencialidad	Colectividad (interés individual)
Visibilidad (secreto)	Accesibilidad (clausura)
Integridad	Accesibilidad (clausura)
Disponibilidad	Colectividad (interés individual)
Visibilidad (secreto)	Accesibilidad (clausura)

Fuente: Elaborada con datos de Rabotnikov (1998) y Kissel (2013).

echa mano de la colectividad y la accesibilidad para procurar el acceso controlado a la información y que esté disponible solo para quien le es de interés personal la información y tenga acceso para visualizar o clausurar el acceso para quienes no les sea de incumbencia.

Hay diversos tipos de amenazas informáticas y técnicas utilizadas por *hackers* y delincuentes informáticos para obtener datos e información personal, que ponen en peligro la privacidad de los usuarios de las TIC, siendo un peligro para la pérdida del control de la información personal, el acceso limitado al YO y el secreto.

La privacidad es un derecho que se ha desarrollado por más de 3 000 años (Ferenstein, 2015) plasmado como derecho humano en el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) en 1948 así como en el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos de 1976.

El auge de las TIC y la interconexión de millones de personas por medio de estas tecnologías, principalmente mediante internet y redes sociales, las ha convertido en parte integral de nuestra vida. Sin embargo, esta facilidad de acceso a la información, rapidez en la transmisión de datos y el bajo costo en la comunicación trae consigo riesgos (Sancho, 2017).

A lo largo de la historia, han existido personas dispuestas a comerciar privacidad por conveniencia, riqueza o fama (Ferenstein, 2015). Hoy en día, esta práctica es común entre individuos que van desde *youtubers*, *bloggers* y hasta usuarios comunes de redes sociales, quienes ponen en riesgo su privacidad.

Aunque los usuarios periódicamente reciben información sobre nuevos ciberdelitos ante los cuales están desprotegidos (Sancho, 2017) están cada vez más conscientes de los riesgos que implica el uso de la tecnología, al adquirir un nuevo dispositivo

y demandan seguridad y privacidad, pero esa preocupación no la reflejan en sus hábitos y prácticas de seguridad (O'Brien, Budish, Faris, Gasser y Lin, 2016).

Debido al uso de internet, los usuarios propagan huellas digitales (*digital footprints*) las cuales son los rastros que dejamos cuando utilizamos internet (Society, 2014) que en su conjunto conforman expedientes digitales de cada uno de los usuarios. Cada foto en redes sociales, información de contacto, fecha de nacimiento, estado de ánimo, datos bancarios, relaciones sentimentales, gustos, preferencias, formación académica, ubicación u otro tipo de huella digital pone en riesgo nuestra privacidad e incluso la de terceros. Lo cual abre las puertas a una intromisión a nuestra esfera de intimidad por parte de usuarios maliciosos o ciberdelincuentes que pueden hacer mal uso de información sensible que fácilmente puede ocasionar algún perjuicio.

Así, también los perfiles de redes sociales se vuelven una representación de la realidad y en ellas los individuos pueden perder la noción entre lo público y lo privado, así también pueden comportarse en una forma distinta a como lo hacen en la realidad mostrando una versión distorsionada de su personalidad.

La sociedad ha sido calificada por el sociólogo alemán Ulrich Beck (1998) como una sociedad de riesgo, donde los mismos avances de la industria y la modernización se ven acompañados de riesgos y peligros que contaminan y dañan el medio ambiente así como a los individuos víctimas de esa contaminación.

En la actualidad es un hecho que la producción de las TIC y la basura electrónica contaminan el ecosistema, además estas tecnologías son sensibles a la contaminación por software malicioso creado también por usuarios maliciosos que además utilizan técnicas como la ingeniería social, convirtiendo a los usuarios de las TIC en víctimas que están en peligro de perder el

control sobre la información que se administra y procesa en sus dispositivos.

Beck (1998), señala que en la antigüedad, a diferencia de la actualidad, los peligros eran perceptibles mediante los sentidos, mientras que los riesgos civilizatorios escapan a la percepción, tal es el caso de aquellos riesgos que acompañan a las TIC, donde la mayoría de éstos se vuelven intangibles. De tal manera que con la modernización evolucionan los riesgos, los cuales son esencialmente consecuencia del desarrollo técnico económico mismo.

Con la llegada y masificación de las TIC con sus nuevos riesgos inherentes a su uso, tanto para dispositivos y la información sensible que en ellos se procesa y almacena la cual puede derivar en perjuicios financieros, morales o de bienestar de un individuo o una sociedad entera. Dando la posibilidad de poner al usuario en un papel de víctima, victimario, espectador o juez. Debido a la masificación de colectividad, visibilidad y accesibilidad que permiten las TIC.

Para Beck, al igual que el reparto de la riqueza, los riesgos se reparten de forma desigual, existiendo privilegiados como aquellos que tienen poder ya sea económico o de educación. Siendo el riesgo y la seguridad un gran negocio como lo describe Beck, ya que actualmente los consumidores son dependientes de los proveedores en cuanto a seguridad y privacidad (O'Brien *et al*., 2016), se refiere y los usuarios con mayor poder (económico o educativo) pueden mitigar el riesgo adquiriendo dispositivos más caros y seguros, mientras los usuarios comunes prefieren menor precio e ignoran los conocimientos necesarios para tomar decisiones de compra para aumentar su seguridad y privacidad.

Los riesgos de la modernización afectan más tarde o más temprano también a quienes los producen o se benefician de ellos (Beck, 1998). Lo que hace tener un efecto búmerang, ya que

aquellos con mayor poder económico y capacidad de mitigación de riesgo, se vuelven blanco de esos riesgos al tener más que perder.

Douglas, una de las críticas de Beck, considera que la percepción de un riesgo también depende de las nociones éticas y morales (citado en Montenegro, 2005). Por lo tanto, en cuanto a la afectación, los mismos ataques pueden tener un significado completamente diferente para personas distintas de acuerdo con la edad, el sexo, los hábitos alimenticios, el tipo de trabajo, la información, la educación, etc. Por lo cual, el análisis del riesgo de su información privada varía de persona en persona.

Para Douglas (Montenegro, 2005), las formas de percibir los riesgos se ordenarían según códigos privilegiados, por lo cual el usuario común no ve los riesgos igual que los expertos, debido a privilegios técnicos o de educación. Ya que la educación y un comportamiento sensible en relación a la información abren nuevas posibilidades de enfrentarse a los riesgos y evitarlos.

De igual forma para Beck y Douglas, citados por Montenegro (2005), el problema de los riesgos no se vincula a un proceso de educación, ya que supondría aceptar la teoría de que los sujetos podrán realizar una elección probabilística de determinados peligros. Donde Douglas introduce el concepto de "inmunidad subjetiva", presentada en la tabla 3, se subestiman los riesgos que se consideren controlados y sean vinculables a los acontecimientos que se dan rara vez.

Tabla 3
Percepción del riesgo "inmunidad subjetiva"

Peligros cotidianos más comunes	Riesgo considerado	Peligros de baja probabilidad

Fuente: Elaborada con datos de Douglas citado por Montenegro (2005).

Con dicha consideración, "inmunidad subjetiva" se reduce considerablemente la percepción de los peligros en un análisis de riesgo. Lo que puede hacer creer a un usuario que su información privada está más segura.

Creando una tolerancia al riesgo estableciendo valores de aceptabilidad de acuerdo con el sistema cultural en el que se fraguan los niveles éticos y morales (Montenegro, 2005). Lo que se traduce en la aceptación del riesgo por parte de los usuarios de la vulneración de la privacidad mediante las TIC.

Una vez que usted tome en cuenta las medidas recomendadas, considere la tolerancia al riesgo de la privacidad que está dispuesto a aceptar, si cree que aun así corre un riesgo alto, replantee la colectividad, visibilidad y accesibilidad de sus datos por medio de las TIC.

CONCLUSIONES

Con base en lo anterior, se infiere la concepción de privacidad a partir de los criterios establecidos por Rabotnikof (1998) y Solove (2002), centrando la atención en los riesgos generados a ésta por el uso de las TIC. Donde la información privada desempeña un papel de relevancia al contener datos personales y huellas digitales que conforman expedientes digitales de todos y cada uno de los usuarios de las TIC. Información que cuenta con las características de confidencialidad, integridad y disponibilidad que se empatan con los criterios de colectividad, visibilidad y accesibilidad en su carácter de lo privado. Se llega a la conclusión de que toda la información privada por medio de cualquier TIC debe contar con dichos criterios para mantener la cualidad de privado.

Debido a los riesgos inherentes a la modernización y el uso masivo de las TIC, los usuarios deberían ser capaces de percibir

los riesgos de intrusión a sus dispositivos e información personal, no solo obteniendo una posición de poder económico que les permita adquirir dispositivos más caros y con mayor seguridad, sino por medio de un proceso de educación y capacitación por parte de expertos u obtención y estudio de más y mejor información del uso de las TIC. Para lo cual es importante siempre realizar un análisis de riesgo de éstas que puedan abrir una puerta a nuestra privacidad, debido a los perjuicios que pueda causar una intromisión no autorizada en nuestra vida íntima, así como sus efectos secundarios debido a la potencialización de la colectividad, visibilidad y accesibilidad que puede alcanzarse con las nuevas tecnologías; mismos criterios que deben incluirse en un análisis de riesgo considerando los valores y principios éticos personales, y de la sociedad en la que nos encontramos, ya que las afectaciones en cada individuo dependen de estos valores.

Es importante analizar la producción de riesgos por parte del usuario, evitando delegar por completo a terceros la seguridad de nuestros datos personales y el acceso a nuestra vida privada, así como disminuir la tolerancia al riesgo, reduciendo los extremos de la "inmunidad subjetiva" no subestimando los riesgos que se consideren controlados y los peligros de baja probabilidad, debido al importante perjuicio que pueden ocasionar a los usuarios.

Tal es la magnitud y evolución de los riesgos que suelen surgir comunidades para mitigar amenazas. Como lo son los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés). Centros a los que los usuarios pueden acercarse para obtener información relacionada con amenazas de seguridad informática, así como medidas de prevención.

BIBLIOGRAFÍA

Albornoz, M. B. (2016). "Cibercultura y las nuevas nociones de privacidad", *Nomadas*, 28. Recuperado a partir de http://nomadas.ucentral.edu.co/index.php/21-ciberculturas-metaforas-practicas-sociales-y-colectivos-en-red-nomadas-28/258-cibercultura-y-las-nuevas-nociones-de-privacidad

Beck, U. (1998). *La sociedad del riesgo*. Vasa. https://doi.org/10.2307/2579937

Chauhan, S., y N. K. Panda (2015). *Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques* (1a. ed.). Amsterdam: Syngress.

Ferenstein, G. (2015). "The Birth And Death Of Privacy: 3,000 Years of History Told Through 46 Images", *Medium*. Recuperado a partir de https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e.

Garzón Valdés, E. (2012). *Lo íntimo, lo privado y lo público*. IFAI, Ed. (5a. ed.). Méxi. Recuperado a partir de http://187.216.193.232/biblos-imdf/sites/default/files/archivos/00482CuadernosdetransparenciaIFAI06.pdf.

Kissel, R. L. (2013). *Glossary of Key Information Security Terms.* NIST Interagency/Internal Report (NISTIR) - 7298rev2. Recuperado de https://www.nist.gov/publications/glossary-key-information-security-terms-1.

Krutz, R. L., y R. D. Vines (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* (1a. ed.). Indianapolis: Wiley.

Montenegro, S. M. (2005). *La sociología de la sociedad del riesgo: Ulrich Beck y sus críticos.* Pampa, 1(1), pp. 117-130. Recuperado de http://www.colsan.edu.mx/investigacion/PAYS/archivo/La_sociologia_sociedad_del_riesgo.pdf

O'Brien, D.; R. Budish; R. Faris; U. Gasser, y T. Lin (2016). "Privacy and Cybersecurity Research Briefing", Rochester, NY, *Social Science Research Network*. Recuperado a partir de https://papers.ssrn.com/abstract=2842801.

Rabotnikof, N. (1998). "Público-Privado". *Debate Feminista*, 18, 3-13. Recuperado a partir de http://www.jstor.org/stable/42625368.

Sancho, C. (2017). "Ciberseguridad. Presentación del dossier/Cybersecurity". Introduction to Dossier. URVIO - *Revista Latinoamericana de Estudios de Seguridad*, 0(20), 8–15. https://doi.org/10.17141/urvio.20.2017.2859.

Society, I. (2014). "Digital Footprints: An Internet Society Reference Framework | Internet Society". *Internet Society*. Recuperado a partir de https://www.internetsociety.org/doc/digital-footprints-internet-society-reference-frameworkchauhan.

Solove, D. J. (2002). *Conceptualizing Privacy*. Recuperado a partir de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103.

Warren, S., y L. D. Brandeis (1890). "The right to privacy". *Harvard Law Review.*

3
AVENTURAS Y AVATARES DE UN ACADÉMICO QUE SE PROPUSO USAR TOR

Raúl Ornelas

Hace algunos años, como parte del Instituto de Investigaciones Económicas de la UNAM y el Observatorio Latinoamericano de Geopolítica (OLAG), donde trabajamos temas como hegemonía mundial, competencia entre corporaciones trasnacionales, militarización, nuevas tecnologías, y en particular, nuevas tecnologías de control social —es decir, con informaciones de los sectores militares y gubernamentales de México y Estados Unidos— nos preocupó la posibilidad de que, al visitar ciertos sitios en internet, nuestras informaciones fueran retenidas, analizadas y eventualmente utilizadas para localizar desde dónde nos conectábamos, a través de nuestras direcciones IP, y por esa vía, dar directamente con nosotros.

Comparto aquí mi experiencia en el uso de Tor, una tecnología de anonimato en internet, para ofrecer una perspectiva distinta a la de los creadores de estas tecnologías especializadas y la de los promotores de su uso, esperando con ello establecer un diálogo que ayude al conocimiento, difusión y mejora de ellas.

En otro sentido, cabe destacar que en nuestra experiencia hallamos un uso no previsto de Tor: superar las restricciones de algunos sitios de información, especialmente diarios y revistas, que en la búsqueda de rentabilizar sus contenidos, ofrecen un número limitado de artículos. A través de la función de "nueva identidad" hemos logrado un acceso irrestricto a tales sitios, como sería el caso de *The Economist*, *Le Monde*, *New York Times*, etcétera.

De este recorrido, se distinguirá un tema esencial para el uso de las tecnologías de anonimato: establecer cuál es la necesidad a la que se debe atender. Entre la tecnología "genérica" que entregan los programadores y las maneras en que es utilizada, hay una gran cantidad de tareas de aprendizaje y adaptación a tomar en cuenta si queremos que el uso de tecnologías de anonimato se generalice. Si las tareas de aprendizaje son atendidas a través de recursos genéricos como manuales de instalación y configuración, "preguntas frecuentes" y foros de discusión, las tareas de adaptación requieren de una mayor proximidad entre quien conoce las tecnologías y quien las utiliza. Al igual que con todo el software libre, es necesario contar con una instancia dedicada a responder cuestiones específicas a los ambientes en que se intenta implantar las tecnologías de anonimato.

CRONOLOGÍA

Hace un par de años, en OLAG, conocimos la existencia de un conjunto de instituciones dedicadas al espionaje, en México y el mundo, y elaboramos una presentación general del sistema ECHELON, herencia y desarrollo de las prácticas de espionaje y la llamada "inteligencia" durante la segunda guerra mundial, sistema anclado en el mundo anglosajón. Tiempo después, las reve-

laciones de WikiLeaks y Edward Snowden nos mostraron nuevas prácticas comunes de los gobiernos a todos los niveles: intrusiones a la vida privada, vigilancia sobre personas que son críticas del sistema, creación de enemigos siguiendo las doctrinas de la guerra asimétrica y de la dominación de espectro completo, y de manera alarmante, la "creación de evidencias" para acusar y encarcelar injustamente a esas personas que resultan "incómodas" al sistema imperante.

Frente a tales realidades, nos pareció obvio buscar formas de protegernos de las intrusiones y otras prácticas de espionaje, y de ahí nació el doble interés de, por una parte, conocer las tecnologías de espionaje cibernético y, por otra, indagar sobre las medidas que permiten evadir las prácticas intrusivas.

De aquel tiempo, recuerdo que iniciamos con *scripts* para cambiar en cada arranque de las máquinas las direcciones MAC, nuestro fomento del uso de sistemas GNU-Linux, particularmente de la distribución Debian, y el uso de Tor. Las preocupaciones sobre eventuales intrusiones fueron atendidas a través de medidas "cosméticas" como la clásica cobertura del lente de la cámara de las computadoras, la inhabilitación del micrófono, y la consigna de no guardar informaciones personales en las máquinas de uso "profesional".

Fue a partir de indagaciones muy elementales, y gracias a las mejoras del programa Tor en su empaquetamiento y el lanzamiento de su navegador (browser) que elegimos esta tecnología como la solución con mejor desempeño para lograr un mínimo de anonimato en nuestro trabajo con las fuentes que podrían implicar prácticas de vigilancia e intrusión. Estos pequeños cambios resultan esenciales en crear una cultura informática común a programadores, militantes y usuarios. Antes de ello, el uso de Tor estaba limitado, pues requería instalarlo y configurarlo a través

de la línea de comandos. Aunque se trataba de operaciones sencillas, fáciles de codificar en manuales del usuario, esas acciones son ajenas al usuario lego, dependiente de la cultura Windows que nos ha condicionado a instalar y configurar programas con el "doble click". Nunca está de más reiterar que facilitar el uso de los programas no es una traición a la filosofía del software libre, sino, por el contrario, una de los mejores medios para su difusión.

Una vez que nos colocamos en la vía del uso de Tor, aparecieron dos dificultades significativas para consolidar en nuestro equipo el recurso a esta tecnología. La primera es quizá las más comentada y conocida: la ralentización de las conexiones, que hace algunos años era significativa, en particular para los sitios que tienen gran cantidad de información y, por tanto, su despliegue a través de Tor resultaba poco útil dado el tiempo que tomaba: la obtención de información tiene un ritmo que no es compatible con conexiones más lentas que la velocidad promedio habitual. La segunda dificultad ha sido la prohibición de ejecución de ciertos programas, especialmente Flash y Java, debido a las reservas de Tor que evitan tales programas, dado que, eventualmente, pueden facilitar la localización de las conexiones. Esto es relevante porque muchos de los sitios más "profesionales", sitios gubernamentales y empresariales, utilizaban esos programas, de suerte que Tor no era una opción para visitarlos: la elección en estos casos era sencilla, tales sitios deben ser visitados sin Tor, o desactivando algunas de sus restricciones, y por tanto, poniendo en riesgo el anonimato.

Es importante decir que ambas dificultades han disminuido, gracias al aumento del débito de las redes, al crecimiento de los nodos (relays) de Tor, que permiten conexiones anonimizadas más rápidas, así como por el abandono de las tecnologías que

permiten la localización de las conexiones en la mayoría de los sitios que nos interesan. Cabe anotar que en los últimos dos años hemos encontrado una tercera dificultad para conectarnos a través de Tor a sitios que tienen algún tipo de protección, suponemos que contra ataques de denegación de acceso, y esto afecta sobre todo a sitios gubernamentales y de iniciativas políticas "opositoras" (por ejemplo, el sitio de Radio Mundo Real http://rmr.fm).

Como sabemos, en el terreno de las tecnologías de la información y la comunicación, las dificultades técnicas tienden a ser superadas a través de mejoras de las tecnologías involucradas; sin embargo, el aspecto que consideramos cualitativo en el uso de las tecnologías de anonimato es el "factor" humano. En nuestra experiencia, el principal obstáculo para la implantación y la consolidación del uso de Tor fue la dificultad para tomar conciencia, tanto de los riesgos, de las formas en que tales riesgos se concretan en tecnologías y prácticas de espionaje e intrusión, como de lo que está en juego, y que va más allá de las consecuencias directas para los integrantes y el propio grupo de investigación. Esta cuestión impide comprender que al practicar el anonimato no sólo nos protegemos sino que ayudamos a combatir prácticas nefastas por parte de instancias gubernamentales y poderes fácticos, por ejemplo, las empresas que recopilan informaciones personales para luego comercializarlas. Tal incomprensión fracturó una cuestión esencial en el uso de Tor: que todos los integrantes del equipo lo utilicen.

Este conjunto de dificultades ha hecho que el uso de las tecnologías de anonimato sea parcial y, por tanto, se haya perdido el objetivo inmediato, que era proteger nuestras conexiones a sitios que pudieran estar practicando la vigilancia o intentando las intrusiones a los equipos clientes.

A MANERA DE CONCLUSIÓN

Después de este recorrido, tenemos tres ideas generales que pueden servirnos para mejorar el uso de las tecnologías del anonimato.

En primer lugar, es preciso trabajar el tema de la cultura informática. El dominio del paradigma Windows obliga a hacer un trabajo educativo que ha sido ya emprendido de larga data por los creadores y las instancias coordinadoras del software libre. Es preciso difundir y desarrollar la "filosofía del software libre" para crear el terreno común que permita comprender la importancia del uso de las tecnologías de anonimato, enfatizando, tanto los riesgos actualmente existentes, como la importancia del uso de estas tecnologías para el conjunto de sociedades enfrentadas a gobiernos e instituciones intrusivas y proclives al espionaje y la represión.

En segundo lugar, y ligado con lo anterior, es preciso que las soluciones tecnológicas sean integrales. En un primer paso, debemos fomentar no sólo el uso de Tor sino también el de los sistemas operativos menos sujetos a los imperativos comerciales y a las manipulaciones que facilitan el espionaje, las intrusiones y la comercialización de la información que manejamos y producimos. Sabemos que la discusión sobre qué distribución de Linux es la más adecuada para estas tareas es muy amplia, pero hay un punto que puede servir como referencia inicial: qué distribución de Linux permite llevar a cabo las prácticas de anonimato de la mejor manera posible.

Un tercer tema es de orden cualitativo y tiene que ver con cómo "traducimos" las complejas cuestiones que implican las prácticas de control social, para que sean motivo de atención y acción del mayor número de personas posible. En general, la

respuesta ante la propuesta de uso de tecnologías de anonimato es el terrible sentido común de que "el que nada debe, nada teme", y la calificación de los usuarios de esas tecnologías como "paranoicos". Se trata de construir colectivamente prácticas y opciones tecnológicas y comunicativas que muestren la importancia estratégica del control social contemporáneo, no sólo en los casos de represión política y social, sino directamente en la vida cotidiana de los usuarios de las redes y de las tecnologías de la información y la comunicación.

Finalmente, y como un tema colateral y no obstante, muy urgente, hay otro campo esencial para fomentar el uso del software libre y para la adopción de las tecnologías de anonimato que es la mejora y ampliación de las opciones de "paquetería" de código abierto. En muchas ocasiones, mantenerse en la órbita Windows (o para el caso, Mac) depende de la inexistencia de programas con un desempeño similar al de los programas comerciales, esto es muy común en los campos del diseño, la animación, la grabación y edición de video, así como programas especializados en manejo de estadísticas y de matemáticas aplicadas. Un ejemplo banal, en un campo donde no parece que se hagan avances significativos es el del LibreOffice. Tanto la calidad de los formatos de texto (plantillas de estilo), como la inexistencia de un manejador de bases de datos Access, son dos ejemplos de las razones que nos empujan a seguir utilizando programas propietarios. Al existir referentes comerciales, las mejoras del software libre parecen asequibles. Eso ayudaría a impulsar la adopción de otras opciones tecnológicas y a mejorar nuestras posibilidades de protegernos contra las tecnologías de control social en boga.

SEGUNDA PARTE

PROFUNDIZANDO EN LAS HERRAMIENTAS

4

TOR: LA PRIVACIDAD EN INTERNET EN LA ERA DE LA GRAN VIGILANCIA

Roger Dingledine

Tor es una organización sin fines de lucro establecida en Estados Unidos. Está facultada para recibir donaciones libres de impuestos. Es también un programa que puede utilizarse para lograr mayor seguridad en internet; es una red de voluntarios alrededor del mundo que participan con nodos (*relays*) que envuelven y redirigen al tráfico de Tor. También se refiere a un grupo de gente alrededor del mundo —Tor es una comunidad de investigadores, desarrolladores y usuarios que le enseñan a los demás por qué la privacidad es necesaria. Es importante mencionar que, a donde sea que vaya, se encuentran grupos en universidades realizando algún tipo de investigación sobre Tor. Hay personas en esta universidad trabajando en cómo mejorar el rendimiento de Tor, o cómo aumentar su seguridad.

Tor es un programa que puede instalarse en cualquier computadora, típicamente lo que querrán instalar es el Navegador Tor (*Tor Browser*), y lo que persigue es que se pueda navegar la red sin ser vigilado; aprender qué hacen los sitios Web que visitamos, y sin que la gente del otro lado sepa desde qué parte del mundo provienen dichas visitas. Sin que haya posibilidad

para quien opere un punto en el camino de la comunicación de rastrear qué es lo que está haciendo el usuario en cuestión. Esa es la idea básica de lo que persigue Tor.

Tenemos muchos usuarios. Es un sistema que brinda anonimato, por lo cual es difícil saber a ciencia cierta cuántos usuarios tenemos, pero estimamos que alrededor de dos millones de personas usan Tor cada día. Recientemente se publicó un artículo que presentaba datos apuntando a que serían más bien entre ocho y diez millones. Así que podemos decir que es una comunidad mundial, muy grande y constantemente creciente, de gente interesada en la privacidad. Pensemos, pues, en el modelo de amenaza. ¿Qué es lo que intentamos proteger?, ¿qué es lo que nos preocupa?

Pensemos en una usuaria llamada *Alice*. Ella está intentando comunicarse con un sitio Web llamado *Bob*. ¿Dónde está el reto?, ¿de qué nos preocupamos? Tal vez el atacante esté vigilando la red local de *Alice*, tal vez sea alguien utilizando la red inalámbrica en el mismo edificio que ella, o tal vez sea alguien que trabaja para la compañía telefónica local. Esa es una opción. Por otro lado, el atacante puede estar del lado del atacante —Tal vez está viendo las acciones de *Alice*, tal vez ella está conectándose con Wikileaks, y quiere averiguar cómo lo está haciendo. Tal vez están en el sitio destino, puede ser cnn.com, y quiere saber cómo es la conexión de *Alice*, para comparar.

O tal vez el atacante esté en algún lugar en el medio, tal vez sea AT&T o Horizon, o las operadoras de comunicación troncal de México, intentando observar la comunicación completa y observar quién está hablando con quién. Así que hay diferentes lugares en los cuales puede estar el atacante, y contra los cuales debemos construir un sistema que mantenga a usuarias y usuarios tan seguros como sea posible, dado que pueden ser atacados en cualquier punto por el cual pase el tráfico.

Y otro punto importante a considerar: el anonimato no es lo mismo que el cifrado. Mucha gente responde inmediatamente diciendo, "no necesitamos de Tor porque usamos VPN (redes privadas virtuales), usamos cifrado, por lo que estamos seguros''. El problema es que alguien puede estar vigilando su tráfico mientras éste se está produciendo. El cifrado es bueno, debemos utilizar el cifrado, pero un atacante puede de todos modos obtener información acerca de con quién se está llevando a cabo la comunicación, cuándo ocurre dicha comunicación, qué tanto volumen de información se intercambia. Las agencias de inteligencia no están intentando romper el cifrado, nadie intenta hacerlo. En general, intentan construir grafos sociales, indicando con quién y cuándo se comunica cada sujeto, para entonces encontrar a alguna persona en el medio que sea más vulnerable que los actores principales, para atacar ahí al flujo de información. Así que el grafo de la red social es donde se encuentran las cosas interesantes de las agencias de inteligencia. No están intentando romper el cifrado, les importa más obtener metadatos. Esto nos brinda una imagen más bien tétrica del chico que trabaja para la NSA (Agencia de Seguridad Nacional) en Estados Unidos.

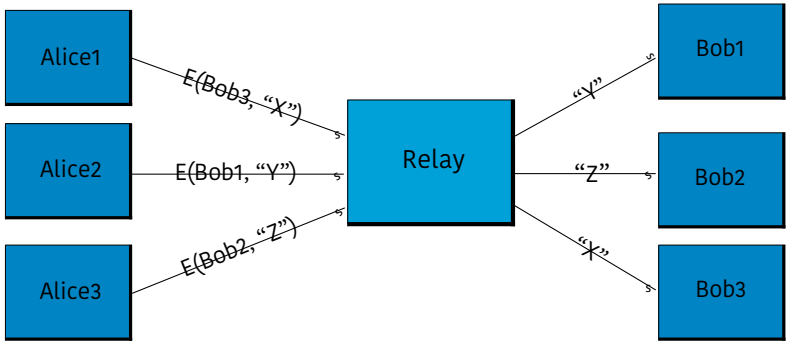
Entonces, consideren que el cifrado protege el contenido efectivo en el tráfico de red, y la seguridad de metadatos es proteger a la información acerca de con quién estamos hablando, hacia dónde va nuestro tráfico, y ese tipo de cosas. Esto es importante porque hemos aprendido de documentos tan importantes que Ed Snowden sacó a la luz acerca de cómo realizan su trabajo las agencias de inteligencia, no sólo en Estados Unidos, sino que en muchos otros países.

De hecho, sólo se emplea la palabra "anonimato'' cuando estamos hablando con otros profesores, investigadores o científicos relacionados con Tor. Cuando hablo con mis padres, les

digo que estoy trabajando en un sistema de privacidad, porque la privacidad es un valor importante. El anonimato da miedo, y si bien "no sé si el anonimato es bueno o malo'', la privacidad es buena. Entonces, mantengan eso en mente para comprender lo que hago.

Al hablar con compañías, es acerca de la seguridad en redes y comunicaciones, porque el anonimato asusta. Ya dijo Scott McNealy (ex-CEO de Sun Microsystems, posteriormente adquirido por Oracle) que la privacidad estaba muerta, así que muchas compañías lo aceptan y no la consideran como algo valioso. Pero a las compañías sí les importa la seguridad; tal vez quieren esconder a qué competidores están investigando en internet. Goldman Sachs, una de las principales compañías de inversionistas, utiliza Tor porque no quieren que sus competidores encuentren a qué compañías están investigando para invertir en ellas. Cuando se habla con gobiernos y representantes militares, es acerca de resistencia al análisis de tráfico en las redes de comunicaciones. Esta es una frase complicada, pero de nuevo, se refiere a las mismas propiedades de seguridad. Para cada grupo, y para cada tamaño de grupo, hay que frasear lo que hace Tor de una manera adecuada a sus necesidades y modelos de amenaza en red. Y hay una cuarta categoría: la gente que está bloqueada y sufre de censura, a quienes no se les permite conectarse a sitios donde está la información que requieren. Hay gente en el mundo que no puede abrir el sitio de la BBC, o no pueden entrar a Facebook, y queremos brindarles las herramientas para que puedan hacerlo. Así que, ¿cómo funciona esta cosa llamada Tor?, ¿cómo podemos construir un sistema que brinde anonimato, o privacidad, o seguridad? La respuesta simple es que hay un gran servicio central. Así es como funciona una VPN (red privada virtual), y así es como funciona *Anonymizer*. Si, como lo muestra la imagen 1, tenemos

Imagen 1
El diseño más sencillo para buscar el anonimato es utilizar un anonimizador centralizado



una computadora central, y todos sus usuarios piden una determinada página, esta computadora la solicita y envía a sus usuarios. Es muy simple. Cada usuario cifra sus comunicaciones de forma que únicamente la computadora central (que provee el servicio de anonimización) pueda descifrarlo, y ésta lleva a cabo las consultas requeridas.

Pero, ¿qué pasa si este servidor central resulta comprometido?, ¿qué pasa si ellos tienen algo por ganar de conocer el tráfico que anonimizan, o si un atacante malicioso obtiene acceso a sus sistemas y logra infiltrarse, obteniendo la capacidad de monitoreo?, ¿o qué pasa si les llega una orden gubernamental de reportar las acciones de alguno de sus usuarios, o a todo usuario que se conecte a determinado sitio?

Más aún: incluso si el comportamiento de este anonimizador es 100% ético, y toman la seguridad de sus operaciones tan en serio que resulta imposible penetrarlos, tienen puntos específicos de conexión a la red. Si el proveedor de telecomunicaciones del anonimizador monitorea los paquetes entrantes y

salientes, puede hacer una correlación de tráfico sobre el tiempo. Un atacante de tipo gobierno nacional, claramente, seguiría este camino sin alertar al anonimizador en cuestión.

Un usuario cuidadoso entonces podría elegir pasar su conexión por una serie de sistemas anonimizadores (a los que ahora llamaremos *relays*), de forma que ningún atacante pudiera razonablemente vigilarlos a todos. De esta manera, si *Alice* quiere comunicarse con *Bob*, solicita el establecimiento de *cuatro* conexiones: la primera, de ella al *relay R1*. Éste sabe quién se está conectando, pero dado que el contenido está cifrado, no puede conocer más que el destino de su conexión: el segundo *relay*, *R2*, recibe una conexión proveniente de *R1*, y su destinatario es otro *relay*, *R3*. De esta manera, *R2* no tiene ningún dato que le permita vincular a los dos extremos de la conexión. Por último, *R3* recibe la comunicación de *R2*, y se conecta por fin con *Bob*. Si asumimos que la conexión a red y la administración local de los tres *relays* es independiente, y que un mismo actor no puede comprometer o monitorear a los tres, no hay manera de rastrear la conexión entre *Alice* y *Bob*. Y eso es precisamente, como lo muestra la

Imagen 2
La conexión de *Alice* cruza por tres relays antes de llegar a *Bob*

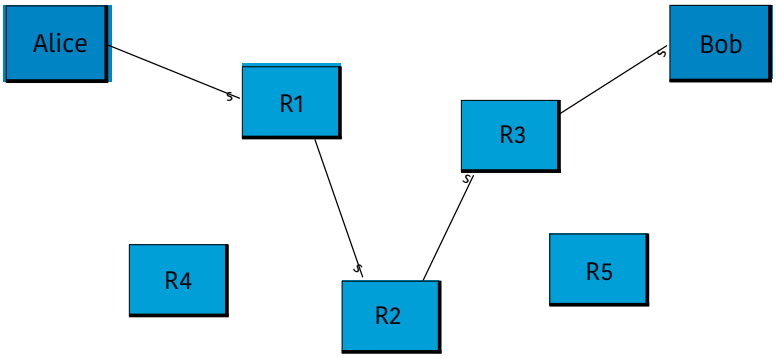


imagen 2, lo que hace Tor: todas las comunicaciones pasan por tres nodos, denominados *relays*, elegidos automáticamente de entre miles de *relays* disponibles al iniciar una conexión.

Además de esto, se ha trabajado mucho en un uso correcto del cifrado. Hablar acerca del cifrado excede el Tema de este trabajo, excepto por un punto interesante. La forma en que utilizamos la criptografía incluye asegurar la propiedad de *secreto perfecto hacia adelante* (*perfect forward secrecy*), lo cual significa que si un atacante vigila nuestro tráfico en internet, y demuestran que dicho tráfico cruzó por determinado *relay*, no es posible obligar al operador de dicho *relay* a descifrar el tráfico —no podrían hacerlo, porque ya no existe la información necesaria para que pueda ser descifrado. Esto significa que, para atacar el cifrado de Tor, el ataque debería realizarse en el momento preciso que la persona está enviando dicho tráfico. No puede atacarse una grabación del tráfico al día siguiente.

Lo presentado hasta este punto es únicamente la primera mitad de la respuesta a "¿qué es Tor?''. Esto es lo que llamamos anonimato a nivel de red, o privacidad a nivel de tráfico. Hay un segundo término importante, el de privacidad a nivel aplicación. La primera parte es que no es posible observar a qué sitios destino se dirige determinada conexión, y los sitios destino no pueden averiguar de dónde viene determinada conexión. La segunda parte está dentro del navegador Web. Muchas personas están familiarizadas con el concepto de *cookies*: resulta que cada vez que entramos a nuevamente un sitio Web, nuestro navegador complacientemente le informa al sitio cuántos píxeles de ancho y alto mide nuestra pantalla, qué idiomas comprendemos, cuántas extensiones tenemos instaladas, y literalmente cientos de cosas por el estilo. Estas cosas pueden identificarnos ante el sitio Web, aunque no necesariamente le dice al sitio cuál es

nuestro nombre o dónde estamos, pero le da suficiente posibilidad de reconocernos con el paso del tiempo. Si entro hoy al sitio, aprenderá suficientes cosas acerca de mí como para poder reconocerme como el mismo usuario cuando lo visite mañana.

El sólo hecho de poder obtener toda esta información es peligroso, y nuestro objetivo es ofrecer privacidad por omisión, con configuraciones seguras. Corresponderá a usuarias y usuarios decidir qué tanto *quieren* decirle al sitio que visitan. Tiene sentido entrar a Facebook desde Tor, e identificarse para entrar a su servicio. Nos identificamos ante los servicios que deseamos usar, pero alguien que esté monitoreando la conexión de red no sabe dónde nos estamos conectando o desde dónde lo hacemos. Alguien monitoreando a Facebook tampoco sabe dónde estamos, ni siquiera Facebook lo sabe. ¿Por qué tendría que saber Facebook que estoy en México ahora mismo? Incluso si entro para decir "¡Hola! Soy Roger", ¿por qué deberían los metadatos de mi tráfico decir desde dónde viene mi tráfico? No tienen por qué saberlo. Hay muchos pedazos de lo que puede significar el anonimato. No es únicamente para esconderme del destinatario de la comunicación.

La manera que más frecuentemente recomendamos para el uso de Tor es mediante el navegador derivado de Firefox con modificaciones en su comportamiento respecto a la privacidad que distribuimos, el Tor Browser. Sin embargo, hay otras maneras de usar Tor, presentamos un par de ejemplos.

TAILS

Tails es básicamente un CD vivo, o un sistema que puede arrancar de una unidad USB, que corre sobre Debian, una distribución de Linux, y viene preconfigurado tal como debería estarlo. Pre-

senta todas las aplicaciones que son habitualmente requeridas preconfiguradas, evitando aplicaciones como Microsoft Word, que en muchos sentidos van en contra de la privacidad. El objetivo con Tails es tener un sistema auto-contenido. Periodistas que trabajan con documentos clasificados, como los revelados por Ed Snowden, usan Tails para gozar de mayor seguridad al compartir dichos documentos.

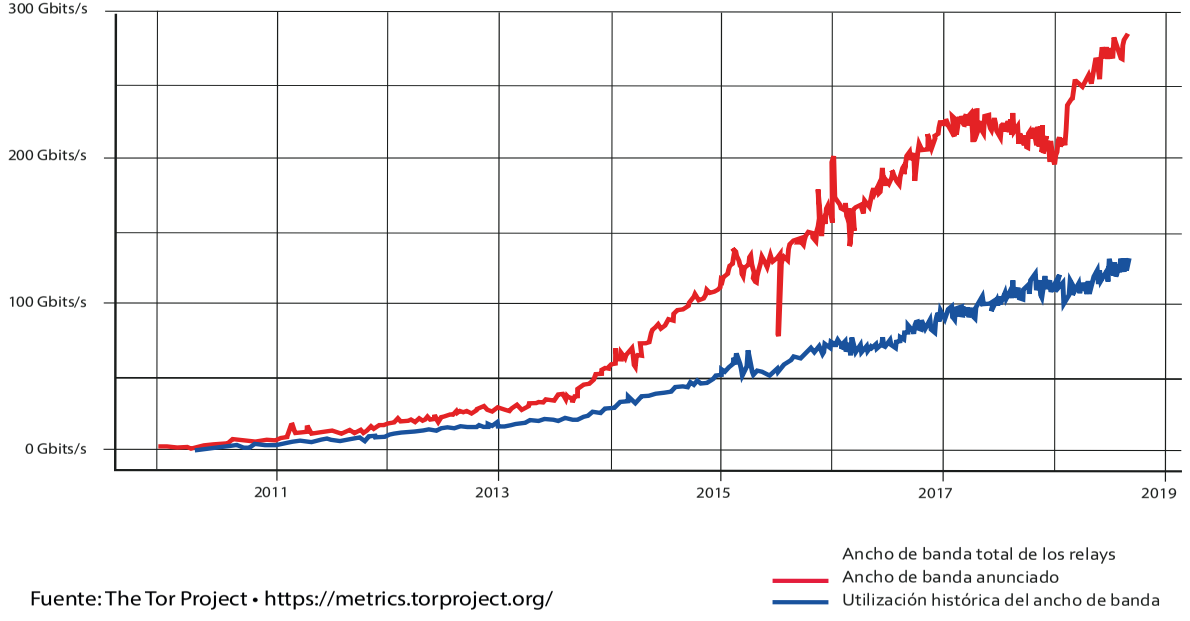
ORFOX

Recientemente liberamos una versión del navegador Tor para Android, además de la existente para Windows, Linux y Mac. Ahora Tor cubre también al ecosistema Android, lo cual es buenísimo. Es el mismo navegador de Tor. El problema que teníamos en Android era cómo funcionaba la parte de Tor: el anonimato a nivel red funcionaba, pero el navegador para brindar la privacidad a nivel aplicación, las *cookies* y demás, no eran del mismo navegador Tor. Ahora tenemos ya un mismo programa que puede correr en las diferentes plataformas, y todas ellas reciben el mismo nivel de seguridad. No podemos aún hacer una versión para iOS, porque Apple controla qué navegadores pueden correr en los iPhones, y el único navegador autorizado es el propio de Apple. Nos resulta imposible ofrecer una opción segura en esa plataforma.

RENDIMIENTO

Discutamos un poco acerca del rendimiento. En la imagen 3 se aprecia la gráfica del tráfico total transportado por la red Tor a lo largo de los últimos ocho años. La línea violeta es el tráfico efectivo de la red, y la línea verde es el tráfico que la red puede manejar. Pueden ver cómo las dos líneas se cruzan.

Imagen 3
Ancho de banda total de los relays de Tor, desde 2010 hasta 2019



Fuente: The Tor Project • https://metrics.torproject.org/

No es divertido usar Tor cuando todo es lento y es necesario esperar a que otra persona reciba su página antes de que carguemos la nuestra. Las líneas se han ido separando, por lo que Tor puede utilizarse mejor y más naturalmente, porque hay más capacidad en la red, y todo el tráfico puede pasar más ágilmente. Sí, siempre habrá necesidad de más *relays*, ese es un tema al que volveremos, por eso, invitamos a todos a hacer activismo en sus universidades; una universidad es un lugar ideal para correr *relays* que ayuden al crecimiento y sostenimiento de la red Tor.

LA SEGURIDAD DE TOR VIENE DE SU DIVERSIDAD

¿Y qué pensamos del nivel de seguridad que Tor provee? Hay dos maneras de responder a esta pregunta. Una es considerar dónde están físicamente localizados los *relays*. Si en los hechos tuviéramos una red Tor con todos los *relays* en el MIT, Harvard, Princeton, en un área geográfica pequeña, resultaría muy sencillo monitorear todas las conexiones de red que cruzaran por nuestra red; podría correlacionarse todo el tráfico que entra a Tor con el que sale, y sería posible montar un ataque desanonimizador. Por esto, entre más *relays* tengamos, y entre mejor estén distribuidos en lugares más distintos, resultará más difícil para un atacante obtener el tráfico entrante y saliente de todos estos lugares para vigilar las conexiones de internet y atacar a Tor. Esto es, entre más *relays* haya en lugares más interesantes, mejor podremos asegurar el anonimato.

Otra manera de medir la seguridad es, ¿qué es lo que hacen los usuarios?, ¿por qué emplean Tor? Tenemos un muy buen ejemplo. Digamos que hay alrededor de 50 000 personas que utilizan Tor a diario para activar en pro de todas las disidencias políticas. Imaginen que todos los usuarios de Tor lo hacen porque quieren

forzar un cambio en su gobierno. Esto los hace a todos sujetos de interés desde la perspectiva del gobierno en cuestión. En ese caso, el mero hecho de correr Tor es interesante y peligroso. Afortunadamente, la mayor parte de la gente usa Tor para evadir el bloqueo a Facebook, para evadir el bloqueo de comentarios Web, para poder ver fotos de gatitos y perritos, arcoíris, o cualquier cosa que hace la gente normal en internet. La gente común instala Tor para hacer cosas comunes y corrientes. Dichas cosas comunes y corrientes son críticas para la seguridad que requieren esas 50 000 personas. El que la gente común use Facebook desde Tor ayuda a que los demás usuarios de Tor resulten menos peligrosos o interesantes para quien pudiera representar una amenaza para ellos.

LA TRANSPARENCIA ES VITAL PARA TOR

Otro factor fundamental de Tor es la transparencia. Tor es un proyecto de software libre/*open source*. Te damos el código fuente, pero va mucho más allá que eso. También están disponibles públicamente los documentos de diseño, que detallan lo que intentamos construir. Están las especificaciones, los estándares de diseño de internet aplicables a lo que hacemos. Así que te decimos qué es lo que queríamos, te decimos cómo lo estamos haciendo, y te damos el código fuente. Si eres bueno leyendo código y lo comparas con la especificación, y dices que yo introduje un fallo, o si eres un investigador y analizas los documentos y especificaciones de diseño, y decides construirlo, pero no obtienes lo que esperas, tienes argumentos sólidos para respaldarlo.

Parte de nuestros objetivos es que Tor sea software libre. Es un buen inicio, pero tenemos que proporcionar todo para que nos ayuden a asegurar que lo hicimos bien. Viajamos a diferentes lugares para dar pláticas sobre Tor, conocemos a mucha gente,

y lo hacemos público. Mi nombre es Roger, y los desarrolladores presentes también les dirán sus nombres, eso es parte de la transparencia que busca nuestro proyecto —y eso es fundamental para lograr la confianza.

Hablando con la gente vemos que se ríen de la aparente contradicción de que éste es un proyecto que tiene como foco principal la privacidad, y que lo que nos importa es la transparencia. No es una contradicción; la privacidad es una elección, la privacidad requiere de control. Elegimos identificarnos públicamente para que el proyecto sea más seguro y fuerte, y esa es una elección importante para nosotros. Así pueden conocernos abiertamente, hablar con nosotros, y decidir individualmente si Tor los hace sentir seguros.

¿Y QUÉ HAY ACERCA DE LA *GENTE MALA*?

Siempre hay alguien que nos pregunta, "¿y qué hay de los criminales? Ustedes los están ayudando". Hay muchas respuestas para esto, daremos algunas, y posteriormente podemos platicar más a fondo. Una de ellas es que Tor tiene millones de usuarios a diario, y sí, hay algunas personas malas, igual que en internet, pero mucha gente se pregunta acerca de las personas malas en Tor. Parecerían creer que Tor tiene 10 usuarios, y que todos ellos están haciendo cosas ilegales. Entonces, ¿cuál sería el punto?

La respuesta es que, probablemente, hay millones de personas que ellos no están considerando porque son personas normales que están usando Facebook y Google sobre Tor, haciendo lo que sea que la gente normal hace en internet, y nunca vemos a esta gente normal. Esa es una manera de responder a esta pregunta.

Otra respuesta es que la seguridad es para el beneficio de toda la gente. Sí, también beneficia a la *gente mala*, pero hay

que verlo en balance. Tiene algunos aspectos buenos y malos —es una herramienta, y como tal, tiene distintos usos posibles. Pero yendo incluso más allá, esta caracterización no describe fielmente la situación de Tor. La gente de bien tiene muy pocas opciones para mantener su privacidad en línea; la *gente mala* tiene muchas más opciones a su disposición. Si intento ser malo en línea, hay más maneras en que puedo lograrlo. Puedo vulnerar computadoras ajenas y utilizarlas para mi *bot net*. La gente de bien no puede considerar esa opción.

Imaginen la siguiente situación hipotética. Opción uno: quiero construir una herramienta que sirva para un millón de personas y brinde servicio por todo el año, y te cuento todo lo necesario para que me ayudes a construirla. Ese es el planteamiento de Tor. Veamos otro escenario: quiero construir una herramienta para 20 personas, para utilizarla la semana entrante, y mantendré mi diseño en secreto. Ese es el planteamiento de la *gente mala*. Hay muchas maneras de resolver el segundo escenario: puedo ocultar información codificada, una guerra de ediciones en Wikipedia o en imágenes en *EBay*. Si no tengo que demostrar públicamente que mi sistema soporta escrutinio, y no requiero que escale más allá de un par de personas, y no es necesario que sobreviva el paso del tiempo, hay muchas maneras de implementarlo. Tor ha desarrollado un sistema que escala, es transparente, y ha durado décadas. Ese es un problema para la gente de bien, y es lo que la gente de bien necesita.

EL SITIO WEB DE TOR

En la imagen 4 pueden ver distintas capturas del sitio Web oficial de Tor como lo ven los ciudadanos de distintos países del mundo. Podemos ver, “este sitio está bloqueado por contenido

contrario a las leyes del Estado". "¡Navegue seguro! Este sitio Web no puede ser accedido". Esto es lo que ven los usuarios que intentan abrir *torproject.org* desde Dubái o Arabia Saudita, y en varios otros países. "El acceso a este sitio está permanentemente bloqueado", "el sitio al que intenta acceder ha sido bloqueado".

Imagen 4
Varias capturas del sitio Web de Tor, como se presenta en países que ejercen la censura

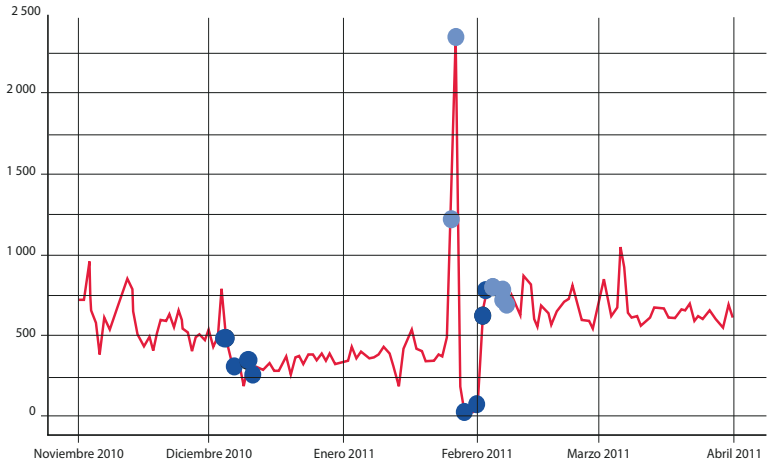
En algunos casos, incluso el censor nos dice el nombre y dirección del usuario. ¿Por qué será que están censurando esto? Pero más aún, ¡intentan hacerlo parecer divertido! Dice, "¡Ups! Estamos censurando la red. Es divertido, es un error, no somos dictadores".

Esta es la primera imagen de Tor con que se encuentran millones de usuarios en todo el mundo. Ven estas imágenes en vez de nuestro sitio Web.

MÉTRICAS DE TOR

Hace varios años comenzamos a preguntarnos quién usa Tor y cómo responde la red. Podemos ver en la imagen 5 la cantidad de gente conectándose a Tor desde Egipto cuando ocurrió la revuelta de la Primavera Árabe en Egipto, en la plaza Tahrir. Pueden observar claramente cuándo fue bloqueado Facebook, por el pico en la gráfica de los usuarios de Tor. También se ve cuándo desco-

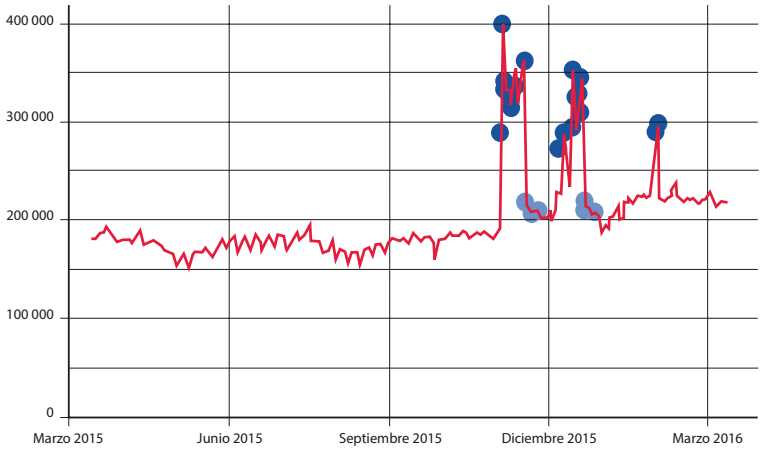
Imagen 5
Usuarios conectándose directamente a Tor desde Egipto, 2010-2011



nectaron por completo el servicio de internet, pues todo desapareció por varios días. La parte favorita de esta gráfica es el efecto acumulado: muchos más usuarios nuevos siguieron utilizando Tor una vez que la red volvió a la normalidad. Posiblemente pensaron, "los militares están a cargo, la infraestructura de vigilancia es un problema, ahora sabemos que están monitoreándolo todo, así que continuaré protegiendo mi tráfico".

La imagen 6 es más reciente, corresponde a Rusia en 2015. Vemos a 200 000 usuarios, aunque obtener esta proyección es difícil, y si los números que estamos evaluando son correctos, probablemente sean en realidad cinco veces esta cantidad. Puede ser alrededor de un millón de usuarios. Vemos un pico repentino, que cae, y posteriormente se repite junto con su caída. Nos preguntábamos qué podría haber causado este patrón. La gente de Facebook, y ellos dijeron que tienen exactamente la gráfica opuesta a ésta en sus sistemas. En Facebook, tienen un gran

Imagen 6
Usuarios conectándose directamente a Tor desde Rusia, 2015-2016



flujo de tráfico desde Rusia. De tiempo en tiempo, Facebook es bloqueado en Rusia, y todo este tráfico desaparece. Y cuando funciona de nuevo, vuelve bastante rápido a sus niveles habituales. Así que tenemos a una gran cantidad de gente que comienza a usar Tor cuando esta censura se activa.

CENSURA

¿Cómo funciona la censura? Hablamos ya acerca de *relays* públicos, cruzamos tres *relays* para anonimizar nuestro tráfico. Los primeros pasos de la censura son bloquear nuestro sitio Web para que resulte difícil bajar Tor, pero si lo recibes de un amigo o de cualquier otro lugar, el siguiente paso para censurar la conexión al servicio de Tor es bloquear a los *relays* públicos. Hay una gran lista, son unos 7 000. Cualquiera puede obtener esta lista, incluyendo los censores, y pueden bloquear las conexiones a los *relays* por dirección IP. Esto dificulta las cosas a quien quiere conectarse a Tor, todo está bloqueado.

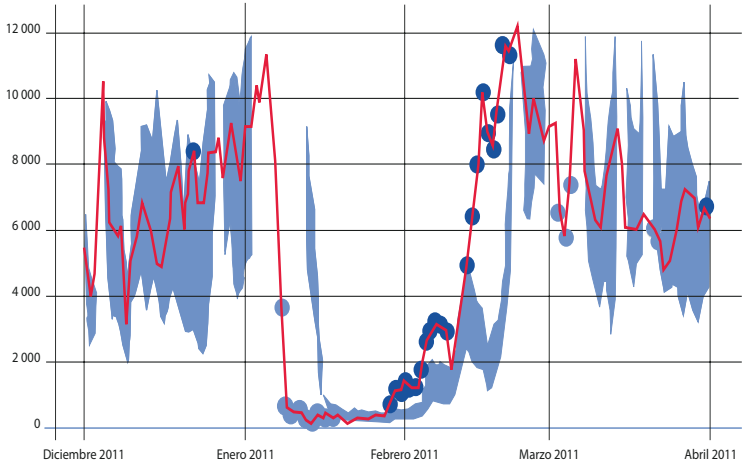
La defensa contra esto es lo que conocemos como *relays puente* (*bridge relays*). La idea es que pedimos a voluntarios que abran *puentes*; éstos son sencillamente *relays*, pero no están listados en ninguna lista pública, por lo cual un censor no puede saber dónde están, y no puede bloquearlos.

En este caso, mudamos el problema: ya no es *cómo publicar siete mil direcciones IP sin que China levante una alarma,* efectivamente un problema muy difícil, sino que *cómo coordinar las direcciones de miles de voluntarios y dárselas una a la vez a las personas que las necesitan, sin que China levante alarmas sobre todas ellas*. Eso es lo que buscamos con los *relays* puente.

Eso funcionó por varios años, hasta que apareció el siguiente obstáculo en el mapa. Irán compró una computadora especia-

lizada de Nokia, que realiza *Inspección Profunda de Paquetes (Deep Packet Inspection, DPI)*. DPI analiza las conexiones y, para cada una de ellas, va determinando, *esto es Bittorent, esto es http, esto es Tor*... Y pueden simplemente cortar el tráfico de Tor, a pesar de que se dirija a una dirección IP que no reconozcan. Irán hizo esto a principios de 2011, como lo muestra la imagen 7. Para hacer esta discriminación se fijan en puntos específicos del protocolo de cifrado que intercambiamos, y les permitió cortar el tráfico hacia Tor. Afortunadamente, hemos podido ir mitigando este reconocimiento, y cabe decir, vencer a la aplicación de DPI contra Tor ha resultado en realidad muy divertido.

Imagen 7
Usuarios conectados directamente a Tor desde Irán, 2010-2011



TRANSPORTES CONECTABLES

La respuesta que ha encontrado Tor a esta situación es lo que llamamos *transportes conectables* (*pluggable transports*). La

idea es que, para que la red Tor se ocupe de cuidar la privacidad, anonimato y algunas otras cosas de población que de otro modo estaría sujeta a la censura, ellos conectan un transformador de tráfico (*traffic transformer*) para convertir al tráfico en algo que el censor no pueda bloquear. Puede convertir el tráfico en Skype, en *http*, o en otra cosa. Hay muchos proyectos de investigación disponibles construyendo distintos transportes conectables para disfrazar al tráfico de algo que los censores no quieran bloquear.

BLUE COAT

Hay una historia que todos deberían saber, ocurrida hace tres a cinco años. Un grupo de gente afiliada con el colectivo hacker *Anonymous* revisaron computadoras en Siria, y encontraron un servidor *http* mal configurado que estaba entregando varios gigabytes de bitácoras de conexión para una computadora llamada *Blue Coat* (abrigo azul). *Blue Coat* es un sistema de vigilancia y censura, producido por una compañía basada en Sunny Valley, California. Hace DPI y vigilancia, fundamentalmente, para censurar internet. Lo que encontraron en la bitácora fueron miles de líneas diciendo, "la dirección IP *X.X.X.X* solicitó el sitio Web *yyyyyy.yyy*, y la bloqueé".

Este servidor ofrecía un registro completo del tráfico Web visitado desde Siria. Estados Unidos tienen una ley que prohíbe prestar servicios de vigilancia y censura a varios países, y Siria es uno de ellos. La gente de *Anonymous* se dirigió entonces a *Blue Coat* para preguntar, "¿qué están haciendo? Están rompiendo la ley, están manteniendo infraestructura de vigilancia en Siria". *Blue Coat* lo negó, y cuando les dieron más detalles técnicos que hacían indudable que el equipo provenía efectivamente de *Blue Coat*, respondieron que ese equipo había sido vendido a

Dubái. "¿Cómo íbamos a saber que lo echarían a andar en Siria? Somos respetuosos de la ley, no podemos saber cómo usan sus computadoras".

Anonymous demostró entonces que los equipos estaban recibiendo actualizaciones diarias. *Blue Coat* replicó, "estamos desactivando y limitando esa funcionalidad", pero *Anonymous* ha demostrado que los números seriales de actualización siguen siendo válidos. Está demostrado que *Blue Coat* miente. Y el final de esta triste historia es que *Blue Coat* puede incluso obtener el Premio de Derechos Humanos del Departamento de Estado de Estados Unidos por su colaboración en investigar este tema. Son una compañía terrible, y parte importante del problema es que hay muchas compañías más dispuestas a construir un ecosistema para la vigilancia. Cisco construyó el sistema de vigilancia de China y en Birmania, y pasado cierto tiempo, la compañía Fortinet los desplazó de ese mercado. Hay una fotografía terrible en internet con el vendedor de Fortinet alegremente estrechando la mano del líder militar de Birmania.

Hubo un congreso hace algunos años en Túnez, poco después del cambio de gobierno, y el responsable de la agencia gubernamental de internet dijo en su discurso, "sí, hacemos filtrado de contenido. Le pagamos a una compañía estadounidense un millón de dólares cada año para utilizar sus filtros". Piensen en cuánta comida podrían comprar con ese dinero; ¡tal vez no deberían censurar su red! Y las cosas van todavía más allá: el filtro no es operado por Túnez, una empresa francesa (no mencionó cuál) es subcontratada para llevar a cabo esta tarea, con lo que hay un segundo gobierno nacional que puede filtrar todo lo que pasa en la red de Túnez, intervenir las páginas Web que reciben los usuarios. Esto incluye realizar censura y vigilancia en las operaciones del ejército tunecino por parte de una compañía francesa.

Ya no únicamente se trata de cuestiones de libertades civiles o derechos humanos, es ya un tema de soberanía nacional. Ellos no tienen el control de su país si dejan que una compañía extranjera que es en realidad su internet.

Hace algunos años participamos en una reunión en el Ministerio Exterior alemán donde se intentaba decidir si Europa debería intentar evitar que las compañías europeas construyeran estos dispositivos y los vendieran a países con regímenes represores. Hay una compañía italiana llamada *Hacking Team* a la que acuden distintos gobiernos del mundo para comprar ataques. *Hacking Team* se especializa en encontrar la manera de instalar *puertas traseras* donde sean necesarias para poder realizar espionaje. El Ministerio Exterior alemán estaba buscando cómo evitar que esto ocurriera, cómo crear leyes para dificultar a las compañías europeas tener este tipo de prácticas. En la reunión, era el único ingeniero; todos los demás participantes eran abogados, diplomáticos, gente dedicada a la creación de las políticas. Para todas las preguntas técnicas que había, preguntaban, "Roger, ¿y qué piensa la comunidad técnica respecto a esto?", era el único representante de todos los ingenieros del mundo ante el gobierno alemán.

Es necesario aquí presentar al término *intercepción legal* (*lawful intercept*). Las leyes de Estados Unidos y de Europa requieren que todos los ruteadores de internet tengan una puerta trasera: un puerto adicional en el que se puede conectar un cable, al cual se manda una copia de todo el tráfico que cruza por el ruteador. Ellos lo llaman *intercepción legal* , se le llama *puerta trasera*; insisten en que es una característica documentada públicamente, por lo que no es secreta. Tal vez sea más correcto el término *puerta frontal* —el problema es que hay una manera sencilla de espiar todo lo que pasa por los equipos. Tal vez en

Estados Unidos o en México haya un sistema y un proceso judicial, que requiera acudir a la Corte antes de llegar a la decisión de si es legal espiar lo que pasa por un ruteador en internet. Pero si estamos en Arabia Saudita y alguien pregunta, "¿y para qué es ese puerto?", la respuesta es "¡Ah! Es el puerto para la intercepción legal", podemos esperar que nos digan "Yo soy la ley, ¡conéctalo!''

Tal vez en algunos países haya contrapesos y balances, pero los dispositivos que diseñamos se venden a países donde esta protección legal no existe. Y tampoco es que funcionen excepcionalmente bien en nuestros países, pero esa es otra discusión. Los funcionarios explicaban: "ustedes nos forzaron a implementar puertas traseras en los ruteadores, y ahora se quejan cuando las usamos para monitorear el tráfico de la gente. Es culpa de ustedes que la comunicación sea tan fácil de espiar. Las reglas que siguieron para el diseño hacen que sea fácil espiar, y ahora se oponen si utilizamos las puertas traseras con que ustedes lo construyeron".

Pienso que es crítico. Tenemos que pensar acerca de cuando Estados Unidos y Europa toman decisiones que afectan al resto del mundo. Si estas decisiones no son necesariamente buenas para nosotros, con toda claridad no son buenas para el resto del mundo.

Australia censura internet. Inglaterra censura internet. Dinamarca censura internet. Suecia censura internet. Eso significa que cuando se discuten derechos y políticas y se critica a China por la censura que realizan, el contraargumento es simple: "mantenemos a nuestros ciudadanos seguros, al igual que lo hacen ustedes. Todos censuran, nosotros censuramos, no hay problema. ¿Qué tiene de particular lo que hacemos?" El hecho de que cada vez más países occidentales lo hagan hace cada vez más difícil

describirlo como algo dañino. Se está normalizando la censura de internet, y entre más países lo hagan, más difícil será oponerse a ello.

Otro ejemplo interesante es Wikipedia, podemos leerla utilizando Tor, pero no editarla. Wikipedia tiene un problema con el vandalismo, gente que quiere editarla por diversión, o que quieren empeorar su contenido y funcionamiento por las razones que sean. Comenzaron bloqueando las direcciones IP de toda esta gente, y los vándalos respondieron utilizando *proxies* (computadoras intermedias; la palabra en inglés significa *representantes*). Wikipedia entonces bloqueó la edición anónima desde las direcciones de los *proxies* mejor conocidos. Entonces, los vándalos comenzaron a penetrar computadoras vulnerables de usuarios comunes en todo el mundo. Wikipedia tiene una lista negra de millones de direcciones IP que no tienen permitido editarla. Dicen que Wikipedia es construido por todo mundo, que quien quiera puede editarla, pero tienen una lista cada vez más grande de gente que no puede hacerlo. Hace 10 años era mucho más fácil contribuir con Wikipedia, pero estas restricciones han ido limitando la cantidad de gente que contribuye su tiempo a mejorar Wikipedia. Hay grupos interesantes de estudio en ciencias sociales que buscan medir qué tanto se está perdiendo Wikipedia. ¿Cómo se puede medir la pérdida para Wikipedia que significan todos estos usuarios que no están contribuyendo? Hay mucha gente que participaría editando páginas, pero si se les impide, no contribuyen para seguir mejorando el contenido. Piensen en páginas relacionadas con el aborto, o con el Partido Republicano de Estados Unidos, o sobre algún tema socialmente sensible que la gente no quiere que se vincule con su identidad. ¿Cómo puede medirse lo que falta?, ¿cuánto daño está haciendo a Wikipedia el hecho de que se bloquee o evite que la gente lo haga?

EDWARD SNOWDEN

Una de las imágenes que más circuló cuando se publicaron las filtraciones provistas por Edward Snowden fue la de él usando su computadora, en la que tenía un *sticker* de Tor. Para muchos reporteros, éste fue su primer contacto con Tor. Muchos contactaron al proyecto, preguntando, "Edward Snowden escribió una cosa llamada Tor, y nos interesa saber más al respecto". Una y otra vez tuvimos que replicar, "no, somos una organización sin fines de lucro, y existimos desde hace mucho más tiempo que estas filtraciones, pero con gusto te explicamos respecto a Tor". Lo que sí resulta importante es que Snowden se esforzó en localizar tantos documentos como le fuera posible acerca de Tor, para que como desarrolladores supiéramos todo lo que se circula respecto a nosotros dentro de la NSA y GHCQ y otros grupos de inteligencia —particularmente respecto a cómo atacan a Tor.

Entre los documentos que recibimos hay una presentación de junio de 2012 describiendo cómo se intentan atacar sistemas como el de Tor; hay una cita graciosa, en que —a falta de mejores calificativos— presentan varias láminas con el título "/Tor stinks/" (Tor apesta). Indican que intentaron atacar a Tor de diversas maneras, y no lograron obtener ninguna información de valor. Presentan una cita que nos gusta replicar: "Tor sigue siendo el rey del anonimato altamente seguro y de baja latencia en internet". Y no hay ningún proyecto que se acerque.

SERVICIOS CEBOLLA

Hasta este momento, hemos hablado del primer caso de uso de Tor: quiero entrar a un sitio Web, y quiero estar seguro mientras lo hago. Hay otra manera de usar Tor, que denominamos los *ser-*

vicios cebolla (*onion services*) o servicios ocultos. Si se quiere correr un sitio Web, o algún otro servicio, de manera que nadie sepa desde dónde se está operando, pero que sí puedan llegar a él desde la red Tor. La manera de resolver esto es tomar la idea básica de los tres circuitos de *relays*, y conceptualmente "pegar" dos de estos circuitos, para ambos lados utilicen Tor para mantenerse anónimos (incluso mutuamente), y se encuentren en la mitad del camino. Eso significa que el usuario no sabrá cuál es el destino de su conexión, el destino no sabe de dónde viene el usuario, pero pueden hablar entre sí.

La forma en que esto funciona en la práctica para los sitios Web es con *direcciones onion*. En vez del URL con que normalmente ubicamos un recurso, se utiliza una cadena de letras aleatorias, utilizando como dominio principal ".onion". Esta cadena aleatoria es el *hash* de la llave pública del servicio cebolla, así que esto brinda además propiedades de seguridad muy interesantes. Una de ellas es que los servicios son *auto-autenticantes*. Si conocemos la *direccion onion*, nuestro navegador automáticamente hará lo necesario para asegurar que estamos hablando con el destinatario correcto. Se asegura que estamos hablando con un sistema que conoce la llave privada correspondiente al nombre que escribimos. En la red abierta es frecuente que veamos direcciones como https://facebook.com/, y podemos verificar que realmente nos otorga un certificado SSL que asegura que el sitio destino es efectivamente Facebook, pero esta verificación depende de una *autoridad certificadora*. Nuestro navegador tiene una lista de unas 300 compañías a quienes confía ciegamente cuando cualquiera de ellas dice, "este es efectivamente facebook.com".

Entonces, lo que ocurre es que la empresa de telecomunicaciones turca tiene una autoridad certificadora. La empresa de tele-

comunicaciones China tiene una. Había otra compañía holandesa llamada *Diginotar*, y operaban una autoridad certificadora, hasta que un atacante se adueñó de sus sistemas y comenzó a crear certificados SSL falsos —en Facebook, de Google, del proyecto Tor. El gran problema aquí es que, si hay 300 compañías de este tipo, y puedo meterme en cualquiera de ellas, puedo pretender ser cualquier sitio Web en internet.

Los servicios cebolla son inmunes a este problema porque no dependen de un tercero que emita el certificado. Ya no es decir, "confío en esta compañía", no "prometieron que verificarían", el puro nombre es suficiente para validar que estamos en el destino correcto, sin necesidad de involucrar a terceros. Además, dado que toda la comunicación tiene lugar dentro de la red de Tor, obtenemos un cifrado de extremo a extremo. Y ni siquiera hace falta que el operador del servicio lo deje *alcanzable* desde internet; podemos operar un sitio Web, y la gente lo puede encontrar incluso si no tenemos direcciones IPv4 públicas. Incluso si nuestra conexión no nos permite recibir conexiones normales, podemos ofrecer servicios, operar un *blog*, cosas por el estilo.

Otro uso interesante para los servicios cebolla es que mucha gente opera sus servidores ssh en su servidor de casa o del trabajo únicamente accesibles desde una dirección onion. Entonces, configuran su firewall para que bloquee todas las conexiones entrantes, por lo que no hay ninguna manera de conectarse fuera de hacerlo por este canal sobre Tor, que provee automáticamente seguridad extremo a extremo, autenticación, cifrado, y esto limita el área de la superficie de ataque tanto que resulta casi imposible atacar su computadora: bloquean todo lo que entra excepto las conexiones Tor, en las cuales confían.

¿Y qué tanto del tráfico de Tor viaja de esta manera? Hemos revisado el uso de tráfico en la red Tor; partiendo de que el tráfi-

co total en Tor es de aproximadamente 125Gbps, y el tráfico hacia direcciones cebolla es de apenas 1Gbps. Sumando a esto lo que no podemos ver, las conexiones internas y saltos entre *relays*, encontramos que la proporción de servicios cebolla es de alrededor de 3%. Del tráfico 97% son personas que entran a servicios normales, en internet abierta, sitios como Facebook, Amazon o Gmail. Los servicios cebolla conforman una pequeña parte del tráfico global. Así que si escuchan, como lo hemos leído varias veces, que las agencias de la ley detuvieron a algún servicio Tor y causaron una gran afectación, es seguramente falso. Hay un uso de red apenas de 3% dedicado a servicios cebolla.

Y esto es completamente diferente de la imagen del iceberg con que siempre nos confrontan preguntando acerca de la *Dark Web,* de la *Red Oscura*. Hace algún tiempo, la revista *Time*

Imagen 8
La engañosa y sensacionalista imagen del iceberg popularizada por la revista *Time*

publicó una imagen que se ha repetido hasta el cansancio, y que presentamos aquí como nuestra imagen 8: mencionaban que, en contraste con el contenido de la internet "normal", había unas 99 *internets ocultas,* a las que sólo se puede llegar mediante el navegador Tor. Esto implica que la red abierta conocida por todo mundo es únicamente la superficie, y es posible ir entrando a capas más y más profundas —y es una tontería. Es sólo basura sensacionalista con la que intentan vender anuncios, intentan vender revistas. En realidad, al día de hoy hay unos 7 000 sitios Web disponibles con *direcciones onion*, lo cual no es nada comparado con los miles de millones que forman a internet. Los servicios cebolla son meramente un juguete de hace unos 14 años, que tienen potencial interesante, pero a fin de cuentas casi nadie los usa hoy en día. Hace algún tiempo, la BBC presentó un artículo titulado, "puedes comprar drogas en internet, y aquí te decimos cómo", recibieron una gran cantidad de comentarios diciendo, "¡gracias! Ahora ya no tengo que ir a arriesgarme a la esquina de esa calle oscura. ¡Gracias por proveer información acerca de cómo comprar drogas de forma segura!". Una semana más tarde, publicaron un segundo artículo, reportando que en un afán investigativo, compraron dichas drogas, ¡y estaban buenísimas!... ¿Cuál es la motivación de la BBC?, ¿están intentando darnos noticias cuando no hay nada que reportar?, ¿están buscando que hagamos "click" en sus anuncios?, ¿están intentando mantenerse relevantes al compararse con CNN o Fox, o algo así? Parecería que todos los días hay algún medio que presenta a la famosa imagen del iceberg para asustar y confundir a sus lectores. La "red oscura" es minúscula, y no hay nada del otro mundo en ella.

Dicho eso, ¿cuál será el sitio Web más importante hoy en día en la red oscura? Es Facebook. En 2016 presentaron un artículo de blog donde decían, "hemos dado seguimiento a cuánta gente

se conecta a nuestro sitio Web utilizando Tor, y en el periodo de 30 días comparado con el promedio de hace dos años, un millón de personas más se conecta a Facebook utilizando Tor". No puedo contar hasta un millón, ¡eso es mucha gente! Nos parece sorprendente, es una fracción enorme. Si Facebook tiene mil millones de cuentas, una milésima parte de sus usuarios está conectándose sobre el servicio cebolla. 0.1% puede parecer poco, pero a nosotros nos parece un gran éxito. Y Facebook tiene la misma opinión. Dicen, "nuestros usuarios están demostrando que quieren privacidad, y nosotros vamos a configurar nuestros servicios para que estén tan seguros como lo requieran". Y esto tiene sentido porque Facebook tiene usuarios en Turquía, y si abrimos Facebook desde allá, el gobierno turco intercepta y censura la conexión, dándonos un Facebook falso. Lo han hecho de manera que resulte muy difícil darse cuenta de que no es el sitio legítimo. Los usuarios quieren saber que están, en efecto, comunicándose directo con el servicio de Facebook. Y esto no es la red oscura —pueden considerar que es como https, pero con mayor seguridad en los metadatos.

Uno de los retos que veo son las compañías denominadas de *inteligencia de amenazas*. Uno de los servicios que ofrecen es buscar qué información acerca de alguna persona o tema aparece en la red oscura. Uno de ellos comentó hace algún tiempo, "encontré una copia de Facebook en la red oscura". La respuesta fue, "no, lo que encontraste es un sitio Web llamado Facebook". Puedes abrirlo usando http o https, pero también puedes abrirlo usando su *dirección onion*, es el mismo sitio Web. No es una cosa separada llamada red oscura, es un conjunto distinto de propiedades de seguridad que nos brindan una manera de comunicarnos sobre internet. Es como https, pero mejor.

Hay otro caso de uso interesante para los servicios cebolla: lo llamamos *SecureDrop*, es una plataforma para realizar

denuncias anónimas, facilitando el contacto entre periodistas y personas que tienen documentos, notas o información acerca de corrupción o de acciones ilegales. Tenemos conocimiento de unas 50 diferentes organizaciones, como el *The New York Times* o el *Washington Post*. Hay muchas organizaciones que buscan permitir el contacto con sus periodistas de la manera más segura posible, porque la alternativa es simplemente enviar un correo electrónico, y "prometemos no decirle a nadie quién es nuestra fuente". Eso es malo, porque ellos *sí* saben quién es la fuente, y eso podría poner a los denunciantes en gran peligro. También es peligroso, porque quien sea que observe la conexión del *The New York Times* puede encontrar el correo en cuestión y los datos de su remitente. Sobre un *SecureDrop* podemos interactuar bidireccionalmente, pueden enviar preguntas y pedir aclaraciones, pero el denunciante se mantiene en control de su privacidad.

Y para ilustrar los servicios cebolla de una manera distinta, hablemos de *Ricochet*. Hasta ahora, mencionamos sitios Web configurados de forma que no divulgan su ubicación. *Ricochet* es una herramienta de mensajería instantánea que opera sobre un servicio cebolla. Si para nuestra mensajería utilizamos XMPP, Jabber, iMessage o Signal, todos esos diseños tienen una misma arquitectura: hay una computadora central que sabe dónde estamos tú y yo, sabe que hablamos, sabe cuándo hablo con cuál de mis amigos, y conoce mi lista completa de amigos. Eso significa que si intento atacar la privacidad de alguno de sus usuarios, puedo atacar al servidor central y obtener toda esta información. Estos servicios anuncian desde hace tiempo que implementan cifrado de extremo a extremo; si es así, y si está bien implementado, el atacante no sabrá lo que se dice en cada una de las conversaciones, pero se divulgan los metadatos. *Ricochet* está construido para evitar este tipo de ataque.

Un ejemplo más es *OnionShare*. Si fuéramos periodistas en posesión de los documentos de Snowden, y quisiéramos hacérselos llegar al periodista que se sienta en el escritorio de junto, ¿qué haríamos?: ¿enviarlos por correo?, ¿compartirlos por *Dropbox*? *Dropbox* está bien, pero comparten públicamente todos los archivos que reciben. ¿Configurar un servicio FTP en nuestra computadora? Estaría bien, si todos los periodistas supieran hacerlo. La realidad es que no hay muchas maneras seguras de compartir archivos grandes. *OnionShare* es un programa muy fácil de usar, con clientes para Windows, Mac y Linux. Lo lanzamos indicándole el documento que queremos compartir, y lanza un servidor Web configurado sobre una *dirección onion*. Le damos a nuestro compañero la dirección generada, y una vez que descargan el archivo desde su navegador Tor, el servidor Web se desactiva y desaparece. Nuestra *dirección onion* desaparece, y no queda ningún rastro. Dado que no hay ningún servidor central, es una buena manera de compartir archivos en internet. No hay ningún lugar que atacar, no hay dónde buscar cuando alguien busca correlacionar qué periodista habla con otro.

PROBLEMAS A ENFRENTAR CON TOR

Tor no es perfecto. Hay varias categorías de problemas a considerar y los principales son los relacionados con *OpSec* (seguridad de operaciones). ¿Qué pasa si configuro un blog sobre un servicio cebolla, escribo un artículo, y lo firmo con mi nombre? Tal vez eso era lo que buscaba hacer, pero puede ser un sencillo error mío. Si nos olvidamos que estamos intentando mantenernos a salvo, anónimos, es fácil que bajemos la guardia. “Siempre entro a Tor cuando accedo a este sitio Web, pero hoy se me olvidó... Y ahora tienen mi dirección IP”. Cada vez que se habla con un agente

del FBI, cuentan acerca de cómo estaban buscando rastrear a alguien que utilizaba Tor, y les resultaba muy frustrante porque no pueden encontrarlo. Y, una y otra vez, bastó ser pacientes y mantenerse atentos, porque eventualmente esta persona comete algún error, como no utilizar Tor al identificarse, lo cual lleva a poder encontrarlos. Así que, usar Tor incorrectamente es con mucho el punto más difícil que tenemos que enfrentar.

Otro problema son los metadatos del navegador. Cada vez que sale una nueva versión del navegador, hay algunos nuevos retos que pueden utilizarse para rastrearnos. Por ejemplo, hace unos años Google habilitó una característica que informa al servidor qué tanta batería tiene el dispositivo. Si vas a un sitio Web, y éste pregunta por el nivel de carga, la computadora dirá "tengo 67.74% de carga". Si se entra a otro sitio Web, y éste pregunta también por la batería, obtendrá la misma respuesta. Y como es muy poco probable que haya muchos usuarios de Tor con exactamente mi nivel de carga, es algo que debemos proteger y ocultar de los sitios Web, para que esta información no pueda utilizarse para desanonimizar. Cada nueva versión de cada navegador tiene cosas como ésta que tenemos que descubrir, investigar y corregir.

Un tercer problema es que los navegadores Web no son tan seguros como deberían. Son programas muy grandes y complicados, y siempre hay algún fallo en cómo presentan alguna imagen, o implementan Javascript, o entran a ciertas páginas Web. Hay gente que puede aprovecharse de estos fallos para tomar control de las computadoras cuando entramos al sitio Web equivocado. Esto es cierto en Firefox, es cierto en Chrome —y es cierto también en el navegador Tor.

El cuarto problema a considerar es el análisis de tráfico público, donde las grandes agencias de inteligencia buscan pun-

tos clave de internet. No es imposible que, si vigilan suficiente tráfico, puedan encontrar quién se está conectando hacia dónde.

¿CÓMO AYUDAR?

¿Cómo pueden ayudar? Si están en una universidad con buen ancho de banda, una eficiente manera de ayudar al proyecto es operar *relays*. Cada *relay* tiene una política de salida que nos deja especificar a qué direcciones permitiremos que nuestros usuarios lleguen desde nuestra dirección. Si van a operar un *relay* intermedio (no de salida), todas las conexiones salientes se mantendrán dentro de la red de Tor, nunca serán el último punto antes de salir, y no tendrán ningún problema por parte de los responsables de las redes. No habrá afectación hacia su red. Todos quienes puedan deberían operar *relays*.

También, es importante ayudar a que otras personas comprendan cómo opera Tor. Si sus amigos les muestran la imagen del iceberg, explíquenles acerca de los servicios cebolla en lugar de hablar de la red obscura.

Hay varios puntos a investigar listos para ser atacados. Al respecto, tenemos un congreso anual llamado PET Symposium (*Privacy Enhancing Technologies*, Tecnologías para mejorar la privacidad), su sitio Web es https://petsymposium.org/.

Por último, invitamos a quien tenga la posibilidad de hacerlo a hacer donaciones económicas desde https://donate.torproject.org/.

5

HABLEMOS DERECHO DE TOR, LA HERRAMIENTA QUE GARANTIZA PRIVACIDAD

Cynthia Solís y Alfredo Reyes Krafft
(Lex Informática)

Tor es un software y red libre que permite ser usada por miles de personas de forma anónima, lo cual, entre otras cosas, abre la posibilidad de ejercer el derecho a la libertad de expresión de forma privada, confidencial y abierta. Su finalidad es evitar la vigilancia que cualquier persona, empresa o gobierno pudiera ejercer sobre las personas vulnerables, haciendo esto posible con tan solo pasar los datos por medio de tres servidores.

Tor no toma su nombre del hijo de Odín, heredero del Trono de Asgard; es el acrónimo de The Onion Router, o literalmente El Enrutador Cebolla, que toma la metáfora de las capas de esta planta para poner de manifiesto su objetivo central: enviar información entre distintos puntos o capas de internet de forma segura. Es como picar cebolla: tu información está ahí y llegará en fragmentos, pero no perderá su sabor ni consistencia. Pero como todo, también tiene deficiencias, pues si es utilizado de forma incorrecta la privacidad que pretendía construir, desaparece.

Y es que los avances tecnológicos traen innumerables ventajas para la comunicación entre personas, como acortar distan-

cias y obtener información de casi cualquier cosa, divulgar y obtener información con tan solo teclear, pero donde todo clic es un arma de doble filo, pues también puede convertirnos en un blanco fácil: nuestros datos generados o compartidos durante la navegación pueden caer en las manos equivocadas y, con ello, afectar nuestra seguridad personal y patrimonial.

Por estas posibles situaciones, un grupo de genios de la informática junto con samaritanos de la neutralidad de la red decidieron ceder sus conocimientos e infraestructura para que más gente pudiera gozar de las libertades que ofrece internet, y de esta forma crearon el Proyecto Tor.

RESPONSABILIDADES Y LEYES

¿Cualquiera puede usar Tor? Claro, es un programa especializado en anonimato en red, que busca ser fácil y sencillo de usar, y hoy es utilizado a diario por millones de personas, en especial por aquellas que desean no ser rastreadas, como denunciantes de actos de corrupción, periodistas, activistas, disidentes políticos, personas con acceso restringido a la web y... como no todo es miel sobre hojuelas, también un número reducido de individuos que hacen mal uso de esta herramienta.

Entonces, ¿de quién es responsabilidad *real* del uso de este "proyecto cebolla"?, de cada uno de los usuarios de internet que lo utilizan. Al ser anónimo, no se generan ni conservan registros de los sitios visitados, medios de conexión o paquetes de datos utilizados. Esto quiere decir que incluso el Proveedor de Servicios de Internet (ISP) está librado de toda responsabilidad en caso de que la herramienta sea mal utilizada, pues en la actualidad en México, no existe legislación alguna que prevea la corresponsabilidad por violaciones en materia de propiedad intelectual (PI) o

por hechos que se consideren delito, sean cometidos con un uso *normal* de internet, o empleando Tor.

Y sobre las leyes, por una parte, su uso trae implícito hacer válida la garantía a nuestros derechos fundamentales como la libertad de expresión, la privacidad de datos, el anonimato y uso de seudónimos, derechos plenamente reconocidos en diversos instrumentos jurídicos internacionales y nacionales; por el otro, debemos tener clara cuál autoridad nacional tiene facultades para intervenir, por lo general, la división de policía cibernética, ya sea para defender o demandar a particulares, en controversias por su uso.

Y si Tor tiene que ver con las leyes, ¿quiere decir que la información generada, obtenida, almacenada y difundida en el proyecto puede ser prueba en un asunto legal? Sí, siempre que las evidencias se hayan obtenido de forma lícita y estén relacionadas directamente con la conducta que pretende probarse, sin embargo, su valoración quedará sujeta a criterio del juez quien tendrá que hacerse de los medios necesarios para lograrlo.

Por todo esto, consideramos que Tor garantiza la privacidad y el anonimato de las personas que lo utilizan para ejercer su derecho a la libertad de expresión, pues mediante sus capas de cifrado de la información, el mensaje se entregará a su destino de forma segura, íntegra y secreta, sin que esto cree problemas de ningún tipo con las leyes nacionales.

ACERCA DEL ANONIMATO Y PSEUDONIMATO

El anonimato no solamente es una alternativa para cuidar o proteger la privacidad, sino que es un derecho. Irónicamente, si se han dado cuenta, a pesar de que tenemos acceso a muchísima información, hay muchas cosas que vemos en blanco y negro,

donde ciertas tecnologías *per se* están satanizadas (siendo que en realidad son neutrales al uso), como puede ser el caso de las criptodivisas tipo *bitcoin*: cuando un usuario no avezado escucha esta palabra, la reacción instintiva es tomarlo. Y bueno, sí, con bitcoin puedes comprarte una pizza o exigir el pago de un rescate, pero no es que la tecnología sea mala. El uso que se le da a una tecnología puede presentarse en paralelo a utilizar un bate de beisbol para jugar o matar a alguien. En ese sentido, lo mismo pasa con el tema del anonimato en línea.

Si bien nuestra formación es en derecho, tenemos ya varios años dando clases a ingenieros, y hemos establecido un lenguaje común. En el entorno jurídico es común escuchar hablar de la red Tor, y el comentario directo es, "oye, pues eso es malo ¿no?" O la *Deep web:* todo lo que viene de ésta es malo acríticamente y por omisión.

Nosotros sabemos que hay muchos procesos de industrias completamente lícitas que se llevan a cabo por cuestiones de seguridad en la red profunda.

Siempre explicamos el tema de los derechos que confluyen como si fuera una alberca de pelotas que al final tienen que coexistir y convivir. Tenemos derechos constitucionales a la transparencia, a la libertad de expresión, sí, pero también están consagrados al mismo nivel el derecho a la privacidad, y en particular a la autodeterminación informativa.

Nosotros podemos decidir también, sin necesidad de ningún procedimiento legal, técnicamente hablando, cómo controlar nuestra privacidad, y esto es algo muy añejo. Si hacemos referencia, por ejemplo, a las fiestas en Venecia con las máscaras venecianas, desde épocas renacentistas la posibilidad del anonimato para lograr un *ligue* en época de carnaval está implícito; había códigos incluso en la época de Luis XV donde las mujeres,

según los lunares que exhibían formaban parte de un lenguaje. Una persona podía ir a las fiestas, e indicar discretamente si estaban con intenciones de conseguir pareja, de estar comprometida o casada. Son códigos que, de alguna manera, nos han ayudado toda la vida a tratar de cuidar nuestra privacidad.

El tema de la publicación de obras bajo pseudónimos, aún hoy es perfectamente vigente. Pueden contraargumentarse casos en que, por seguridad pública, se ha limitado este derecho: en algún momento se prohibió tener cristales polarizados en los vehículos, pero no significa que fuera ilícito ponerle una placa o una mica, que no es lo mismo que el vidrio polarizado, pero de alguna manera trata de crear un entorno más privado —es lo mismo que colocar cortinas. Cada quien decide cuánto exhibe de su vida; el tema del anonimato en red también sirve, no solamente para tener acceso a información que no se encontraría en la red abierta, sino que también protege la vida de muchos periodistas. Es por todos conocido que México es un país muy peligroso para dedicarse al periodismo, y muchas de las investigaciones que vemos publicadas, por ejemplo, el tema de la corrupción en el sexenio de Enrique Peña Nieto, difundido en medios como la *Casa blanca,* y otras investigaciones, se han dado gracias al uso de la red Tor. En realidad, el uso periodístico de mecanismos de anonimización en realidad no es algo nuevo, y no es algo que *per se* esté prohibido.

Las leyes de varios países consideran, como en el caso de Venezuela, el uso de identificadores anónimos como una conducta expresamente prohibida. En algunos otros lugares del mundo, las conexiones deben de identificar quién está conectándose; es una cuestión en la cual cada país determina soberanamente sus reglas.

En Estados Unidos se consideran a la familia: siempre digo que esta es la principal prioridad de los derechos humanos. A

muchos le habrá pasado en la infancia o adolescencia, cuando usábamos predominantemente el teléfono fijo, que estabas hablando con tu amiga, y la mamá del otro lado oyendo. O al llegar correspondencia, el consabido "¡ay hijo! ya te abrí tu correspondencia porque a lo mejor era algo urgente". En Estados Unidos, por ejemplo, supuestamente se reconoce el derecho a la privacidad como algo fundamental, pero en aras de la seguridad nacional viola sistemáticamente derechos humanos, como ocurrió en el caso San Bernardino,[1] mismo que revivió una legislación del siglo antepasado que permite que, con la simple sospecha de alguna actividad que vaya en contra de la seguridad nacional de Estados Unidos, pueda intervenirse la comunicación privada.

Entonces, realmente hay un tema: ¿cómo podemos, como ciudadanos sea de donde sea que lo seamos, y particularmente si acostumbramos viajar y entrar a distintas jurisdicciones, mantener nuestra privacidad, cuidarla, al igual que nuestra identidad, si basta una *sospecha fundada* para que nuestros dispositivos sean vulnerados?

Por otro lado, muchas personas —tomemos por ejemplo a los funcionarios públicos— tienen cuentas alternas en redes sociales. La ocupación profesional de una persona significa indirectamente que se tiene que *cuidar la pose,* esto es, no pueden decir cualquier cosa en redes, se espera que disocien sus opiniones personales de las emitidas oficialmente. Esto puede verse como un factor que en lo personal limita su libertad de expresión; incluso que estén cometiendo ilícitos en su calidad de servidores públicos, por lo que muchos prefieren abrir una cuenta alterna con la que sí puedan decir lo que piensan, aunque tal vez inclu-

1. Caso en que el FBI hackeó el teléfono celular de uno de los ejecutantes del ataque terrorista de diciembre de 2015 en que resultaron asesinados 14 personas (n. del e.).

so vaya en contra de la política de su entorno laboral. Esto es, el derecho a tener una identidad *oficial* y una distinta para el ámbito privado puede incluso leerse como un tema de derechos humanos.

Como lo comenté, hemos tenido la fabulosa experiencia como docentes y consultores de trabajar con muchas instituciones de seguridad pública, personas de la Marina, del CISEN, de la Policía Federal, que gracias al uso de la red Tor han logrado desmantelar redes, por ejemplo, de trata de personas, de pornografía infantil —porque naturalmente, las operaciones de inteligencia policial tienen que ir al lugar donde suceden las cosas. Las redes de anonimato existen, y el uso que se le da a la tecnología depende del usuario, no se puede trasladar una carga moral a una herramienta. Las redes de inteligencia policial también requieren del anonimato. Lejos de ver las cosas en blanco y negro, hay que entender que estamos en un mundo donde todo o muchas cosas sean en escala de grises. Tener la posibilidad de manejo del anonimato no es bueno ni malo, sino que es una excelente herramienta para diversos fines, incluido para que nosotros nos sintamos seguros o incluso protegemos nuestra vida.

LA PERSPECTIVA DE LOS USUARIOS

La gente hoy en día usa Tor para realizar todo tipo de actividades. Si eres una de ellas, probablemente lo haces de forma segura, tranquila. Sin angustia de que alguien vaya a llegar a tener acceso o de alguna forma vincularte con un contenido específico. Y no por que seas un delincuente: normalmente no estás buscando comprar armas o comprar drogas, sino únicamente llegar a la información sin dejar un rastro que vincule de vuelta hacia ti. Y es en este sentido como nosotros podemos actuar,

vean; la red Tor tiene un promedio de dos millones de usuarios, aunque en México, solamente alrededor de 15 000.

Estamos procurando en este sentido tener la oportunidad de que la propia UNAM participe en un proyecto importante y trascendente en relación de apoyo a la red Tor, pero nos topamos con una inquietud fuerte: jurídicamente, ¿podemos hacerlo? Es decir, para una institución como la UNAM, ¿qué implicaciones tendría operar o administrar o integrar una red Tor o integrarse a la red Tor?, ¿incurriría en alguna responsabilidad como institución? De alguna forma, ¿podría esto, en lugar de ayudar, perjudicar a los que participen de manera directa o indirecta?

Y derivado de lo que ya se ha comentado, nos dimos cuenta de que no. Hay, sí, algunas espadas de Damocles por ahí por eso, tal y como comentamos previamente, y como otros participantes del coloquio han comentado, y como parte de la renegociación del T-MEC[2] posiblemente, esto suponga un cierto foco amarillo o rojo que debemos de cuidar para el beneficio de todo esto, pero en un análisis concienzudo nos dimos cuenta de que, por el contrario, es menester garantizar precisamente la privacidad y las libertades fundamentales de los partícipes de ésta y muchísimas otras organizaciones.

ANONIMATO, DERECHOS DE AUTOR Y DERECHO A LA PRIVACIDAD

Un punto importante a tratar, independientemente de la parte relacionada con la privacidad, es la que toca la Ley Federal del

2. En las fechas en que tuvo lugar el coloquio que este texto recoge, el Tratado de Libre Comercio de América del Norte (TLCAN) estaba en proceso de renegociación para convertirse en el acuerdo trilateral México-Estados Unidos-Canadá (T-MEC) (n. del e.).

Derecho de Autor en relación con el anonimato (*Diario Oficial de la Federación,* 1996) y toda la parte de prestadores o proveedores de servicios de internet (ISP), y también lo que dice La Ley Federal de Telecomunicaciones (*Diario Oficial de la Federación*, 2014a) precisamente en el apartado de colaboración con la justicia, es el de qué manera, directa o indirecta, pudieran afectar o tocar estos temas que nos atañen. ¿Qué responsabilidad puede llegar a tener un prestador de servicios de internet respecto del contenido que viaja en su red?

Aquí hay una cuestión interesante porque hay diferentes posturas en el mundo. Según el modelo europeo, se asemeja a los prestadores de servicios de internet con editores. Cuando publicamos algo en internet, primero se queda en un espacio intermedio (llámese *espacio pre-publicación* o similar), y únicamente después de un proceso se publica. Entonces, hay algunas tesis y disposiciones europeas para algunos de sus países, en particular que indican que el proveedor de servicios de internet funge como un editor, luego entonces, tiene una responsabilidad compartida con quien publica en caso de tener algún tipo de problema relacionado con la propiedad intelectual. ¡Y esa es una responsabilidad muy fuerte! Ese proceso es automático, y el proveedor de servicios no hace análisis del contenido que transmite.

Por otro lado, en Estados Unidos manejan que el proveedor de servicio de internet no asume ninguna responsabilidad, hasta en tanto tenga noticia o conocimiento de que el contenido infringe derechos de autor. Si ese es el caso, y sólo si no toma medidas en consecuencia, se vuelve corresponsable.

En México había una problemática en relación a qué vamos a hacer, a qué postura vamos a tomar. La postura que tomamos algunos proveedores de servicios de internet en el Congreso se estuvieron trabajando y planteando algún modelo de operación.

El símil que utilizaban —y fue una postura, y no de Telmex ni nada de eso, porque no vamos a hablar de proveedores, pero una postura interesante— era en el sentido de que si se presenta una llamada por teléfono que hace un secuestrador a la familia de un secuestrado, ¿vamos a volver corresponsable del delito de secuestro al operador de servicio de telefonía? No, puesto que, ¿éste qué culpa tiene? El proveedor de telefonía fue el medio, fue el canal. A fin de cuentas no tuvo que ver con el contenido precisamente de esa comunicación y era el punto de referencia que se manejaba precisamente en México.

LA CONSERVACIÓN DE METADATOS

No fue sino hasta un poco después, hace unos años, que se modificó el título octavo de la Ley Federal de Telecomunicaciones y Radiodifusión (*Diario Oficial de la Federación*, 2014a) con un capítulo denominado de la colaboración con la justicia, donde los concesionarios de telecomunicaciones, y en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito fundado y motivado de autoridad competente en los términos que establecen las leyes. Por tanto, todos los concesionarios de telecomunicaciones, y en su caso los autorizados, deberán entre otras cosas, conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice una numeración —propia o arrendada bajo cualquier modalidad— que permitan identificar con precisión los siguientes datos: nombre, denominación o razón social y domicilio del suscriptor; tipo de comunicación: transmisión de voz, buzón vocal, conferencia, datos, servicios suplementarios, como el reenvío o transferencia de llamada; servicios de mensajería multimedia, incluidos los servi-

cios de mensajes cortos servicios multimedia y avanzados; datos necesarios para rastrear e identificar el origen de destino de las comunicaciones de telefonía móvil; número de destino; modalidad de líneas o contrato de plan tarifario como la modalidad de líneas de prepago; datos necesarios para determinar la fecha, hora y duración de la comunicación así como el servicio de mensajería multimedia. Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio, y la etiqueta de localización, es decir, identificador de celda desde la cual fue activado el servicio. En su caso, identificación y características técnicas de los dispositivos incluyendo entre otros los códigos internacionales de identidad, de fabricación del equipo y del suscriptor. La ubicación digital del posicionamiento geográfico de las líneas telefónicas y la obligación de conservación de datos comenzará a contarse a partir de la fecha en la que se haya producido la comunicación, tendría una vigencia de un año y si hay un tipo de recorte o modificación tendría que conservarlo por un año más.

Cabe mencionar que, si bien la ley obliga a conservar toda esta información, por término de un año, muy pocos proveedores tienen la capacidad tecnológica para hacerlo. La mayor parte de ellos, en la práctica, reducen el tiempo de conservación a unos tres meses. Y esto nos obliga a preguntarnos ¿esto nos preocupa?, ¿por qué?

Es importante anotar que todos estos puntos constituyen a los *metadatos* —la información acerca de la comunicación. Es interesante que no se está pidiendo conservar el contenido de la comunicación, sino que únicamente se conserva el dato de conexión, la referencia.

Sin embargo, uno de los principales problemas del uso de metadatos y de recopilación de ese tipo de datos es que faci-

litan a cualquier proveedor o plataforma generar la suficiente información como para eventualmente inferir de qué se trató esa comunicación, crear perfiles de usuario.

Disposiciones como esta ponen en riesgo precisamente a los usuarios que acceden a través de redes anonimizadoras, como lo es Tor. Por eso es importante integrar esto con una situación como la que estamos viviendo. Ahora, ¿por qué sí es importante, por así decirlo, el derecho de contar con esa información para las autoridades investigadoras? Argumentemos desde el otro lado de la moneda: ¿servirá de algo realmente a las autoridades? Hacer imputación no necesariamente, pero cuando menos propiciar o facultar la investigación de un hecho ilícito.

En la práctica, tenemos que aterrizar hacia la situación real. Se habla mucho de que el gobierno espía y demás, y no lo ponemos en duda. Pero honestamente, no creo; esto es, no todos somos dignos de ser espiados, porque ni siquiera se tiene la capacidad para hacer un monitoreo tan a profundidad de la sociedad.

Hay un grupo de personas que son blancos importantes para los gobiernos, que indudablemente están siendo monitoreados, pero no es del grueso de la población. Ahora, en el tema de imputaciones legales, realmente en la práctica para llevar una causa penal es suficientemente complicado, porque para empezar estamos hablando ya de delitos. Para obtener la información que mencionamos, el primer paso es asegurar que la conducta específica que se busca perseguir esté tipificada, es decir, que esté específicamente descrita en una norma. Hay diferentes elementos del delito que estén identificadas, las partes como el sujeto activo y el sujeto pasivo, que la conducta realmente se haya llevado a cabo la intencionalidad. Entra en juego, incluso, lo que conocemos como las causas de justificación, es decir, que no se haya actuado en cumplimiento de un deber o en

ejercicio de un derecho o en legítima defensa o por un tema de estado de necesidad.

Entonces realmente, en la práctica, para que una causa penal llegue o abra una carpeta de investigación tampoco es tan sencillo. En toda investigación, debe existir un análisis donde hay jueces de control y otras autoridades que exijan determinados puntos. Sin embargo, hay otras que con solo levantar el teléfono puedes solicitar precisamente esta información. Y debemos de considerar, que algo tan sencillo como una dirección IP es precisamente una referencia básica, un número único que identifica un equipo en una red. Se vuelve necesario debatir, ¿qué es lo que se identifica?, es decir, ¿es mi dirección IP realmente un dato personal?, ¿o es simplemente un número, que si acaso podría identificarme si hay una referencia de manera directa o indirecta?

El establecer una obligación legal de conservación por un año a partir del momento en el que se genera una comunicación supone el riesgo, como una espada de Damocles en la cabeza. Debemos de tener cuidado, todos los puntos e inquietudes que se presentan al respecto son alertas; muchos usuarios comparten información personal o compartimos datos que nosotros mismos autorizamos de formas probablemente más rastreables aún que lo que hasta aquí se ha abordado.

¿Qué porcentaje de los usuarios ha leído el contrato de prestación de servicios de empresas proveedoras de infraestructura? Gmail, Facebook y similares. A todos esos proveedores los autorizamos precisamente en muchos términos de lo establecido en el contrato a seguirnos, a conocer nuestra ubicación, a lo que tanto se critica que hacen los proveedores y gobiernos. El empleo de mecanismos de anonimato nos sensibiliza, sí, a toda la información que compartimos con consentimiento. Piensen

en la riqueza de información que se otorga a los asistentes digitales como los teléfonos con servicio de geolocalización, monitores de actividad deportiva, etc. —y si queremos aprovechar su funcionalidad, no podemos ocultarles la información que nos interesa que procesen.

HACIA ADELANTE Y HACIA LA CONCLUSIÓN

Y si bien nos preguntan frecuentemente si se puede apuntar hacia una modificación a las leyes para armonizar mejor los derechos, esto resulta muy complicado. Tomemos como ejemplo las reformas de 1999, en que por disposición legal se establece que la intrusión a un sistema se va a considerar como un delito solo si éste vulnera un mecanismo de seguridad. Eso sería tan tonto como decir que: voy a entrar a tu casa, o a meterme a tu casa, pero sólo si tiene puerta; si no tiene puerta, no voy a cometer allanamiento de morada. Lo peor es que no define qué se entiende por mecanismo de seguridad, es decir, si no existe coincidencia entre la parte jurídica y la parte técnica, con el avance tecnológico que se está haciendo en el mundo electrónico vamos a perder. Esto es, el análisis jurídico no puede hacer una separación de responsabilidades diciendo, "yo no tengo nada que ver con lo tecnológico" o viceversa —todos tenemos que saber de ambos lados.

Y obviamente, estamos hablando de no satanizar o criminalizar a la tecnología porque *per se,* una tecnología no es ilícita ni lícita. Debemos de buscar como principio la neutralidad tecnológica.

En México no hay ninguna disposición que prohíba el cifrado. Por el contrario, lo válida el modelo de firma electrónica; la ley de firma electrónica avanzada (*Diario Oficial de la Federa-*

ción, 2014) utiliza modelos de cifrado, es decir, para poder firmar requerimos cifrado asimétrico, o cifrado con la clave privada del firmante, y eso constituye una firma electrónica. Hay disposición e incluso obligación legal para la administración pública y posibilidad de utilizar modelos de firma electrónica para la actividad comercial sin limitación alguna. Una gran fortaleza de los esquemas de anonimato basados en cifrado es que, si el cifrado es lícito para ciertos usos, el cifrado es lícito y punto.

A modo de conclusión, el uso de una red de anonimato es indudablemente lícito. Hay muchos casos en que nuestro anonimato puede romperse, la identidad puede exponerse, y vale la pena revisar las muchas maneras en que un usuario tiene que *hacerse responsable* de su uso del cómputo; parte importante de lo que intentamos abordar aquí son las tensiones —así como las consonancias— que hay en el entramado legal, los derechos del individuo y de la colectividad.

BIBLIOGRAFÍA

Diario Oficial de la Federación (1996, 24 de diciembre). *Ley Federal del Derecho de Autor*. Ciudad de México, México. Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=4907028&fecha=24/12/1996.

Diario Oficial de la Federación (2014, 21 de marzo). *Ley de Firma Electrónica Avanzada*. Ciudad de México, México. Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5337860&fecha=21/03/2014.

Diario Oficial de la Federación (2014a, 14 de julio). *Ley Federal de Telecomunicaciones y Radiodifusión*. Ciudad de México, México. Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014.

6

CREAR TECNOLOGÍA QUE RESPETE AL USUARIO. DISEÑO DE EXPERIENCIA DE USUARIO EN TOR

Antonela Debiasi

Mucho antes de ser parte del equipo de experiencia de usuario en el Proyecto Tor, pasé semanas leyendo los canales públicos de IRC de la comunidad. Ahí, note que la palabra diseño (*design*), se utilizaba para referirse a una gran diversidad de aspectos: el software, la red, los dibujos, la topología, el código... confuso, pero la amplitud del concepto es la prueba fáctica de que el proceso de diseño es un método proyectual que atraviesa distintas disciplinas. En tal caso, es natural vivir el proceso de diseño como un trabajo abierto.

En el Proyecto Tor se considera que la manera en que se trabaja te define, por eso decidimos hacerlo de manera abierta y colaborativa.

Creemos que la forma en la que trabajamos —la modalidad de los procesos— tiene una relación directa con lo que producimos. Si cambiamos la forma de trabajar, transformamos los resultados de la producción. El colectivo Tiqqun,"órgano de enlace del Partido Imaginari", cita a Moulier-Boutang en su manifiesto *La hipótesis cibernética* (Tiqqun, 2013):

Su teleología ya no es la del proletariado o de la naturaleza, sino la del capital. Su perspectiva es profundamente en la actualidad la de una economía social, de una "economía solidaria", de una "transformación del modo de producción", no ya por colectivización o estatización de los medios de producción, sino por colectivización de las decisiones de producción. Como lo muestra por ejemplo un Yann Moulier Boutang, finalmente de lo que se trata es de que sea reconocido "el carácter social colectivo de la creación de riqueza".

MÉTODO Y EQUIPOS DEL PROCESO DE TRABAJO ABIERTO

"Abierto, remoto y libre", este es el modo de trabajo que aplicamos a nuestra metodología de diseño, donde desarrolladores y comunidad trabajan en conjunto para mejorar el software y el equipo de diseño funciona como un conector de ideas o un puente. Usando esta modalidad de trabajo abierta, hicimos iteraciones internas basadas en conceptos surgidos de investigaciones anteriores, de ideas de users y de sugerencias en *tickets*, que en su conjunto nos ayudaron a definir el flujo más seguro e intuitivo para nuestros usuarios.

Lo primero que debemos entender es que hay momentos de divergencia y otros de convergencia. Y a su vez, es importante mantener el ritmo entre ellos. Aquí el proceso:

1. *Partimos del planteamiento de un problema*. Ese es el inicio, no es exactamente el problema a resolver, sino una descripción que sirve para identificar los síntomas a resolver.
2. *Exploramos el problema y las interrogantes que dispara el análisis*. Realizamos preguntas sencillas, de no más

de ocho palabras, para definir el espectro del problema a resolver y sus alcances. Una vez que visualizamos estos aspectos, comenzamos a pensar en cómo resolverlos.

3. *El abanico de posibilidades se vuelve a abrir*. Repensar el problema y proyectar soluciones implica analizarlo desde distintas perspectivas. La única manera de que esto ocurra es teniendo un equipo diverso.
4. *Probamos (testing) con usuarios y volvemos al punto 1.*

Por otra parte, el grupo de experiencia de usuario del Proyecto Tor, que trabaja de forma horizontal, se divide en varios equipos:

- Red. Desarrolla el *backend* de Tor, básicamente, todo lo que envía y recibe bytes de la red.
- Métricas. Se encarga de las mediciones y estadísticas de la red.
- Aplicaciones. Desarrolla y mantiene Tor Browser para computadora y Android.
- Comunidad. Encargado de establecer vínculos entre organizaciones que defienden derechos humanos, como Karisma en Colombia o Derechos Digitales en Chile.

Respecto a este último punto de la comunidad, podemos hacer una aclaración: la situación geográfica de un usuario no debería modificar su condición de ser humano. Los usuarios censurados viviendo en países opresores tienen las mayores dificultades para lograr comunicaciones seguras y anónimas (Fifield, 2017).

Como parte de nuestra iniciativa del Sur Global, nos conectamos con comunidades que se encuentran físicamente en-

tre la línea del Ecuador y el Círculo Polar Antártico, como India, Uganda, Colombia y Kenia. Viajamos y realizamos pruebas de usabilidad, en su mayoría con personas que se definen como "usuarios del día a día", haciendo alusión a su relación con la tecnología, pero también aplicamos las pruebas con aquellas que se reconocen como expertos técnicos (Habib *et al.*, 2018; Duck Duck Go, 2017).

CREAR TECNOLOGÍA QUE RESPETE AL USUARIO ES UNA DECISIÓN DE DISEÑO

En las evaluaciones realizadas, 93% de las personas a las que llegamos dijeron que creían que necesitaban alguna clase de protección online. Siguiendo el método de los cinco usuarios (Nielsen, 2000), realizamos rondas de pruebas de usabilidad sobre algunas mejoras específicas que trajeron luz sobre los diversos modelos mentales y niveles de conocimiento técnico que tienen nuestros usuarios. Por ejemplo, en nuestros viajes conocimos en Colombia a una agricultora que forma parte de una productora de café autogestionada que usa Tor para tener comunicaciones seguras entre las compañeras del grupo y en Uganda, a un activista ambiental y periodista de la ciudad de Hoima que utiliza Tor para publicar su blog de forma anónima. Esta inmersión sirve para validar —o no— nuestras respuestas en distintos contextos.

Parte del trabajo con las pruebas de usabilidad, nos permitió llegar a las personas que utilizan nuestro software en condiciones extremas, como por ejemplo una infraestructura deficiente, paquetes de datos muy costosos o hardware muy antiguo. Ademas, en abril de 2018, fuimos a dictar un taller de seguridad digital y a realizar pruebas de usuarios con un grupo de activistas ambientales a Hoima, una ciudad petrolera de 30 000 per-

sonas, a 200 kilómetros de Kampala, la capital de Uganda. Me acompañaba Alison Macrina, activista y feminista, en ese entonces líder del equipo de comunidad, y una, como parte del equipo de usabilidad. Las computadoras eran viejas, tenían Windows 98, pero habíamos logrado convocar a la reunión. A los cinco minutos de iniciado el taller, se fue la luz. Una pequeña tragedia comparada con otras amenazas comunes en otros lugares que visitamos: secuestro de computadoras portátiles por parte de la policía local o el partido político en turno, obligando a periodistas a desclasificar sus fuentes.

La principal reflexión en este proceso, es que sería egoísta no preguntarnos sobre estos contextos y los valores que definen la toma de decisiones en la práctica. Por lo tanto, conocer la realidad de nuestros usuarios nos ayudó a entender su contexto, empatizar con ellos y pensar soluciones adaptadas a sus necesidades (Qu *et al*., 2019). Los integrantes del equipo de Tor creemos que debemos ser capaces de ofrecer un producto que pueda usarse sin conocimientos técnicos. No queremos distribuir software sin educación. Queremos empoderar a nuestros usuarios mediante la educación. Hoy, tener un *switcher* expuesto en la interfaz de usuario, que permita al usuario decidir si compartir o no, *opt-in* u *opt-out*, sus datos a terceros, es una decisión política.

EDUCAR A LOS USUARIOS PARA QUE TENGAN EL CONTROL DE SU NAVEGACIÓN

Nuestra iniciativa de educación del usuario es pensar en el primer acercamiento al navegador como una oportunidad de usar metáforas locales y palabras simples para explicar conceptos complejos (Sundblad, 2010). Todos los mitos tecnológicos surgen de una falta de comprensión (Moran y Salazar, 2018). Además,

el proceso de trabajo abierto aplicado en todos los equipos del proyecto, sumado a los análisis resultantes de las pruebas de usuarios, incentivaron grandes mejoras en la interfaz de usuario y en el desarrollo del software (Oates *et al*., 2018).

El Tor Browser 8 se lanzó en septiembre de 2018 con tres novedades: indicadores de seguridad para sitios .onion; nueva pantalla de circuito; *Onboarding* para nuevos usuarios.

- Indicadores de seguridad para sitios *.onion* (imagen 1). Antes, cuando los usuarios visitaban un sitio onion sobre http recibían como *feedback* de seguridad, con mucha suerte, un signo de información [i] y un candado rojo. En pos de aumentar la confianza de los *onion services*, decidimos identificar a estos servicios con un icono de cebolla que refleja el estado de seguridad del sitio, considerando sus certificados y alertando sobre sus riesgos (Winter *et al*., 2018).
- Nueva pantalla de circuito o circuit display (imagen 2). Es un componente de la interfaz de usuario de Tor Browser, y parte de su experiencia. Cuando se escribe una *url* en

Imagen 1
Indicadores de seguridad presentados al visitar un sitio onion, con diferentes niveles de seguridad a nivel protocolo

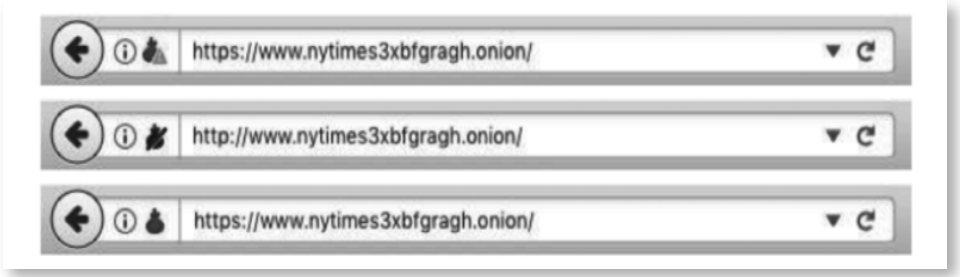
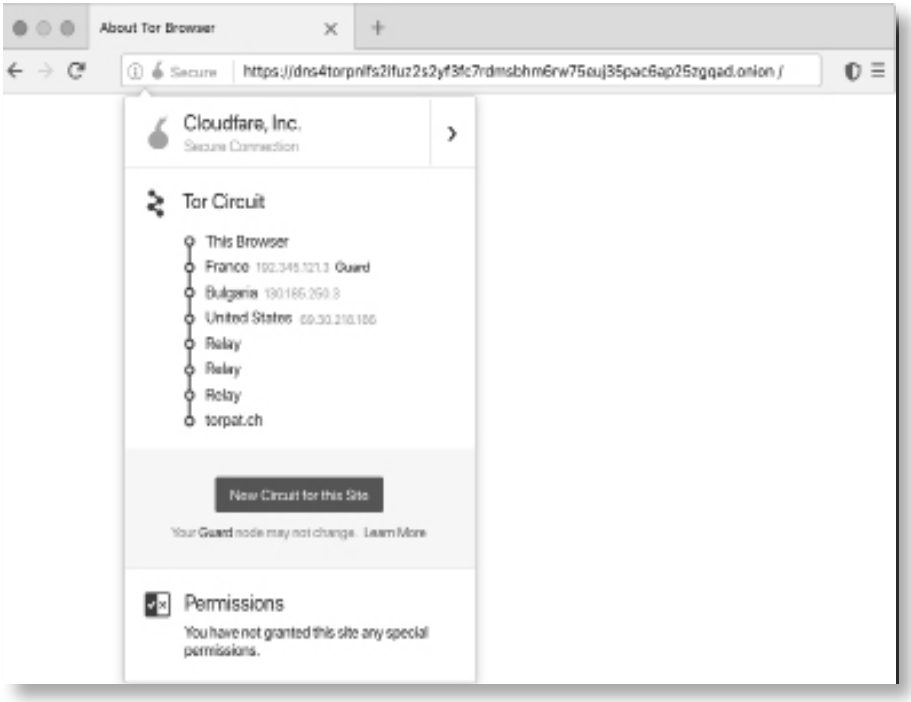


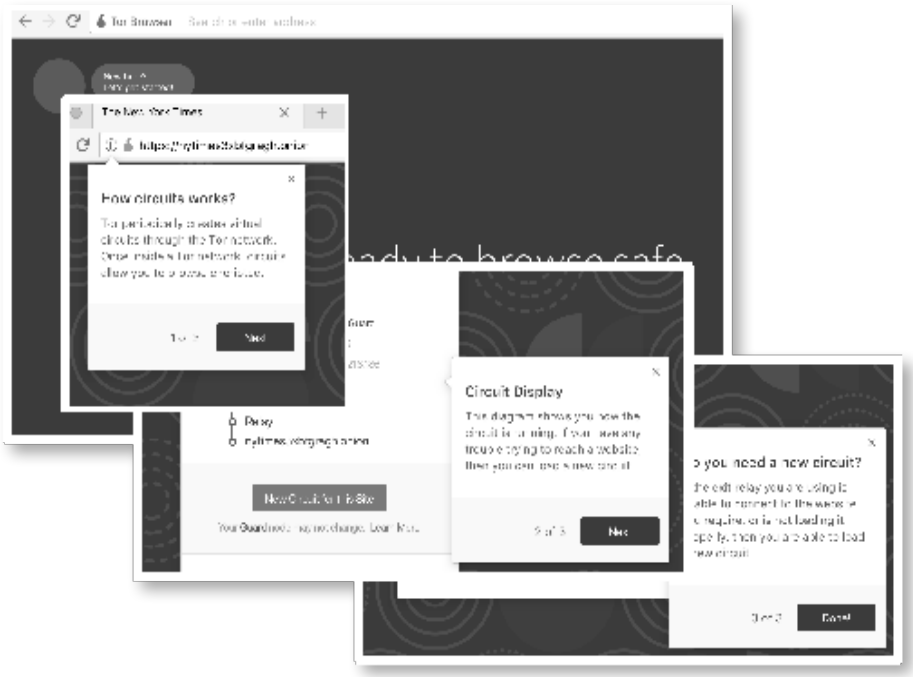
Imagen 2
Pantalla de circuito, o circuit display, en Tor Browser 8



la barra de direcciones, el navegador hace una conexión a la red Tor. Este diagrama muestra cómo se ha realizado la conexión entre nodos. Mirando el *display*, los usuarios pueden rastrear su conexión y mejorar la comprensión sobre cómo Tor ha construido su circuito, identificar su nodo, y guardar y pedir un nuevo circuito si lo necesitan.

- *Onboarding* para nuevos usuarios (imagen 3). Ayuda a establecer confianza con los primerizos, a través de éste nos esforzamos por enseñar cómo la privacidad y seguridad de Tor pueden proteger a los usuarios en diferentes niveles: la capa de aplicación y la capa de red.

Imagen 3
Parte del proceso de onboarding: explicación acerca del uso de circuitos



CONCLUSIÓN

Todos los integrantes del equipo del Proyecto Tor creemos firmemente que educar usuarios es empoderarlos, y que la infraestructura define la experiencia.

El acceso a tecnologías de la privacidad y el anonimato en internet es clave para crear entornos seguros de intercambio y reflexión. La forma más transparente y escalable de facilitar el acceso es creando lazos entre comunidades vecinas y vulnerables, y distribuyendo software usable para todo el mundo.

BIBLIOGRAFÍA

Duck Duck Go (2017). *A Study on Private Browsing: Consumer Usage, Knowledge, and Thoughts*. Consultado en https://duckduckgo.com/download/Private_Browsing.pdf (2020.10.05)

Fifield, D. (2017). "Threat modeling and circumvention of Internet censorship" (Tesis doctoral , UC Berkeley). Consultado en https://www.bamsoftware.com/papers/thesis/ (2020.10.05).

Habib, H., *et al.* (2018). "Away from prying eyes: analyzing usage and understanding of private browsing", en *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (pp. 159-175). Consultado en https://www.usenix.org/system/files/conference/soups2018/soups2018-habib-prying.pdf (2020.10.05).

Moran, K., y K. Salazar (2018). "Technology Myths and Urban Legends". *Nielsen Norman Group.* Consultado en https://www.nngroup.com/articles/technology-myths/ (2020.10.05).

Nielsen, J. (2000). "Why you only need to test with 5 users". *Nielsen Norman Group,* Consultado en https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/ (2020.10.05).

Oates, M. *et al.* (2018). "Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration". *Proceedings on Privacy Enhancing Technologies,* 2018(4), 5-32. Consultado en https://content.sciendo.com/downloadpdf/journals/popets/2018/4/article-p5.xml (2020.10.05).

Qu, L. *et al.* (2019). "Towards better security decisions: applying prospect theory to cybersecurity", en *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (*pp. 1-6). Consultado en https://dl.acm.org/doi/10.1145/3290607.3312782 (2020.10.05).

Sundblad, Y. (2010). "UTOPIA: participatory design from Scandinavia to the world", en *IFIP Conference on History of Nordic Computing* (pp. 176-186). Springer, Berlin, Heidelberg. Consultado en: https://link.springer.com/content/pdf/10.1007%2F978-3-642-23315-9_20.pdf (2020.10.05).

Tiqqun (2013). “La hipótesis cibernética”, en *Tiqqun. Organe de liaison au sein du Parti Imaginaire* (2). Consultado en: https://tiqqunim.blogspot.com/2013/01/cibernetica.html (2020.10.05).

Winter, P. *et al.* (2018). “How do Tor users interact with onion services?”, en *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 411-428). Consultado en https://www.usenix.org/conference/usenixsecurity18/presentation/winter (2020.10.05).

7
INVESTIGACIÓN DE USUARIOS Y SOFTWARE LIBRE

Sajolida
(Proyecto Tails)

El presente artículo abordará el Proyecto Tails, nombre elegido al ser acrónimo de *The Amnesic Incognito Live System* (El Sistema Vivo, Amnésico e Incógnito). Compartiremos algunos métodos que estamos usando para asegurarnos que sea cada vez más fácil de usar, aspecto que llamamos *usabilidad*, así como reflexiones sobre la investigación de necesidades de usuarias y usuarios, buscando comprobar que éstas queden satisfechas y, con ello, la gente use nuestros programas. Porque pienso que hay algunos conflictos y algunos roces con la cultura que veo en torno al software libre.

THE AMNESIC INCOGNITO LIVE SYSTEM

Tails es un sistema operativo portable que protege tu privacidad y ayuda a evitar la censura. Es parecido a Windows, macOS o GNU-Linux, es decir, es un entorno de computación completo pero en vez de instalarlo en el disco duro del ordenador, Tails se instala en una memoria USB. Para usarlo, con la computadora apagada se conecta la USB con Tails, la prenderemos eligiendo

que cargue desde la USB en vez del disco duro y listo, podremos trabajar y navegar sin usar el sistema operativo del ordenador.

Tails tiene un diseño sencillo de ventanas, escritorio, menús y aplicaciones, pues está basado en otras propiedades y características:

- *Es software libre.* Es una distribución Linux basada en Debian y que depende de muchos otros proyectos de software libre como Tor, una red para el anonimato, o GNOME, el entorno gráfico por defecto en Debian y en Ubuntu.
- *Es un sistema portable.* Sólo correrá en la memoria RAM del ordenador y cuando lo apaguemos no dejaremos ningún rastro de lo que hicimos en la computadora. Esto nos permite, por ejemplo, llevar nuestro USB de vacaciones y usar el ordenador del cibercafé sin dejar nuestros datos ni depender del sistema operativo instalado.
- *Ayuda a evadir la censura en internet*, porque todo el tráfico que sale del ordenador (navegación, correos, mensajerías, etc.) está pasando por la red Tor.
- *Es una caja de herramientas para la privacidad.* Incluye muchas herramientas instaladas, configuradas y listas para usar con la seguridad en mente: el navegador Tor, el cliente de correo Thunderbird, el gestor de contraseñas KeePassXC, OnionShare para compartir archivos, etcétera.

Al hablar de los usos, el usuario más famoso de Tails quizás sea Edward Snowden. Dijo que todos los periodistas que reportaron las revelaciones sobre la vigilancia de masas en el 2013 dependían de Tails y trabajaban con él únicamente a través de Tails. Ampliando un poco el abanico de posibilidades, presentaré brevemente tres ejemplos:

- Periodistas en México usan Tails para investigar violaciones de derechos humanos por parte de empresas privadas. Cuando hacen investigación en internet sobre estas empresas, lo hacen desde Tails para que las empresas no sepan quiénes les está investigando. Luego lo usan para comunicarse de manera segura con las comunidades afectadas por estas mismas empresas.
- El *National Democratic Institute* en Estados Unidos usó Tails hace unos años para crear un sistema de recogida de información en torno a unas elecciones en Bielorrusia. Enviaron observadores internacionales que recogían información o incidencias de lo que pasaba durante estas elecciones de manera segura desde Tails.
- Una asociación de profesionales de la seguridad, también en Estados Unidos, está trabajando con casas de acogida para sobrevivientes de violencia doméstica para que usen Tails. Si, por ejemplo, tu marido te maltrata, quizás también este vigilando lo que haces en tu ordenador o qué programas tienes instalados en tu teléfono. Tails te puede dar un entorno más seguro y permitirte evitar la vigilancia aunque estén viviendo debajo del mismo techo.

NUESTRO PROCESO PARA LA USABILIDAD

En los últimos años, el tiempo dedicado a la investigación de usabilidad dentro del proyecto ha sido para asegurarnos que nuestros programas sean cada vez más fácil de manejar. La usabilidad, esta siendo un problema bastante común en el mundo de la privacidad y del software libre. Aquí compartiremos algunos de los métodos que usamos.

PASO CERO, ¿QUÉ DISEÑAR?

Reflexionar sobre para qué servirá nuestro diseño, pensar a qué necesidad responde y entender por qué estamos creando este programa. Este es un debate muy amplio en el cual no se entrará en detalle por el momento.

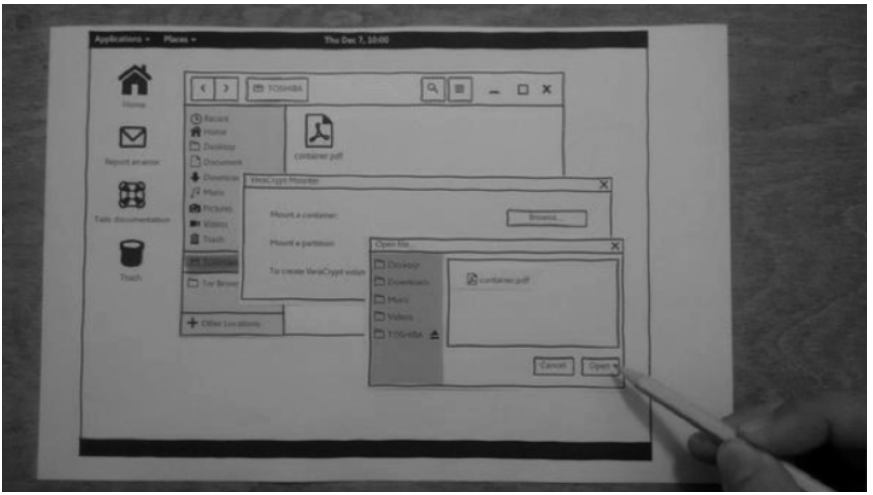
PASO UNO: PROTOTIPOS EN PAPEL

Una vez que tomamos la decisión de desarrollar una nueva funcionalidad o un nuevo programa, ¿qué metodología podemos usar para lograr que este programa sea fácil de usar? Esto es lo que llamamos *usabilidad,* y todas las prácticas que nos llevan a estas conclusiones constituyen lo que llamamos *investigación de usuario*. El primer paso que practicamos en repetidas ocasiones fue hacer un diseño que se pueda testear con personas que utilizan, antes de escribir cualquier línea de código. Hacer prototipos en papel es una herramienta que parece muy sencilla pero en realidad es mágica.

La imagen 1 muestra la fotografía de una prueba de usabilidad que hicimos hace unos meses. Dibujamos las ventanas del sistema operativo y las ventanas de los programas que van a aparecer. Trabajamos con personas representativas: les damos un lápiz que usarán de mouse, para hacer clic, o de teclado, para escribir algo.

Es amable emplear esta metodología junto con un desarrollador. Somos tres personas en la sala: un diseñador, la persona que va luego a escribir el código y una usuaria. La persona que utiliza pretende usar el programa pero con base en los dibujos en papel. El diseñador cambia los dibujos en la mesa para abrir una ventana, una aplicación, etcétera.

Imagen 1
Prueba de usabilidad empleando un prototipo en papel



Para crear los dibujos usamos el programa *WireframeSketcher.* No es software libre, es software propietario, pero funciona con Linux, macOS y Windows. Incluso lo hace con Tails y tiene una versión de demo que permite dibujar estas ventanas de manera muy rápida.

Podemos dibujar el prototipo de papel de la primera idea que tengamos y probarla casi de inmediato. Cuando concluye la prueba, podemos extraer una serie de problemas y corregirlos de manera muy fácil, cambiando sólo los dibujos o haciéndolos nuevos. Esto nos permite ir mejorando el diseño cada vez que testeamos con una persona nueva y así mejorar el diseño de manera muy rápida a lo largo del día. Hicimos varios *sprints* de tres días, empezando de cero: sacar un primer diseño en un par de horas, testear, mejorar, testear otra vez, mejorar otra vez, etc. Después de los tres días ya sabíamos que lo que íbamos a desarrollar sería razonablemente fácil de usar.

Los prototipos de papel, o de baja calidad (*low-fi*) con otras técnicas, nos permite un trabajo:

- *Más rápido,* porque nos ahorra escribir código que luego no funciona con la gente y que tendríamos que tirar a la basura. También nos evita tener debates eternos dentro del equipo sobre lo que va a funcionar, dónde estarán los problemas, si tenemos que hacer A o B, etc. Podemos probar la primera idea que tengamos y aceptar o invalidarla inmediatamente con su uso. También nos ahorra tiempo porque los mismos dibujos sirven de especificaciones a la persona que va a escribir el código. El desarrollador está con nosotros en la sala y ve cómo funciona el programa en directo.
- *Mejor*, porque nos evita diseñar algo que luego no sea posible de implementar o demasiado complicado y nos permite ajustar a lo que es factible. Teniendo un desarrollador en la sala, también le permite proponer soluciones o tener ideas que los diseñadores no tuviéramos o que hubiéramos creído demasiado complicadas. Así nos ajustamos el diseño al máximo de las posibilidades técnicas.
- *Más entregado* porque, al confrontar los desarrolladores al uso, al ver las personas pelear con el diseño, y al haber colaborado en la resolución de estos problemas, los desarrolladores tienen un incentivo muy fuerte a la hora de trabajar en las soluciones. Es un gran trabajo de empatía.

Un libro que destaca sobre el tema y que habla también de metodologías de testeo de usabilidad general es el *Paper Prototyping* (Snyder, 2003).

PASO DOS: CÓDIGO

Una vez que tenemos un prototipo en papel y sabemos que funciona para las personas que lo utilizan, podemos empezar a picar el código.

PASO TRES: PRUEBAS DE USABILIDAD

Después de tener una primera versión del software, nos parece importante volver a hacer otras pruebas de usabilidad.

Reclutamos una persona que la utiliza y le vamos a proponer hacer unas tareas concretas pero con el software ya funcionando en la computadora. Le damos una computadora, unas tareas por cumplir, y la observamos mientras piensa en voz alta: sobre lo que entiende del programa, qué problemas tiene, lo que está haciendo, etc. El objetivo es entender lo que está pasando en su cabeza, e intentar no influenciarla.

La recomendación habitual es hacer estas pruebas con cinco personas. Si lo hacemos con menos, hay un riesgo más alto de no detectar algunos problemas importantes. Pero si lo hacemos con más de cinco personas, volveremos a detectar los mismos problemas una y otra vez y no estaríamos haciendo un buen uso de nuestro tiempo. La recomendación de testear con cinco personas optimiza la cantidad de problemas identificados por el tiempo invertido.

Es preferible grabar las pruebas solo, ya que no se entiende todo al momento y, al volver a mirar la grabación, se ven más matices y más detalles. Los videos también son útiles a la hora de comunicar con los desarrolladores. Cambia mucho si se explica un problema o si lo ven con sus propios ojos.

Para grabar la pantalla (*screencast*) usamos *Kazam*. Para grabar con una cámara externa usamos *VLC*.

Krug (2014) tiene un buen capítulo sobre estas pruebas de usabilidad en su libro *Don't make me think*.

PASO CUATRO: PRIORIZAR LOS PROBLEMAS

De las pruebas de usabilidad vamos a sacar un listado de problemas y priorizarlos.

Con nuestro método, sacamos un listado y apuntamos, cada problema:

- Cuál fue el problema: una frase, empezado con un verbo, que describe lo que ocurrió.
- Con qué participante o participantes ocurrió.
- Qué tan importante es resolver este problema (qué *beneficio* genera): si es un problema muy grave, si ha ocurrido muchas veces, etc. Suelo usar una escala del uno al tres.
- Una posible solución.
- Cuánto costaría implementar esta solución (*costo*). Se puede usar una escala del uno al tres o una sucesión de Fibonacci, como en el desarrollo ágil de software.

Imagen 2
Listado con la priorización de los problemas de usabilidad detectados

Participante	P1	P2	P3	P4	P5	B	C	B/C
Busca a Synaptic pero no puede encontrarlo (sin contraseña de admin)						3	1	3.0
No sabe qué contraseña de admin proporcionar cuando se le pide						2	3	0.7
No encuentra nuestro documento al buscar en línea "cómo convertirse en root en Tails"						2	1	2.0
Intenta primero con "su" en vez de "sudo"						1	3	0.3
No abre el URL del archivo provisto por sudo (sin contraseña de admin)						1	1	1.0

Calculando el *beneficio/costo* podemos priorizar los problemas y arreglar los más importantes primero, optimizando así el uso de nuestros recursos para el mayor beneficio de quien lo utilice.

PASO CINCO: ARREGLAR LOS PROBLEMAS

Con este listado priorizado de problemas podemos volver a picar código para arreglarlos.

Si tienen más tiempo puedan volver a hacer más pruebas de usabilidad, más arreglos e iterar y seguir mejorando la usabilidad cada vez.

INVESTIGACIÓN DE USUARIOS Y SOFTWARE LIBRE

En esta tercera parte compartiré unas reflexiones sobre lo que llamamos *investigación de usuario*, este conjunto de prácticas sirven para entender a las personas que lo utilizan, sus problemas y sus necesidades. Pueden haber algunos roces o conflictos en la manera y la cultura que tenemos a la hora de desarrollar software libre.

LA CULTURA DE *REPORTE DE BUGS*

En el mundo del software libre es habitual depender de lo que llamamos los *reportes de bug*: informes que nos envían por listas de correo o sistemas de seguimiento de fallos (*bug tracking*), como GitHub. Pero muchas veces los desarrolladores nos quedamos a la espera de que la gente nos vaya explicando sus problemas en vez de buscar, de manera más proactiva, cuáles son estos problemas.

Creo que esto conlleva varios problemas:

1. La usabilidad también depende de problemas muy pequeños, como de vocabulario, de contraste, de problemas de posicionamiento de los elementos en la interfaz, de cosas

que la gente no necesariamente piensa en reportarnos y pueden ser muy importantes a pesar de ser pequeños.
2. Nos falta información sobre la gravedad de estos problemas. Saber de éstos no nos dice siempre cuán graves son: cuánta gente está afectada y cómo está afectada.
3. Ver los problemas en primera persona, ver a la gente pelear con el programa nos generará más empatía y más ganas de arreglarlos porque los vamos a vivir de manera más personal.

LA MINORÍA VOCAL

También tenemos que preguntarnos *quién* reporta *bugs*.

Unas 23 000 personas utilizan Tails diariamente. Si hacemos la aproximación de que una persona quizás use Tails una vez a la semana, quizás tengamos unas 150 000 con regularidad. En 2018, en nuestro *bug tracker* sólo tuvimos 32 personas activas. Esto corresponde casi a una de cada 5 000, o 0.02%. La realidad es que casi nadie de quienes usan Tails nos reportan *bugs*.

Matthew Paul Thomas (2008), en un artículo sobre usabilidad y software libre, dijo que:

> Si no se hacen pruebas de usabilidad frecuentemente, los proyectos dependen de retornos subjetivos por parte de pocas personas muy motivadas. Pero lo que éstas dicen no es necesariamente representativo del conjunto de usuarios, ni tanto solo de su propio uso.

La gente que es muy vocal en las listas y en los *bug trackers* es una minoría ínfima y tenemos que buscar maneras de conectar con la inmensa mayoría silenciosa, las 4 999 personas que no van a reportarnos *bugs*.

LA MAYORÍA SILENCIOSA

Una herramienta que nos está sirviendo en Tails para conectar con más gente es *WhisperBack*, una herramienta para informar de un error directamente desde Tails.

En el escritorio hay un lanzador que abre *WhisperBack*, donde se puede explicar qué estabas haciendo y qué problema tuviste. Además, nos enviará toda una serie de información técnica sobre el hardware, la configuración y los sucesos del sistema para que tengamos la información técnica necesaria para entender el problema.

En 2018, recibimos reportes de aproximadamente 500 personas, 15 veces más que la gente que nos está reportando *bugs*.

En la obra de Nichols y Twidale (2003), en otro análisis de la usabilidad del software libre dijeron que: reportes de incidencias integrados son muy buenos para resolver problemas de usabilidad en proyectos de código abierto. Es decir, hacer que los usuarios reporten sus problemas al momento de tenerlos durante el uso de la aplicación.

LOS *PARCHES* (NO SIEMPRE) SON BIENVENIDOS

Otro aspecto de la cultura de software libre, es que se da por entendido que somos una comunidad, que nuestro código es abierto, que todo el mundo puede contribuir, que todo el mundo puede enviarnos parches y que, si el código es bueno, lo pondremos todo en el programa. Pero si no seleccionamos los parches, las contribuciones o peticiones sin criterio de usabilidad, construiremos un programa que será más difícil de usar.

Havoc Pennington (2002), hablando en este caso del proyecto GNOME, el entorno de escritorio, escribió:

> Se le puede dar al usuario literalmente una infinidad de opciones. (*Cada uno puede pedir lo que quiere que el programa haga.*) Pero cada una de estas opciones tiene un costo de usabilidad (*porque va a ser una opción más, una decisión más que el usuario tendrá que tomar, un elemento más en la interfaz, una posibilidad más de equivocarse o dudar, etc.*) Entonces un programa con opciones infinitas es infinitamente malo. El trabajo del diseñador es seleccionar cuáles opciones son realmente útiles.

A veces es complicado decir "no" y más fácil decir que "sí" pero, una vez aceptada una opción o una funcionalidad implementada, es más difícil todavía quitarla, porque la gente la está usando, se acostumbró a ella.

Como se puede ver, todos los artículos citados tienen más de 10 años. No es nada nuevo pero la situación no ha cambiado mucho.

ANÁLISIS DE CAUSA RAÍZ

En vez de prestar tanta atención a las peticiones de esta minoría vocal, es importante pensar en cuáles son las raíces de los problemas y no siempre quedarnos con lo que la gente nos cuenta.

Por ejemplo, si soy médico y un paciente llega con un dolor de espalda y me pide ibuprofeno, quizás le tenga que decir que esa no es la solución a su dolor y ayudarle a buscar la raíz del problema.

Como metodología para este tipo de análisis, Sakichi Toyoda propone preguntarnos cinco veces ¿por qué?, para llegar a la raíz del problema.

Quizás el dolor de espalda viene de una mala postura en su

puesto de trabajo o de una posición demasiado estática. Quizás esta mala postura viene de un puesto de trabajo mal diseñado. Quizás el puesto de trabajo está mal diseñado porque nunca se hizo un análisis del impacto de su ergonomía sobre la salud y la productividad de los empleados, etc. Quizás una baja médica costosa para la empresa y una carta al responsable de las oficinas serían una mejor solución que el ibuprofeno.

OBSERVAR EN VEZ DE ESCUCHAR

En vez de escuchar al usuario, suele ser más importante *observarlo*. Jakob Nielsen, un gurú de la usabilidad, dijo de manera un poco provocativa que la primera regla de la usabilidad es no escuchar a los usuarios (Nielsen, 2001). Hay una diferencia importante entre lo que la gente *dice* y lo que la gente *hace* e incluso lo que la gente *necesita*.

A la hora de seleccionar nuestros métodos de investigación de usuarios, se hace la diferencia entre:

Las técnicas conductuales tratan de observar y de entender lo que la gente hace realmente. Ya hemos hablado de las pruebas de usabilidad y los prototipos de baja fidelidad. En cierta medida, los programas como *WhisperBack*, que permiten a quien usa un sistema reportar un problema en el momento de tenerlo, reducen la diferencia entre lo que la persona piensa y lo que dice; también nos aportan datos técnicos sobre lo que realmente pasó.

Las técnicas actitudinales tratan de lo que la gente dice y también tienen su sentido. Por ejemplo, podemos entrevistara a quienes lo utilizen para entender mejor quiénes son, en qué contexto trabajan, qué desean, etc. Así, si hacemos

encuestas para recoger datos cuantitativos, tendremos que tener en cuenta que es una técnica actitudinal y que habrá una diferencia entre lo que la gente dice y lo que realmente hace. Las listas de correo y los reportes de *bug* también nos dan información sobre lo que la gente dice más que sobre lo que realmente hace.

A MODO DE CONCLUSIÓN

Tenemos que adecuar nuestras técnicas a cada una de nuestras preguntas de investigación.

Para tener un inventario de las muchísimas técnicas que existen para la investigación de usuarios, clasificadas entre conductuales y actitudinales, cuantitativas y cualitativas, véase (Rohrer, 2014).

Por último tenemos un pequeño resumen de lo dicho hasta ahora:

No hacer	**Hacer**
Escribir el código primero, luego testear	Testear, luego escribir el código
Escuchar lo que dicen	Observar lo que las usuarias hacen
Prestar atención a la minoría vocal	Aprender de la mayoría silenciosa
Cumplir con peticiones	Entender la raíz del problema
Decir que "sí" por defecto	Aprender a decir que "no"

BIBLIOGRAFÍA

Krug, S. (2014). *Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability*. New Riders. http://gen.lib.rus.ec/book/index.php?md5=C2C1C494745E3F17A86A2F00BD8A9944

Nichols, D. y M. Twidale (2003). *The Usability of Open Source Software*. First Monday (8-1). ISSN 13960466. https://firstmonday.org/ojs/index.php/fm/article/view/1018/939.

Nielsen, J. (2001). *First Rule of Usability? Don't Listen to Users*. Nielsen Norman Group. https://www.nngroup.com/articles/first-rule-of-usability-dont-listen-to-users/.

Pennington, H. (2002). *Choosing our preferences. Blog* de Havoc Pennington. https://ometer.com/preferences.html.

Rohrer, C. (2014). *When to use which user-experience research methods.* Nielsen Norman Group. https://www.nngroup.com/articles/which-ux-research-methods/.

Snyder, C. (2003). *Paper Prototyping: The Fast and Easy Way to Design and Refine User Interfaces*. Morgan Kaufmann. http://gen.lib.rus.ec/book/index.php?md5=C42914FD52E1201FE23F46202AD709A5.

Thomas, M. P. (2008). *Why Free Software has poor usability, and how to improve it*. Computing & Internet, Usability, 1. https://web.archive.org/web/20080805012124/http://mpt.net.nz:80/archive/2008/08/01/free-software-usability.

8

AUTOCRYPT: REPENSAR EL CIFRADO DEL CORREO ELECTRÓNICO

Daniel Kahn Gillmor

Autocrypt es un protocolo para el cifrado del correo electrónico. Desde hace décadas es posible cifrar los correos electrónicos, pero su adopción ha alcanzado a muy poca gente. Incluso de quienes han aprendido en algún momento a utilizar herramientas como PGP (Zimmerman 1995), GnuPG (de Winter y Mollard, 2003) o Enigmail (Raffo *et al*., 2009), es muy poco frecuente encontrar a usuarios habituales de esta tecnología —que no es nada nueva— (la primera versión ampliamente distribuida de PGP fue publicada en 1991), y que resulta tan importante para una mínima defensa de la privacidad. Con este capítulo, buscamos presentar la problemática particular que presenta el cifrado del correo electrónico, que distingue y aparta sus casos de uso de los demás mencionados en el resto de esta obra, y exponer el razonamiento detrás de la implementación poco ortodoxa de los protocolos e incluso de las prácticas sociales tendientes a la privacidad que estamos proponiendo.

Autocrypt es un proyecto que parte de la realidad observada del manejo del correo electrónico cifrado, tomando como

meta unir la *usabilidad* (que sea un sistema fácil e intuitivo de usar, empleando apoyos visuales y flujos de trabajo simplificados), con la *seguridad*, sin sacrificar los puntos que requieren del seguimiento de parámetros estrictos.

Tradicionalmente, en programación solía decirse que usabilidad y seguridad presentaban tensiones por expresarse en sentidos opuestos, forzando al implementador a elegir entre una u otra (Whitten 1999). Pero en Autocrypt pensamos que posiblemente nuestras herramientas de seguridad, que son "muy buenas", no son utilizadas... porque no tienen buena usabilidad y sólo viendo ésta como un enfoque de seguridad podremos cambiar este modo de pensar. Queremos que la experiencia del usuario sea simple y clara, porque la gente que esperamos que use Autocrypt seguramente no serán partidarios de la criptografía ni de programación, sino entusiastas en términos de cómo queremos que opere la sociedad. Es importante entonces crear una implementación de correo cifrado que funcione para gente que no tiene el tiempo en convertirse en expertos en ingeniería, porque están usando su tiempo en convertirse en expertos en otras muchas cosas, y queremos ayudarles.

LA PRIVACIDAD ES INTERDEPENDIENTE

Comencé en este proyecto porque muchas personas hacían solicitudes como "ayúdame a hacer mis correos más seguros", mismas que se traducían como "¿quieres que te dé una sesión con la explicación para que otro día te muestre cómo ponerlo en práctica y luego vayas con tus compañeros de trabajo y les digas cómo funciona y luego puedan mandar correos seguros entre ustedes?". Porque este tipo de consultas trascienden lo personal, se traducen en "ayúdanos a proteger *nuestros* correos".

Si únicamente una persona adopta un esquema de correos cifrados, resulta inútil porque los correos son un medio de comunicación social. Pensar en cómo llevamos al grupo a adoptar el cifrado para sus correos electrónicos, cómo hacemos que todo el grupo comience a realizarlo, es una de nuestras tareas.

Una persona no puede proteger su correo sin que el resto de las personas lo haga también, porque al momento de mandar un correo, el destinatario se queda con una copia de la información que, si no protege, hace vulnerable al remitente. Desde una perspectiva mayor, si queremos una sociedad donde la gente se pueda sentirse segura, debemos reconocer que este proceso es interdependiente.

DETALLES TÉCNICOS

En cada correo enviado utilizando Autocrypt, los encabezados incluyen la llave[1] cifrada del remitente. El usuario no requiere saber cuáles son sus llaves o las de sus contactos; hay una serie de reglas sensatas acerca de cómo manejarlas, logrando una experiencia de usuario muy simple. No es una serie de reglas de programación, sino expectativas que deberían tener en cuenta todos los programas que usen el correo, para que sea más fácil para todos los usuarios.

Hablemos de la experiencia que estamos que esperando que tenga el usuario. No todos los clientes de Autocrypt lo ha-

1. Una llave criptográfica es, en el contexto de la criptografía asimétrica, un par de números muy grande (dependiendo del algoritmo utilizado, puede ser entre el rango de 2^{256} y 2^{4096}) que cumplen con una serie de propiedades que los vincula entre sí y permite emplearlos de forma única como identificadores para todas las operaciones de intercambio de información cifrada entre pares remitente-destinatario de forma segura (n. del e.).

cen. El esquema general de la experiencia del usuario completa previsto es como sigue:

1. Dar clic en "Activar Autocrypt"
2. Dar clic en "Cifrar este mensaje". De preferencia, esta opción puede estar activada por omisión.
3. El final de la experiencia del usuario es que, cuando se reciba un correo, ese cliente de correo presente un recuadro que diga "Este mensaje está cifrado".

Sencillo, ¿no? Y es que el cifrado mismo involucra toda clase de preguntas difíciles, incluso para los usuarios más técnicos. La meta es dejarlo así de simple y claro, sin preguntas que la gente no sabe contestar. Puede que aún no nos encontremos en esta fase, pero esta es la meta.

El objetivo de Autocrypt es que trabaje con las cuentas de correo ya existentes. Queremos evitar los correos cifrados que por accidente resulten ilegibles, pues sólo deberían ser ilegibles para terceros, no para quienes los intercambian. En estos casos, el destinatario tendría que escribir de regreso pidiendo su reenvío. Pero queremos evitar que los usuarios se vean en la necesidad de saber cuál es su llave; no queremos que requieran entender lo que realmente sucede detrás. Y si en verdad quieren saberlo, queremos que sea lo suficientemente claro para ellos, tanto, que cuando alguien pregunte "¿usas correo cifrado?", la respuesta sea "claro que lo hago, ¿por qué no lo haría?" Además, queremos que el esquema pueda funcionar en varios dispositivos, pues la mayoría de las personas revisa su correo desde diferentes aparatos y lugares.

Reconocemos que independientemente de la manera en la que Autocrypt está diseñada, el mecanismo de comunicación de

llaves *en banda* (*in-band key-passing* o *in-band key-exchange*, esto es, que el intercambio de llaves forme parte del mensaje mismo en vez de transmitirse por separado) es menos segura que el cifrado tradicional. No ofrecemos ninguna medida de prevención en caso de un ataque activo, que esperamos integrar en una futura versión, pero sí protegemos ante adversarios pasivos y la escucha secreta o sigilosa de conversaciones privadas, *eavesdropping*.

Una de las cosas que Autocrypt ofrece son estas ventajas fáciles. Hablamos de la alineación entre seguridad y usabilidad. De hecho, contrario al dilema anteriormente presentado, más usable *significa* más seguro. Pero esto también tiene efecto en la reducción de metadatos, una desventaja de cómo funciona el internet. Los correos cifrados producen muchos metadatos e incluso más metadatos que un correo no cifrado. Pero la claridad que tiene el usuario, la usabilidad, los pasos que sigue el cliente dan como resultado mayor seguridad.

Para ejemplificar respecto a este crecimiento de metadatos, asumamos que, empleando uno de los programas más utilizados, PGP (*pretty good privacy*), Ada y Alan quieren enviarse correos. La obligación de Ada es "adivinar" la llave de Alan. Para esto, Ada tiene que ir al servidor de llaves públicas (*keyserver*) y solicitar la llave de Alan para poder cifrar el mensaje. Alan hace lo mismo, pregunta por la llave de Ada. Esto no siempre funciona; los *keyservers* pueden mentir, tener múltiples llaves para cada persona. Podrían encontrarse físicamente o llamarse por teléfono para verificar la *huella*[2] de la llave, pero poca gente lo hace.

2. Una cadena corta, típicamente de 160 bits (40 caracteres en representación hexadecimal), generada por un algoritmo digestor o de *hash*, que representa con un alto grado de certeza a una llave criptográfica de forma que puede intercambiarse para verificación de forma mucho más sencilla que una llave completa. (n. del e.).

Esta ruta es un estándar idealizado, puesto que los mensajes pasan por unos *mail exchangers* y también se comunican con el *keyserver*, operado por un voluntario asiduo a la criptografía como uno, que podría ver que se están pasando mensaje entre ellos. Si ponemos las llaves en los encabezados, y los encabezados ya están pasando, eliminamos ese paso que involucra metadatos, y no se produce porque estamos utilizando una conexión ya establecida. Esto no necesariamente es de ayuda en presencia de servidores maliciosos que están dispuestos a moderar tus mensajes. Autocrypt no defiende a los usuarios contra un atacante activo, pero lo que no hace es ligar esta gran cantidad de metadatos a los operadores de los *keyservers* sobre quién busca conocer las llaves de quién. Esa es una pequeña ventaja que se tiene al ahorrar unas cuantas interacciones.

Hay mucho trabajo por hacer, Autocrypt no resuelve todo, y los correos son sistemas muy susceptibles de ser corrompidos, aun con este tipo de programas. Necesitamos más protección de los encabezados de los correos, más mejoras para el reenvío de los mensajes. Por ahora las máquinas interventoras de estos intercambios de correo son capaces de moderar tráfico y de ver quién habla con quién, incluso si no modifican el tráfico. Hay un trabajo interesante sobre como enviar correos a través de otro transporte que no sea el tradicional SMTP, y con Autocrypt tenemos estos encabezados de los correos como un lugar común para poner parámetros de seguridad; quizás podamos poner cosas en estos parámetros de seguridad en la misma dirección de correo, pero si quisieras cifrar correos de la forma tradicional con una llave, podrías llegar a este otro modo y tener tus intercambios de correo fuera de la jugada. Eso es parte de lo que tenemos clasificado como trabajo futuro.

Estaría bien ver más trabajo para la defensa en contra de un ataque activo, o al menos la detección de un ataque activo.

Y eso tiende a alinearse un poco con la verificación del usuario, donde se puede decir al usuario "Sí, estableciste un canal de comunicación seguro con esta persona"; cómo hacerlo concretamente es una pregunta abierta a la investigación que implica mucho trabajo, ya que también hay que hacerlo intuitivo para el usuario. Uno de los puntos fundamentales para esto es que esta forma de comunicación segura queda limitada por el número de personas que lo usan.

LA EXPERIENCIA DEL USUARIO ES TAN IMPORTANTE COMO LA CRIPTOGRAFÍA DETRÁS

Si no pensamos en la experiencia del usuario, tampoco podemos esperar que la gente pueda usarlo. En el diseño de un sistema de red como Tor se tiene una compensación de latencia: a menor latencia, menos tiempo le toma a un analizador de tráfico identificar de dónde vienen los paquetes en caso de un ataque. Esto se traduce en que Tor tiene una baja latencia, que podría comprometer al anonimato, pero esta decisión se tomó en dicho sentido para que sea un navegador veloz y, por tanto, que pueda ser utilizado por una mayor cantidad de personas. Si hubiera mayor latencia, comprometería menos al anonimato, pero nadie lo utilizaría por la baja velocidad y su alta latencia. Y la poca gente dispuesta a utilizarlo no tendría con quien mezclar sus datos de todas maneras. Algo similar pasa con Autocrypt: el cifrar correos de forma tradicional tiene una complejidad mayor y, por lo tanto, es más seguro. Sin embargo, esta mayor complejidad hace que sea menos utilizado, y esto conlleva a un peor rendimiento al considerar la seguridad total. Como en este proyecto escogemos algo más fácil de utilizar, el resultado es una mayor cantidad de correos cifrados circulando por la red. Entonces, la compensación

total no queda únicamente en la teoría, sino que interactúa a nivel del ecosistema de la gente que lo utiliza.

Por último, Autocrypt no solamente se concentra en la teoría de mandar correos cifrados, se preocupa también por la experiencia del usuario: cuál es la interacción que ocurre como resultado del proceso criptográfico. Si no se piensa en los pasos finales de la interacción de un proyecto con el usuario, seguramente éste no va a tener el efecto del modo esperado.

BIBLIOGRAFÍA

De Winter, B., y M. F. V. Mollard (2003). *Gnu Privacy Guard (GnuPG) Mini Howto*. Consultado en: http://www.gnupg.org/documentation/howtos.en.html (2020.09.02).

Raffo, D.; R. J. Hansen, y P. Brunschwig (2009). *The Enigmail handbook*. Consultado en: https://www.enigmail.net/documentation/Enigmail_Handbook_1.0.0.pdf (2020.09.02).

Speer, R., y D. Christoforo (2004). Part 1: Enigmail for the Common Man.

Whitten, A., y J. D. Tygar (1999). "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0". *USENIX Security Symposium* (Vol. 348, pp. 169-184).

Zimmermann, P. R. (1995). *The official PGP user's guide*. Cambridge, MIT Press.

TERCERA PARTE

TERRITORIOS/CONTEXTOS

9
LA RED TOR EN MÉXICO

Juan Jacobo Nájera

En 2016, un grupo de investigadores independientes, estudiantes y organizaciones de la sociedad civil, vinculado a los derechos humanos y al software libre, se preguntó cuál era la participación de América Latina, y en particular de México, en la red Tor, tanto en su demografía de usuarios como con infraestructura y desarrollo de la misma, de cara a documentar y enfrentar los principales factores que impiden una mayor participación. Estábamos vinculados con el proyecto Mecanismos de privacidad y anonimato de la UNAM (Pérez-Gómez, 2017) y esa pregunta era parte de las líneas de trabajo, la realización de tareas encaminadas a facilitar la participación en el desarrollo de la red Tor desde México, mientras que la otra se centraba en la divulgación de las herramientas enfocadas en la privacidad y el anonimato en el contexto de la enseñanza a nivel superior.

El punto de inicio del trabajo en este artículo es comprender el estado preexistente de la participación en la red Tor en nuestro país, tanto por usuarios finales como por voluntarios que quieran agregar recursos a la red. Participar con más nodos en

la red resulta necesario para asegurar una máxima *dilución* del tráfico de cada uno de los usuarios, para poder asegurar el anonimato que Tor ofrece. Al inicio de nuestro trabajo, había reportes sin organizar ni sistematizar con dificultad para participar en Tor de nuestro país, y el objetivo fue comprender y contribuir a solucionar dicha situación.

De inicio, y para contextualizar, las principales formas de conectividad en México son: ADSL, internet por cable, fibra óptica, redes de telefonía móvil y conexión vía satélite. Con el acceso a internet en los hogares de 50.9% según la International Telecommunications Union (2017).

Sobre Tor: en México, en 2018, eran poco más de 12 000 usuarios de un total de 3 millones de usuarios totales por año (Alcántar, Nájera y Argüelles, 2019), y para 2020, el trabajo preliminar apunta a que la participación creció aproximadamente a 15 000 usuarios de cerca de 4 millones de usuarios totales. Es de gran interés para el grupo de trabajo saber cuál es la participación activa en la construcción de la infraestructura de la red desde el país, es decir, conocer cuántos nodos, del promedio de los 6 000 que conforman la red Tor (Tor Project, 2009-2018) están distribuidos geográficamente en México.

La red Tor contaba con 6 000 nodos en 2018, donde cada nodo tiene diferentes funciones. Desde la perspectiva de su arquitectura, la red tiene 11 autoridades centrales, y la gran mayoría de los servidores conectados actúan como nodos repetidores (*relays*), mismos que de acuerdo a su configuración y características técnicas pueden ser de cuatro tipos: puentes, entrada, intermedio y salida (Learmonth, 2019). En ese momento se encontraron un par de nodos intermedios y de entrada, y ninguno de salida. Cifra que visibiliza una participación de 0.03 % de México, de 1.5% de nodos que aporta América Latina al total. Estas

cifras tremendamente bajas de participación, tanto en las y los usuarios como en la operación de nodos en perspectiva en toda la región latinoamericana y caribeña.

Los datos permitieron plantear preguntas sobre los motivos o explicaciones de esos bajos niveles, y también sobre el papel actual y potencial que tiene una arquitectura de red con estas características, para buscar formas de incentivar el crecimiento o fortalecimiento de esta red de anonimato (Alcántar, Nájera y Argüelles, 2018).

OPERADORES Y LIMITACIONES

Encontramos dos obstáculos para la plena participación de espacios de investigación y de la ciudadanía en la red para el ejercicio del derecho al anonimato en internet: costo y limitaciones técnicas (bloqueo de direcciones IP e implementación de NAT), que se describirán a continuación. Y aunque hay disposición e interés de personas y colectivos en convertirse en operadores, en muchos casos no es posible que encuentren o contraten otro proveedor para sortear estos problemas:

- *Costo.* Es importante señalar un fenómeno con los operadores de nodos, México cuenta con ellos, pero con infraestructura en otros países. Cuando se indagaba a los operadores sobre los motivos para tener la infraestructura en otros países y no en México, la respuesta fue que lo hacían por motivos de costo. Algunos de los operadores suelen rentar servidores virtuales en servicios de otros países, y ahí instalar el software para operar sus nodos. Esto, por una parte, indica interés en la participación para la construcción de la infraestructura de la red, pero con

limitaciones contextuales, más precisamente el costo, según los testimonios de los operadores.

- *Limitaciones técnica*s. Los proveedores de telecomunicaciones en México ponen dos limitantes para la instalación de nodos que puedan ser parte de la red Tor:

El bloqueo por parte del operador preponderante, Telmex, de 9 de 11 de las direcciones IP que pertenecen a los nodos directorio de la red Tor, lo que en consecuencia no permite la sincronización de los nodos y, por lo tanto, no es posible la instalación. El proyecto Mecanismos de Privacidad y Anonimato comenzó con un llamado para realizar un censo que permitió hasta el momento tener hallazgos preliminares de las limitaciones generales que hay en los proveedores mexicanos. Detectamos con ello el bloqueo a nivel ruta de las siguientes direcciones IP (correspondientes a las autoridades de directorio de la red Tor) en la red de Telmex (Wolf, 2019):

- 171.25.193.9
- 86.59.21.38
- 199.58.81.140
- 194.109.206.212
- 131.188.40.189
- 128.31.0.34
- 193.23.244.244
- 154.35.175.225
- 128.31.0.39

La implementación de técnicas de asignación de direcciones IP por NAT es una práctica en la que el proveedor de telecomunicaciones asigna una dirección IP real u homologada a varios

de sus clientes o abonados (Srisuresh y Egevang, 2001), en algunos de los casos llegando a una sobresubscripción de decenas de miles de equipos por dirección (FancierGull, 2018), que no permite que el nodo pueda tener una dirección pública única asignada al mismo. En definición del Network Working Group, NAT es "un método por el que muchas direcciones de red y sus puertos TCP/UDP (Protocolo de Control de Transmisión/Protocolo de Datagrama de Usuario) son traducidos a una sola dirección de red y sus puertos TCP/UDP". Uno de los argumentos que muestran los proveedores de conectividad para la utilización de NAT en la gestión de su red es como medida para hacer frente al agotamiento de direcciones IPv4, como método de racionalización de los recursos disponibles.

LIMITACIONES LEGALES E INTERMEDIARIOS

En los casos en los que se logran sortear las limitaciones técnicas, surgen las legales como una de las inquietudes más comunes cuando una persona está interesada en la instalación de un nodo. En México la operación es legal,

> bajo el entendido que un nodo de la red Tor no es un concesionario de internet o un proveedor de interconexión pública, sino una conexión privada gratuita que la persona usuaria acepta al momento de acceder a la red Tor, la cual se realiza en el ejercicio de los derechos y libertades de privacidad, acceso a internet, intercambio de información, libertad de expresión y manifestación de ideas que otorgan el artículo 6° constitucional y el artículo 191, fracción XV de la Ley Federal de Telecomunicaciones y Radiodifusión", (Enjambre Digital, 2017).

Como lo recoge Enjambre Digital, una de las organizaciones participantes del proyecto de Mecanismos de Privacidad y Anonimato

Los servicios en internet son parte de lo que en la jerga de las regulaciones de telecomunicaciones se llaman *intermediarios*. En esa dirección, la discusión que se ha dado en torno a las responsabilidades que tiene un intermediario, y en especial un servicio que funciona sobre internet como lo puede ser un sitio web, correo electrónico, entre otros, son de carácter vigente y pueden variar al estar ligadas a la etnografía de las regulaciones.

Desde organizaciones de la sociedad civil se ve reflejado en los llamados Principios de Manila sobre Responsabilidad de Intermediarios (2015). Uno de los eslabones detrás de los principios es el entendido que el conjunto de prácticas, regulaciones y la responsabilidad de los intermediarios tienen una vinculación y efecto en el ejercicio de los derechos humanos de quienes usan las plataformas de internet, como lo es la libertad de expresión, asociación y la privacidad.

Con estos principios busca contribuir al desarrollo de marcos de responsabilidad de intermediarios "que puedan promover la innovación y, a la vez, respeten los derechos de los usuarios consagrados en la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y los Principios Rectores de Naciones Unidas sobre las Empresas y los Derechos Humanos"

Estos seis principios consideran:

1. Los intermediarios deberían estar protegidos por ley de la responsabilidad por contenido de terceros.
2. No debe requerirse la restricción de contenidos sin una orden emitida por una autoridad judicial.

3. Las solicitudes de restricción de contenidos deben ser claras, inequívocas y respetar el debido proceso.
4. Las leyes, órdenes y prácticas de restricción de contenidos deben cumplir con los tests de necesidad y proporcionalidad.
5. Las leyes, políticas y prácticas de restricción de contenido deben respetar el debido proceso.
6. La transparencia y la rendición de cuentas deben ser incluidas en la normativa, políticas y prácticas sobre restricción de contenido.

Estos principios cuentan con especificidades y criterios que los acompañan y que pueden ser consultados en línea. Sin embargo, el motivo de incluir estos principios es compartir parte de uno de los marcos que destacan desde la sociedad civil como ejercicio de discusión informado actual de las políticas públicas y regulaciones de los intermediarios de internet.

Una vez realizada parte de la revisión del contexto de algunas de las discusiones vinculadas a los intermediarios y el papel que pueden tener sus políticas, desde la perspectiva de organizaciones de la sociedad civil que trabajan los derechos digitales, y concluir que el marco normativo legal en México es compatible con la operación de nodos de la red Tor.

Usualmente, los nodos más propensos a recibir requerimientos legales son aquellos que están configurados para ser nodos de salida. Esto se debe a que son el último contacto entre la red Tor y otras redes de internet. Para ello, hay prácticas recomendadas para la operación de este tipo de nodos.

En México, la organización que se encargó del desarrollo y análisis de las normativas, que arribaron en el diseño de un aviso legal, fue Enjambre Digital (2017). Este aviso legal tiene dos

pilares, el primero es el anclaje de la declaratoria de responsabilidad desde la arquitectura propia de la red Tor sobre posibles requerimientos de información por autoridades:

> La responsabilidad respecto a los sitios finales visitados corresponde únicamente a quienes hacen uso de internet. Como parte intrínseca del proceso para preservar el anonimato, este nodo no conserva clase alguna de registro sobre: páginas visitadas, medios de conexión, paquetes de datos que cruzan por él o algún otro dato que pueda identificar a las personas que lo utilizan.

El segundo pilar del aviso es el fundamento legal sobre el ejercicio de derecho a la privacidad, acceso a internet, intercambio de información y libertad de expresión que otorga el artículo 6° constitucional y el artículo 191 fracción XV de la Ley Federal de Telecomunicaciones y Radiodifusión en México.

Finalmente, tras los esfuerzos de los diversos actores involucrados que convergieron en el proyecto de Mecanismos de Privacidad y Anonimato de la Universidad Nacional Autónoma de México se logra el incremento de la participación en la operación de ocho nodos más, incluyendo uno de salida (Wolf, 2019b).

CONCLUSIONES

Lo antes expuesto nos permite concluir que la participación de los y las interesadas en la operación de nodos de la red Tor presentan dificultades por las características técnicas de los mayores proveedores de acceso a internet por el bloqueo de las ocho direcciones IP, y en otros casos por la arquitectura de proveedores que implementan redes sobre NAT. No obstante, se reconocen

los esfuerzos multidisciplinarios para sortear las limitaciones técnicas y políticas y lograr un incremento en la participación de México en la red Tor. En un contexto que se observa con tendencia restrictiva.

Uno de los pasos siguientes es la exploración de los marcos regulatorios que atiendan en diferentes dimensiones, entre ellos de competencia, neutralidad de la red y libertad de expresión y derechos de los consumidores, para así lograr una plena participación de quienes voluntariamente desean contribuir con su infraestructura existente al funcionamiento de la red Tor.

BIBLIOGRAFÍA

Alcántar, S.; Nájera, J., y Argüelles, A. (2018). Colabora en la documentación de las barreras para el despliegue de la red Tor en México. Disponible en https://tor.enjambre.net/convocatoria/ (2020-09-01)

_____ (2019). La Internet anónima: Tor en México. Disponible en https://tor.enjambre.net/ (2020-09-01)

Enjambre Digital (2017). Aviso legal para nodos de salida en México. Disponible en https://www.enjambre.net/tor-mx/ (2020-09-01)

FancierGull (2018). AT&T Internet en casa Tipo de NAT. Consultado en https://forums.att.com/t5/Servicios/AT-amp-T-Internet-en-casa-Tipo-de-NAT/td-p/5508834 (2020-09-01)

International Telecommunication Union (2017). ICT Data Portal: Mexico profile. Consultado en https://www.itu.int/net4/itu-d/icteye/#/countries (2020.09.01)

Learmonth, I. R. (2019). "Privacy-preserving monitoring of an anonymity network", *Free and Open Source Developer's European Meeting 2019 (FOSDEM 2019).* Consultado en https://iain.learmonth.me/content/talks/2019/2019-02-fosdem.pdf

Perez-Gómez, Aurelio (2017). "Mecanismos de privacidad y anonimato en

redes: LIDSOL crea proyecto multidisciplinario para protección de derecho en la red", *Portal de Comunicación de la Facultad de Ingeniería*. Consultado en: http://www.comunicacionfi.unam.mx/mostrar_nota.php?id_noticia=1060 (2020-09-01)

Principios de Manila sobre Responsabilidad de los Intermediarios (2015). Guía de Buenas Prácticas que Delimitan la Responsabilidad de los Intermediarios de Contenidos en la Promoción de la Libertad de Expresión e Innovación. v.1.0. Consultado en: https://www.eff.org/files/2015/06/23/manila_principles_1.0_es.pdf (2020-09-01)

Srisuresh, P. y K. Egevang (2001). "Traductor de Dirección de Red IP Tradicional (NAT Tradicional)". *Grupo de Traducción al castellano de RFC*. Consultado en: https://www.rfc-es.org/rfc/rfc3022-es.txt (2020.09.01)

Tor Project (2009–2018). Tor Metrics — Servers. Consultado en https://metrics.torproject.org/networksize.html (2020-09-01)

Wolf, G. (2019). "Distributed Detection of Tor Directory Authorities Censorship in Mexico". *The Eighteenth International Conference on Networks ICN2019* (82–86). Consultado en https://www.thinkmind.org/download_full.php?instance=ICN+2019 (2020-09-01)

_____ (2019b). *Finally, a sensible increase in participation for Tor in Mexico*. Consultado en https://gwolf.org/2019/01/finally-a-sensible-increase-in-participation-for-tor-in-mexico.html (2020-09-01).

10

MONITOREO, CENSURA DE INTERNET, CASOS DE CIBERVIGILANCIA Y ACOSO DIGITAL EN CENTROAMÉRICA

Norman García

La región centroamericana cuenta con conocidas historias de gobiernos represivos y empresas multinacionales con gran poder económico que se han visto involucradas en violaciones a derechos humanos. Tomando en cuenta esto y el bajo desarrollo económico que existe, se podría pensar que los tipos de violencias o fuerzas ejercidas en contra de organizaciones sociales y ciudadanía en general no ha llegado al plano digital debido al alto costo que puede conllevar la adquisición de herramientas digitales de vigilancia masiva y de monitoreo de comunicaciones o que posiblemente esto se ha dado en pequeñas escalas.

Con la compilación de información que se presenta aquí, se pretende demostrar que los gobiernos de la región sí han invertido en mejorar sus capacidades técnicas en materia de vigilancia y monitoreo en internet, que esto ha venido pasando desde hace unos años y que se ha dado a distintos niveles, desde monitoreo en redes sociales hasta la adquisición de software especializado de análisis de tráfico y control absoluto sobre los proveedores de internet.

Aquí se muestra una recopilación de casos documentados de cibervigilancia y espionaje digital perpetrados en la región centroamericana contra organizaciones civiles y personas defensoras de derechos humanos (DH), no obstante, no pretende ser un instrumento de investigación *per se*.

Hay diversos estudios e investigaciones en la región, pero no se ha encontrado un documento que haga un compendio de éstos. Tomando en cuenta la estrecha relación que existe entre organizaciones sociales y personas defensoras de DH en la región, es importante articular esfuerzos para desarrollar indagaciones en conjunto y difundir estos casos.

La información que se presenta a continuación ha sido obtenida de investigaciones y recolecciones de datos que organizaciones sociales y personas naturales han realizado en esta materia con el fin de registrar los distintos casos que se han dado en los últimos años. A pesar de ello, son pocas las investigaciones que documenten, con pruebas, la existencia de sistemas de monitoreo por parte de los gobiernos hacia sus ciudadanos. A continuación, se comentarán algunos de estos estudios y otras investigaciones que se han realizado para monitorear la censura de internet y la digital en la región centroamericana.

Osorio (2018) dice que el derecho a la privacidad se considera, tanto en el artículo 12 de la Declaración Universal de Derechos Humanos a nivel internacional como en el artículo 11 de la Convención Americana de Derechos Humanos (Pacto de San José) e igualmente en cada país de Centroamérica existen normativas dentro de sus constituciones políticas que protegen la privacidad de las comunicaciones de la ciudadanía. Sin embargo, como se mencionó al inicio, el desarrollo de las tecnologías en la región y el actuar documentado de los gobiernos y sus autoridades han demostrado que estas normativas no son respetadas.

ANÁLISIS DE CASOS EN LA REGIÓN

Bonifaz (2018) afirma que, según el Transparency Toolkit y Privacy International —proyecto que utiliza datos abiertos para mapear información de compra de software de monitoreo por parte de agencias de vigilancia—, se ha hecho uso de herramientas como FinFisher en Panamá; Bluecoat en Nicaragua, Guatemala y Costa Rica; HackingTeam en Honduras y Panamá; EXFO, GammaInternational y NSO en Panamá y de software aún desconocido en El Salvador.

Esto muestra claramente que los gobiernos y sus agencias en Centroamérica sí han invertido en la adquisición de software de monitoreo. Se desconoce el uso que le estén dando a estas herramientas.

INFORME DE FUNDACIÓN ACCESO

Fundación Acceso publica, desde hace un par de años, un informe anual donde se documentan incidentes de seguridad digital a personas defensoras de derechos humanos. En el de 2018, se muestra que: En Guatemala se han sufrido ataques de acoso por parte de netcenters, éstos han sido "hackeos" a cuentas de redes sociales, amenazas directas hacia personas defensoras de DH, ataques de Phishing a cuentas de iCloud y cambios de contraseñas de Gmail. Las direcciones de IP desde donde se hicieron estos ataques están dedicadas a eso. Otro incidente fue un Phishing a través de un enlace de invitación a un grupo de Facebook.

Para Nicaragua, el reporte anual documenta casos de robo de Hardware a organizaciones de sociedad civil, que podría analizarse como algo común pero que se da en un contexto de asedio

y persecución a estas organizaciones. Estos casos de pérdida de hardware abrieron la puerta a robo de cuentas de redes sociales de activistas, debido a que contaban con sus cuentas abiertas en computadora o celular.

Casos de bloqueo de cuentas de Facebook o Twitter a través de cuentas progobierno, en netcenters, que realizan denuncias masivas a perfiles de redes sociales donde se hacen denuncias de violaciones a DH.

EL OBSERVATORIO DE NETBLOCKS

NetBlocks es un grupo de la sociedad civil que trabaja en defensa de los derechos digitales, gobernanza de internet y ciberseguridad y tiene un observatorio de bloqueos en internet que detectó interrupción de éste en ciertas regiones de Nicaragua.[1] Dichas interrupciones coincidieron con momentos en que se producían ataques a población civil ubicada en los "tranques" (barricada popular). Durante estos ataques en ciudades como León, Masaya, Matagalpa, Jinotega, entre otros, las personas mediante redes sociales reportaban una interrupción parcial de internet y de señal de telefonía celular, particularmente de la empresa Claro Nicaragua. Cabe mencionar que dicha compañía desmintió, a través de un comunicado, que hayan interrumpido el servicio de manera intencional y lo atribuyó a problemas técnicos que se dieron justo en el momento de los ataques y que sus cuadrillas de reparación no podían ingresar por lo hostil de la zona.

Todo esto en el contexto político de abril de 2018, donde Nicaragua sufre una crisis severa de violación de los derechos humanos y, al inicio de esta crisis, la población instaló barricadas en algunas

1. https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9.

ciudades y en las principales carreteras del país con el objetivo de paralizar el libre tránsito como una medida de defensa de estas violaciones y agresiones que el gobierno estaba realizando. Durante julio de 2018, la Policía Nacional de Nicaragua en conjunto con paramilitares, decidió iniciar un plan llamado "Operación limpieza",[2] en el que se daban enfrentamientos armados para sacar a la ciudadanía de estos "tranques" y habilitar la circulación.

ATAQUES DOCUMENTADOS DE "ASUNTOS DEL SUR"

De igual manera, "Asuntos del Sur" —organización dedicada a diseñar e implementar innovaciones políticas para desarrollar democracias paritarias, inclusivas y participativas—, en 2018 realizó una investigación enfocada en Nicaragua, en la que se hizo un análisis sobre incidentes digitales sufridos en el país. Se puede observar que, durante los primeros momentos de la crisis sociopolítica en el país, se documentaron casos de ataques de denegación de servicio, el cual es un ataque que puede impedir que un sitio web sea accesible en internet. Los ataques fueron dirigidos a medios de comunicación escrita de circulación nacional como *La Prensa* y *Confidencial*. También se reportó un ataque al medio independiente en línea BacanalNica.

Entidades del gobierno también notificaron ataques a sus sitios webs y fueron anunciados por el grupo AnonymousNicaragua, el cual estuvo anunciando numerosos ataques a infraestructura gubernamental. Entre los sitios webs atacados se encontra-

2. En junio y julio de 2018 el régimen Ortega-Murillo ejecutó una serie de violentos ataques para desmontar los tranques en las principales ciudades del país. Fueron 43 días de horror. Así se realizó la "Operación limpieza". Tomado de *La Prensa* en: https://www.laprensa.com.ni/2019/06/15/suplemento/la-prensa-domingo/2560191-operacion-limpieza-la-masacre-de-daniel-ortega.

ron: Poder Legislativo, Policía Nacional, Canal 6, Aeronáutica Civil, entre otros.

La investigación también documenta reportes de acceso no autorizados a cuentas de redes sociales de periodistas nicaragüenses y, según comentarios de las personas entrevistadas, observaron comportamiento inusual en sus cuentas (León, 2019).

Otro caso interesante, documentado por "Asuntos del Sur", fue el sufrido por clientes de internet residencial de Claro Nicaragua en todo el país, quienes a inicios de junio reportaron un comportamiento inusual en su red inalámbrica casera. Al iniciar la mañana, notaron que el identificador de su red WiFi (SSID) había sido cambiado a "QUITEN LOS TRANQUES" y la seguridad de ésta había sido anulada. Este nombre de SSID hacía referencia a las barricadas que se habían instalado en varias carreteras principales y distintos puntos de ciudades en Nicaragua. Hubo una gran manifestación de reclamo en redes sociales hacia la empresa, pero esta emitió un comunicado público en el que aducía que se trataba de un incidente externo y que estaban trabajando con sus proveedores para solventarlo. Los clientes del internet nunca recibieron mayor aclaración de la causa de este incidente que alarmó a toda la población, pues con el hermetismo con el que se gestionó el incidente se demostraba la poca seguridad que esta compañía brinda a sus clientes o que bien se pudo deber a un ataque interno.

ACCESS NOW: CENSURA Y ACOSO

Por otro lado, también encontramos reportes de parte de Access Now, organización internacional que tiene como objetivo defender los derechos digitales de personas usuarias en riesgo. Para apoyar a la región centroamericana, se cuenta con una línea de

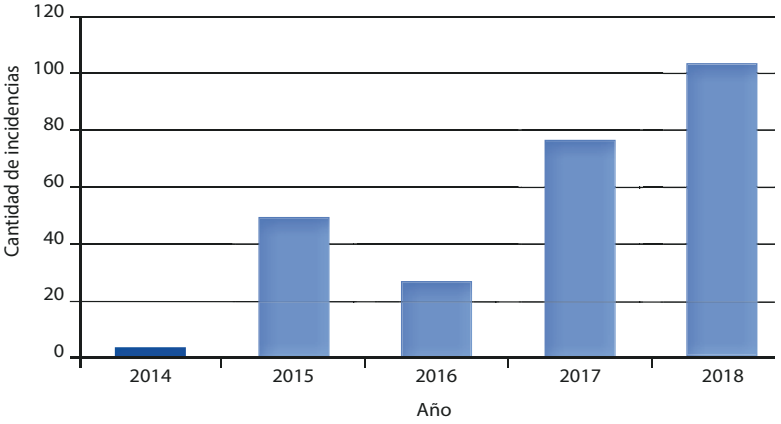
ayuda a la que cualquier persona de la sociedad civil que sienta riesgo digital puede comunicarse y solicitar soporte técnico.

Desde el año 2014, se reportan a través de su línea de ayuda un total de 262 incidentes de seguridad digital, siendo Nicaragua el que más ha reportado con 118, seguidos de Costa Rica con 65 casos, Honduras con 27, Guatemala con 21, Panamá con 17 y, finalmente, El Salvador con 14.

En el periodo comprendido entre 2017 y 2018, se reportan 31 casos a los que se brindó soporte de seguridad a cuentas de redes sociales, que tiene relación con 27 incidentes reportados donde cuentas de redes sociales se vieron comprometidas.

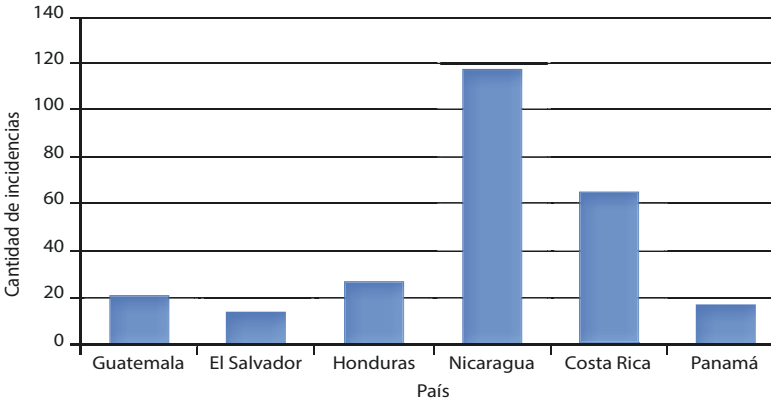
Dentro de su reporte, se pueden mencionar casos de censura (19) y acoso digital (17), cabe mencionar que los casos de censura hacen referencia, en su mayoría, a cierre de páginas de Facebook que se dieron por reportes masivos de abuso en la plataforma de la mencionada red social y por acceso no autorizado a cuentas administradoras de páginas y una vez conseguido el acceso,

Imagen 1
Incidentes de seguridad digital por año en Centroamérica



Fuente: Elaboración a partir de datos proporcionados por Access Now.

Imagen 2
Incidentes de seguridad digital entre 2014 y 2018 en Centroamérica por país



Fuente: Elaboración a partir de datos proporcionados por Access Now.

las personas perpetradoras procedieron a eliminar las páginas, lo que demuestra que estos casos de censura tienen estrecha relación con los casos reportados de compromiso de cuentas.

CONCLUSIONES

Centroamérica cuenta con organizaciones defensoras de la privacidad y de los derechos digitales que realizan estudios/investigaciones sobre monitoreo y censura en internet, pero aún faltan más recursos técnicos y humanos para poder llevar estas investigaciones a nivel de análisis forense. Es necesario que estas investigaciones lleguen a un nivel técnico más avanzado y esto se demuestra por las inversiones que han realizado los gobiernos de la región para la adquisición de software de espionaje.

Se considera importante la articulación entre las distintas organizaciones sociales defensoras de los derechos digitales en

la región, ya que esto aumentará la línea defensiva lo cual es muy necesario ante los ataques que se han documentado.

Un plan en conjunto para promover la ciberseguridad a nivel regional podría ser considerado de gran ayuda para concientizar a la población en general sobre la importancia de aplicar medidas básicas de seguridad y para reconocer de manera más eficiente un ciberataque.

Las investigaciones recopiladas en este documento dejan en evidencia la capacidad de cibervigilancia con la que cuentan los gobiernos a través de terceros que comercializan este tipo de tecnología, así como la capacidad de los gobiernos de instalar recurso humano en netcenters para realizar ataques en redes sociales, por lo que sería un error asumir que debido al poco desarrollo de la región no haya cibervigilancia, espionaje y monitoreo de internet.

Dicho esto, las organizaciones en defensa de los derechos digitales, de privacidad y anonimato, de los derechos humanos deberían de articular fuerzas y de sociedad civil para realizar investigaciones a profundidad sobre análisis de tráfico en internet, como los realizados por el Citizen Lab de la Unviersidad de Toronto o el Proyecto Netblocks.

También se debe de tomar en cuenta proyectos como la implementación de un laboratorio para análisis de malware en teléfonos de activistas de la región.

Otra cosa importante que se debe de realizar, es llevar a cabo un proyecto de análisis de antenas de celular falsas que puedan estar siendo usadas para monitorear las comunicaciones de la ciudadanía. Esto es algo que, según lo investigando en la región no existen investigaciones que puedan descartar esto y con la información encontrada, se puede asumir que esto podría ser una posibilidad.

Una campaña regional para realizar concientización en la ciudadanía sobre la seguridad digital y sobre ingeniería social, ayudaría a educar y evitar futuros ataques de scam o phishing a través de los cuales podrían lograr llevar a cabo ataques digitales.

BIBLIOGRAFÍA

Artículo 12 (n.d.). Disponible en https://dudh.es/12/.

Montero, F. J. (n.d.). Disponible en https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Osorio, José (Guatemala, 2018). Privacidad y vigilancia. Marco de regulación en Centroamérica. [archivo PDF]. Charla presencial entregada en dicho formato.

Access Now (Guatemala, 2018). Encuentro de la Comunidad de Seguridad Digital en Centroamérica [archivo PDF]. Charla presencial entregada en dicho formato.

Bonifaz, R., y J. A. Delgado-Ron (2018). "Casos verificados de uso ilegítimo de software de vigilancia por parte de gobiernos de América Latina 2015-2016", *Revista PUCE* (106), 315–333. Disponible en http://www.revistapuce.edu.ec/index.php/revpuce/article/view/142.

Fundación Acceso (2018). Observatorio Centroamericano de Seguridad Digital, *Informe anual* 2018. Disponible en https://acceso.or.cr/assets/files/Informe_OSD_2018_espan%CC%83ol.pdf.

León, C. (2019, March 19). *Construyendo resiliencia digital con activistas en Nicaragua*. Disponible en https://asuntosdelsur.org/construyendo-resiliencia-digital-con-activistas-en-nicaragua/.

NetBlocks (2019). *Regional internet disruptions in Nicaragua amid protests*. Disponible en https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9.

11
ASPECTOS LEGALES DEL ANONIMATO EN LAS COMUNICACIONES

Jesús Robles
(Enjambre Digital)*

Conforme más pasa el tiempo, me siento más anarquista y más radical en defender la libertad. Como decía Saramago, mientras más viejo, más libre. La que he ido perdiendo en el Estado, la deposité en las personas y la libertad. Y es que nuestra tarea es la de crear más libertades, no la de pensar por las autoridades. Lo digo como provocación: no creo que nuestra tarea sea pensar cómo restringir nuestras libertades para que las autoridades puedan perseguir delitos, y menos, teniendo las autoridades que tenemos; no me enfocaría en darles más poder para que restrinjan nuestras posibilidades de anonimato.

Hay un principio de derecho fundamental que me gusta mucho, porque creo que es también un principio del anarquismo: la autoridad solo puede hacer lo que le está permitido y los ciuda-

* Nota del editor: este último capítulo se presenta como una transcripción de la participación del autor en nuestro coloquio, y el lector podrá apreciar que tiene un tono mucho más coloquial que todos los demás. Consideramos que las experiencias que narra el autor, conocido abogado y defensor de derechos humanos en México, con amplia experiencia en los temas nodales que perseguimos, ilustran de manera excelente los retos legales y extra-legales de la protección a las comunicaciones que respeten la privacidad y el anonimato en el México de inicios del siglo XXI.

danos podemos hacer todo lo que no está prohibido ¿cierto? A esto hay que sumar dos ideas que parecieran ancestrales: que el Estado es un mal necesario y que solo éste puede hacer lo que le esté permitido. Basta platicar con cualquier abogado para saber, con evidencias, que esta última máxima se rompe.

Y es que el Estado continuamente recurre a cosas que no le están permitidas hacer y se salta sus propias normas. En México, por ejemplo, los abusos militares durante la guerra contra el narco —que mucha gente defiende diciendo cosas como "¿querían que los trataran con toallitas o pétalos de rosa?". No, lo que quisiera es que no los mataran ni los ejecutarán, y definitivamente no los estén tratando con pétalos de rosa. Sabemos que cuando la Secretaría de la Defensa se entera de algún delito claramente documentado, puede usar estándares de seguridad nacional, justificaciones legales amplias y capacidades técnicas para intervenir, vigilar y romper algunos tipos de comunicaciones cifradas o privadas. Por eso, necesitamos el apoyo de la comunidad técnica para aumentar el ámbito de las libertades de nuestras comunicaciones, más en el contexto autoritario en que vivimos que por más que queramos y como cree AMLO —mi cabecita de algodón— no va a terminar con el cambio de gobierno el primero de diciembre (2019). Las funciones autoritarias siempre estarán en el gobierno, en todos los gobiernos, en su mismo gobierno, y no veo ningún otro camino responsable para la sociedad que afirmar la libertad.

Hace cinco años viví un ejemplo de cómo las funciones autoritarias han ido creciendo. Hablo del caso de un *anonymous* chiapaneco que defendimos en la organización Enjambre Digital.[1] En ese tiempo estábamos promoviendo diversos derechos

1. Por ejemplo, véase la nota: "Acusan de narcomenudista a miembro de #Anonymous crítico del gobierno chiapaneco", en www.tolucanoticias.com/2013/08/acusan-de-narcomenudista-miembro-de.html.

en internet y vimos la noticia de un videobloguero que había sido detenido en Chiapas por publicar videos que daban cuenta de la corrupción en el Estado, bajo el gobierno de Manuel Velasco, político "chapulín" ahora cobijado, tristemente, por Morena como senador. Muy al principio de su gobierno había un denunciante, un soplón muy bueno y sofisticado en Twitter. Publicaba información muy buena, de vigilancia qué Velasco usaría. Este informante fue retomado por nuestro activista anónimo, menos sofisticado, que subía videos en YouTube y soltó esta noticia, causando revuelo. Ya el informante había alertado sobre tener cuidado, porque estos equipos iban a ser usados contra los opositores. Por otra parte, alguien con muy poca capacidad de análisis le dijo a Manuel Velasco que "El Informante" de Twitter seguramente era el mismo que hacía los videos.

Pronto las autoridades fueron por él, pero como no podían imputarlo como soplón, esperaron a que saliera de su casa para apresarlo y le "sembraron" droga. Obviamente, aunque el videobloguero usó técnicas básicas de anonimato, como esconder en su perfil de YouTube el nombre real de su cuenta, la propia plataforma exige cierta identificación. Cuando vimos el expediente judicial resultó fascinante: decía que habían estado patrullando una zona y que, de pronto, frente al café internet de este joven, el dispositivo GT-200 se había alocado, revelando que ahí estaba la cocaína que buscaban y entonces esperaron a que saliera. Para los que no sepan, el GT-200[2] era un engaño: una cosa parecida a una botella de pet con dos antenas y foquitos que, supuestamente, detectaba armas, droga y todo lo malo (yo creo que hasta pecados, debo decir que durante una operación con este aparato, me desnudaron, pero esa es otra historia).

2. La Wikipedia en inglés tiene una entrada sobre el GT-200 que incluye un apartado sobre su uso por el gobierno mexicano: https://en.wikipedia.org/wiki/GT200#Mexico_2.

Luis Mochán,[3] físico de la UNAM, estudió científicamente el caso y descubrió que ese aparato era un fraude que costaba millones de dólares (en 2010, se calculó que diferentes instancias mexicanas, en su mayoría la Sedena, habían comprado en total unos 940 aparatos por cerca de 26 millones de dólares). Tiempo después testificó en las cortes de Inglaterra en una condena al creador de este embuste (Gary Bolton), que se seguía adquiriendo en Chiapas. Con todo y esto, en Chiapas había gente en la cárcel y cuando fuimos de mi organización a dar una conferencia sobre el GT-200, porque había detectado droga e insistimos que eso era un engaño, el procurador dijo, no les miento y el expediente está ahí: "No se preocupe si no funciona en otro lado, aquí en Chiapas sí funciona, con nosotros no tiene problemas".

Después de cuatro o cinco meses dolorosos logramos salir, pero aprendimos muchas cosas, de inicio, por supuesto, que las técnicas de anonimato básicas o caseras no sirven en un régimen autoritario, qué teníamos que hacer más. Con el tiempo, Jacobo Nájera impulsó y sigue manteniendo un nodo Tor, de nombre Foucault, aquí en México.

Además, empezamos a trabajar promoviendo precisamente formas más seguras de anonimato y, como bien señalan, con cada actualización de los navegadores Tor hay que tener muchísimo cuidado. Los errores más básicos de uso de la herramienta nos puede llevar a equivocarnos, por ejemplo, maximizar ventanas mientras navegamos permite un registro de nuestra actividad o bitácoras en la computadora.

Si nuestro *anonymous* chiapaneco, que usaba la máscara de anonymous con un sombrero de chamula, hubiera tenido ese

3. "Al creador del GT-200, 7 años de prisión" https://archivo.eluniversal.com.mx/nacion-mexico/2013/impreso/al-creador-del-gt-200-siete-anios-de-prision-208488.html.

conocimiento, preservaría su función de denuncia social, de crítica del sistema, además era un vloguero muy visto que tuvo que dejar esa carrera por obvias razones. Los abusos que recibió permitieron llegar a una conclusión obvia y compartida: defender el anonimato es defender la libertad de expresión. En el núcleo de la libertad de expresión se atiende a los méritos del argumento o de la información en buena medida dependiendo del emisor, de su calidad, para decidir si está o no facultado para hablar, si es una persona importante o no. En cambio, defender el anonimato es defender la posibilidad de un debate democrático más profundo, enfocándonos en los méritos del argumento, de la información, pero también, tener en cuenta que estas herramientas pueden usarse para criminalizar a quienes las usan, un tema que surgirá cada tanto tiempo y del que no nos toca preocuparnos sino exaltar las virtudes del anonimato dentro de los sistemas autoritarios como el mexicano, que seguirá en la impunidad mientras no sea juzgado.

Así, cierro haciendo un llamado a la defensa radical del anonimato, donde de inicio no nos importe el uso que se le dé, sino que se vea la importancia de que exista la posibilidad de su ejercicio. Tenemos permitido todo lo que no esté prohibido y comunicarse anónimamente no está prohibido en México: intercambiar, compartir, crear redes anónimas no está prohibido, no es delito; por el contrario, la tendencia en las redes dominantes en internet es generar mayores puntos de identificación contra eso caminamos, busquemos los proveedores de servicio (ISP) que nos defienden y protegen, alejémonos cada vez más de las plataformas que requieren mayores puntos de identificación construyamos más libertad, es lo que se requiere.

Si quieren correr un nodo de Tor en México, existen manuales y folletos con recomendaciones. Pueden crear un punto de

repetición sencillo desde su casa, pero antes es muy importante que tengan algún intercambio de comunicaciones a través de las listas de correo del sitio Tor para compartir que eres un operador e inscribirte a una lista nacional y global donde además de intercambiar conocimientos, tejer redes de solidaridad, pues en los últimos meses ha habido algunos arrestos. Por ello, hay que establecer una política de salida y un aviso legal de excepción de responsabilidad.

Sólo me queda una petición. Tengamos mucho cuidado con la forma en que se expresan las normas restrictivas abiertas que, contrario al principio de que la autoridad sólo puede hacer lo que estrictamente le está permitido, estas normas de seguridad son redactadas con oraciones vagas y no determinadas. Este es el tipo de legislación al que hay que poner mucha atención (si bien normalmente la educación clásica de los ministros de la Corte hace que, en el derecho penal, éstas sean inconstitucionales, como en el caso de las faltas a la moral) cada vez más, la tendencia es a crear estas normas. Y muchas de ellas están incluidas en tratados internacionales, ambigüedad legal que abre la puerta a la autoridad.