Guerras de internet

Un viaje al centro de la Red
para entender cómo afecta tu vida

Guerras de internet

Un viaje al centro de la Red
para entender cómo afecta tu vida

NATALIA ZUAZO

DEBATE

Zuazo, Natalia
Guerras de internet - 1a ed. - Buenos Aires : Debate, 2015.
320 p. ; 23x15 cm. (Debate)

ISBN 978-950-3752-27-8

1. Ensayo Argentino. I. Título
CDD A864

IMPRESO EN LA ARGENTINA

Queda hecho el depósito
que previene la ley 11.723.
© 2015, Random House Mondadori S.A.
Humberto I 555, Buenos Aires.

www.megustaleer.com.ar

ISBN 978-987-3752-27-8

Esta edición de 4000 ejemplares se terminó de imprimir en
Arcángel Maggio - División Libros, Lafayette 1695, Buenos Aires,
en el mes de agosto de 2015.

Índice

TERCERA PARTE
DE SILICON VALLEY A NET MUNDIAL: CÓMO SE COCINA INTERNET

CUARTA PARTE
DE LAS CÁMARAS DE SEGURIDAD A TU CELULAR:
CÓMO LA TECNOLOGÍA TE CONTROLA (AUNQUE NO TE AVISEN)

A los cambios. Y a los valientes.

"Hay algo casi sagrado en internet.
Yo estoy tratando de secularizarlo."

Evgeny Morozov

"La manera como se presentan las cosas no es la manera como son;
y si las cosas fueran como se presentan la ciencia entera sobraría."

Karl Marx

"La historia de las luchas de poder, y en consecuencia las condiciones
reales de su ejercicio y de su sostenimiento, sigue estando casi
totalmente oculta. El saber no entra en ello: eso no debe saberse."

Michel Foucault

VII
Toda la Red es política: usuarios, empresas y gobiernos luchan por la web

"A medida que los Estados se fusionan con internet
y el futuro de nuestra civilización deviene en el futuro de internet,
estamos obligados a redefinir las relaciones de fuerza."

Julian Assange
Criptopunks (2012)

"Internet no es sólo el mejor servicio de video del mundo.
No es simplemente una mejor forma de ver pornografía.
No es sólo una herramienta para planear ataques terroristas.
Éstos son sólo casos del uso de la Red.
Pero ella es el sistema nervioso del siglo XXI.
Es hora de que empecemos a actuar así."

Cory Doctorow[103]

En 2007, a los 27 años, Claudio Ruiz, chileno, ya recibido de abogado, se dio cuenta de que tenía que tomar una decisión. Había terminado la facultad y trabajaba en Derechos Digitales, una organización que había fundado con algunos de sus compañeros. Los primeros años escribían *policy papers*, documentos serios y académicos sobre cómo tratar los nue-

[103] "How Laws Restricting Tech Actually Expose Us to Greater Harm", *Wired*, 26 de diciembre de 2015, http://wrd.cm/18YAEuE.

vos problemas legales que se presentaban con la Red. Pero, en mayo de ese año, la presidenta Michelle Bachelet envió al Congreso Nacional una propuesta para reformar la Ley de Propiedad Intelectual de 1970, en donde se incluían varios puntos relacionados con internet. La ministra de Cultura convocó a Claudio y su grupo, ya con experiencia en derechos de autor en la Red, como asesores. La presión era grande: la reforma se proponía en el marco de la negociación de un tratado de libre comercio con Estados Unidos en el cual la potencia buscaba flexibilizar los acuerdos de *copyright* para beneficiar a su industria.

—Tuvimos que tomar una decisión. Nos llamaron para trabajar asesorando a la ministra de Cultura en temas de derechos de autor. Pasamos de ser buenos técnicos a involucrarnos en una negociación "real" y entender sus códigos. Nos costó, pero meternos en política fue lo mejor que pudimos hacer.

Claudio Ruiz, hoy con 35 años, recuerda aquel momento mientras desayuna un café con leche con medialunas en El Banderín, un bar de Almagro. De espalda ancha y una barba espesa que le cubre la mitad de la cara, Claudio se entusiasma hablando de *su* tema, internet.

—Yo me gano la vida luchando por las cosas que creo: defender los derechos humanos en el ámbito digital. Eso es grandioso. Pero aprendí que para lograrlo tengo que jugar el juego de la política.

En las guerras de internet, Claudio forma parte de un colectivo grande y diverso llamado "sociedad civil". Dentro de él conviven todo tipo de organizaciones que reclaman y luchan, con diferentes herramientas, por la aplicación de derechos y libertades en la Red. Entre ellas también existen diferencias a la hora de pelear las guerras y sobre qué rol tomar frente a los distintos actores que controlan la Red. El primer grupo, más cercano al anarquismo, propone evitar cualquier control: internet no debería estar en manos de nadie (ni empresas ni países); debería funcionar en estado de total libertad. Para el segundo grupo, que podríamos llamar "liberal", la intervención debería darse para proteger los derechos y las garantías que tenemos como ciudadanos en el ámbito *online* y de reclamar transparencia absoluta de la información como forma de llegar

a la libertad de expresión. Para un tercer grupo, más cercano al marxismo o a una visión de lucha política pragmática, la Red es otro ámbito de una disputa del sistema capitalista mismo: para ellos, no existen conflictos *solamente* de internet, sino que son parte de una batalla más amplia (y antigua) sobre quién se queda con qué o cómo se distribuyen mejor los recursos. Sostienen que si la intervención es necesaria para regular desigualdades que produce el mercado, es bienvenida. Por supuesto, para todos ellos, hay luchas comunes, donde unen fuerzas.

Entre estas perspectivas, Claudio se ubica en una posición pragmática que no reniega de la política. Acepta el diálogo y que ninguna guerra puede pelearse fuera de un contexto de luchas de intereses. Sabe que hay que dialogar con todos los involucrados, e incluso educar a ciertos sectores o personas que no tienen por qué conocer sobre todos los temas, algo que sucede a menudo con los problemas de la tecnología.

—Desde las organizaciones de la "sociedad civil" de internet necesitamos entender los códigos de la política para lograr pequeños o grandes cambios.

Claudio lo explica con un ejemplo: cuando se empezó a negociar el Acuerdo Transpacífico de Cooperación Económica (TPP), un tratado de libre comercio multilateral que Estados Unidos promueve y negocia en secreto con once países del Pacífico, su organización sabía que, entre otros efectos, se iban a socavar los derechos de los chilenos en internet. Pero su campaña no se propuso enfrentarse a todo el acuerdo, porque implicaba una lucha política inmensa. En cambio, idearon un eslogan ("No al TTP cerrado") para decirle a la gente que Chile estaba negociando un acuerdo en secreto, donde también se escondían violaciones a sus derechos *online*.

—En vez de explicar todo el palabrerío de la ley, hicimos claro que con el TPP los proveedores de internet podían censurar contenidos sin intervención judicial, endurecer las sanciones a las infracciones del derecho de autor por compartir un video con un amigo o intervenir en el intercambio de información privada.

Lograr que los usuarios comprendan la importancia de las guerras de internet en sus vidas es una parte de su trabajo. Pero Claudio también

sabe que además se necesita educar a los políticos mismos, que muchas veces tienen que decidir sobre problemas nuevos que avanzan a medida que lo hace la tecnología.

—Hay activistas que cometen un error grande cuando dicen "todos los diputados son unos ignorantes en temas digitales". Bueno, hay ignorancia en general sobre asuntos nuevos. De la misma forma en que no le pedimos a un legislador que sepa todo sobre la ley de aguas o el código penal sin informarse con sus asesores, tampoco podemos pretender que sepa todo sobre la neutralidad de la Red. Hay asesores, gente que te puede explicar. Lo importante es dar el debate y no cerrarlo. Por ejemplo, cuando hablamos de propiedad intelectual en internet, les planteamos a los diputados preguntas que tuvieran que ver con su vida real: "¿Tu hijo comparte fotos por Twitter o por mail? ¿Sabes que sólo por compartir una imagen podría ser considerado un delincuente e ir preso?". Desde esa pregunta, es más fácil hablar: cómo te afecta a vos la guerra, cómo toca tus derechos.

Su experiencia también le hizo a Claudio ver de cerca que si el debate no se abría a la sociedad, quedaba en manos de las grandes corporaciones de la tecnología que destinan grandes recursos para favorecer sus intereses.

—Si nosotros no hablamos de esto sencillamente, las grandes empresas se encargan de hacer *lobby* para convencernos de que si compartimos una foto somos delincuentes. La presión de la industria es muy poderosa y el dinero que destina a publicidad, marketing, viajes, fiestas, enorme. Por eso también nos valemos de armas que sí dominamos, por ejemplo, las redes sociales y la movilización digital.

La primera movilización *online* masiva de las guerras de internet sucedió en enero de 2012. Frente a la discusión en el Congreso de Estados Unidos de las leyes SOPA (Stop Online Piracy Act) y PIPA (Protect IP Act), que buscaban limitar y sancionar el intercambio en internet por motivos de derechos de autor, la Red se organizó en una protesta conjunta de usuarios y empresas. A través de un apagón, llamado #SOPABlackout, se unieron grupos de usuarios de todo el mundo,

organizaciones como Mozilla y Wikipedia, y hasta megacorporaciones como Google, eBay y Facebook. La protesta fue un éxito: 15 congresistas cambiaron su postura frente a SOPA y la ley postergó su tratamiento. Sólo en la primera hora de la protesta, el 1% de los tuits mundiales se referían al tema y la portada de Wikipedia, que explicaba cómo podía ser un mundo sin conocimiento libre, fue visitada por 162 millones de personas y comentada por 12 mil. En un comunicado, la Casa Blanca sostuvo que el gobierno de Barack Obama no apoyaría "una legislación que reduzca la libertad de expresión". Los gigantes de internet también firmaron una carta de oposición rotunda al proyecto. Pero quizá el logro más grande del reclamo fue que, por primera vez, la libertad de internet se transformaba en un tema de discusión en los medios y en las redes sociales.

Las batallas por las guerras de internet se hacían cada vez más públicas, impulsadas por el efecto WikiLeaks y la organización de activistas. Luego las revelaciones de Snowden las hicieron estallar nuevamente, con la prueba de que los abusos a la privacidad de los usuarios eran perpetrados por las mismas instituciones que tenían que protegerlos. Hoy, las guerras no sólo ocupan las portadas de los medios *online* o las redes sociales, sino que llegan a las tapas de los viejos medios de papel y a ocupar minutos en los noticieros de la noche.

Para algunos, como Claudio Ruiz, o como yo, las guerras son más claras o más fáciles de comprender. Nuestra edad (los dos tenemos 35 años) tiene mucho que ver. En su libro *El fin de la ausencia*, el periodista canadiense Michael Harris escribe que los que vinimos al mundo antes de 1985 somos los últimos de una especie. "Si naciste antes de 1985, entonces sabés cómo es la vida con y sin internet —dice—. Podés hacer la peregrinación entre Antes y Después." Harris, como nosotros, nació en un mundo diferente, con menos canales de comunicación, menos formas de entretenimiento, menos escrutinio público de todo lo que hacemos o sentimos. Y, según él, no es un mundo ni mejor ni peor, pero nos ofrece una posición privilegiada para comprender los conflictos actuales y los que se acercan: "Si somos las últimas personas en la historia en conocer la vida antes de internet entonces también somos los únicos que podremos

hablar, para siempre, ambas lenguas. Somos los únicos traductores que podemos interpretar fluidamente el Antes y el Después"[104].

Hoy, las discusiones sobre la tecnología forman parte no sólo de las noticias, sino de las conversaciones con nuestros amigos o en la mesa familiar. Las guerras de internet ya no son del futuro. No sólo se debaten, sino que también empiezan a provocar consecuencias reales, enfrentamientos entre presidentes y protestas en la calle. Las guerras de la Red salieron de los aparatos.

¿Cuáles son esas luchas de las que escucharemos hablar en los próximos años? ¿Cómo hacer un mapa de ese campo de batalla para saber dónde estamos parados —o dónde quisiéramos estarlo— en esas luchas? ¿Cómo traducirlas para no quedar atrapados en medio de uno y otro poder? Primero, explicándolas desde lo técnico y lo político, pero también desde sus orígenes históricos, para entender quiénes conforman cada ejército. Aquí, algunas de esas guerras[105].

La guerra por las rutas

Geopolítica: países, corporaciones y el control de la información

La primera es una guerra geopolítica que condiciona el campo en donde ocurren el resto de las batallas. Se trata del enfrentamiento por el control de las rutas de la información, los caños, los tubos y los servidores que todos utilizamos para transportar y albergar nuestros datos. Por allí pasa todo en forma de bits: lo público y lo privado; desde los videos más ingenuos de gatitos en YouTube hasta los secretos de Estado más delicados.

La publicidad nos hace pensar que la información en internet puede tomar infinitos caminos pero la realidad es que, como dice el sociólogo Mariano Zukerfeld, "los tendidos submarinos de fibra óptica, los *back-*

[104] http://www.endofabsence.com/.

[105] La primera guerra es por la neutralidad de la Red, que tratamos en el capítulo 3 de este libro.

bones continentales y los satélites pertenecen a unas pocas empresas que oligopolizan la circulación de los flujos de información digital"[106].

Esa base física de internet, sobre la que se erige el resto de su estructura, tiene pocos dueños que ejercen un gran poder, similar al que detentan quienes dominan las rutas de otros bienes preciados. "Con el control de los cables de fibra óptica, por donde pasan los gigantes flujos de datos que conectan a la civilización mundial, ocurre lo mismo que con los oleoductos. Éste es el nuevo juego: controlar la comunicación de miles de millones de personas y organizaciones", dice Julian Assange en el prólogo de su libro *Criptopunks*. En América Latina, esos caminos de la información pasan, en un 98% por cables, servidores y empresas de Estados Unidos[107], con lo cual hay un claro problema: las comunicaciones están en cada país, pero también están en el territorio de una superpotencia[108].

El resultado de este mapa concentrado es una serie de batallas de soberanía, un campeonato de TEG del poder digital. Si nuestros datos pasan por otras manos y fronteras nacionales, ¿quién decide por ellos, qué ley les corresponde, quién puede controlarlos, espiarlos o utilizarlos? La infraestructura de internet hoy es un territorio que también puede ser atacado para dañar al adversario. O utilizar los datos que pasan por esas vías para lograr un objetivo político: espiar las acciones de otro

[106] "De niveles, regulaciones capitalistas y cables submarinos: Una introducción a la arquitectura política de internet", artículo de Mariano Zukerfeld en la revista *Virtualis,* junio de 2010.

[107] "Lo que pasa con Argentina me tocó vivirlo en carne propia", entrevista de Santiago O'Donnell a Julian Assange en *Página/12*, 7 de septiembre de 2014.

[108] Además de la concentración en los caminos físicos de los datos, también existe una centralización entre las empresas a quienes confiamos los contenidos. Como ya señalamos, en el mundo, un tercio de todo lo que hacemos diariamente en internet pasa por cinco grandes compañías. En la Argentina, el panorama es una réplica de la tendencia mundial, con algunos agregados locales: el mayor porcentaje de las visitas cotidianas lo concentran Google, Microsoft, Facebook, Yahoo y los dos grupos de medios de comunicación dominantes: *Clarín* y *La Nación* (le siguen Mercado Libre, Taringa y Wikipedia). Según datos de ComsCore, en su reporte "Futuro Digital Argentina 2014": http://bit.ly/1vHaf9J.

Estado, a sus propios ciudadanos, desviar informaciones, apropiarse de documentos que permitan tomar decisiones sobre ataques, guerras o disputas diplomáticas. Durante la Guerra Fría era necesario recurrir al espionaje, pero ahora todo está en una serie de caños y servidores que, por el crecimiento de internet en un país (Estados Unidos) y en una serie de corporaciones (generalmente, también de ese país), resultan en una nueva concentración del poder en pocas manos (y la tentación de controlarlo para dominar a otros). Así lo dice Assange: "El Gobierno de Estados Unidos no ha mostrado muchos escrúpulos en transgredir su propia ley al interceptar estas líneas para espiar a sus propios ciudadanos. Y no existen las leyes que impidan espiar a ciudadanos extranjeros. Cada día, cientos de millones de mensajes de toda América Latina son devorados por las agencias de espionaje de Estados Unidos y almacenados para siempre en depósitos del tamaño de ciudades. Los aspectos geográficos relativos a la infraestructura de internet, por lo tanto, tienen consecuencias para la independencia y soberanía de América Latina".

Por supuesto, los usos —y abusos— de la infraestructura de la tecnología se realizan de acuerdo con un mapa de disputas de poder que pelean por otros motivos, especialmente los económicos y los estratégicos. Son luchas de poder de un mundo hasta hace unos años dominado por Estados Unidos, pero que ahora tiende hacia una diversidad de actores, que aunque todavía están lejos del poderío militar (el poder duro) de los Estados Unidos[109], pueden comenzar a disputar un poder blando, con el conocimiento y manejo de otras herramientas basadas en la tecnología. No por casualidad, China y Rusia —dos líderes del bloque Brics— participan activamente en las reuniones de gobernanza de internet, casi siempre con expresiones de disidencia y destinan grandes presupuestos a la inversión en infraestructura tecnológica propia. En San Pablo, tras la lectura del documento final de Net Mundial, un representante de la comitiva de Rusia subió al estrado y expresó no sólo su completo de-

[109] El gasto en defensa de Rusia equivale nada más que al 7% del de la alianza occidental en la OTAN.

sacuerdo con la declaración final, sino también con la forma en que se habían tomado las decisiones. Pero allí estuvo su delegación para participar del debate.

En los últimos años, los países que alientan un mapa del mundo multipolar, como Brasil y el grupo de los Brics, o algunas naciones latinoamericanas, iniciaron dos ofensivas. La primera es diplomática y consiste en denunciar a los grandes poderes, especialmente a Estados Unidos, por utilizar la gran infraestructura de comunicaciones para entrometerse con sus datos: ya sea espiando a ciudadanos, posibles disidentes o terroristas, como a los funcionarios, diplomáticos y hasta presidentes de todo el mundo, sean amigos de la potencia o sus enemigos. Eso fue lo que denunció Dilma Rousseff (y aunque su país también hubiera espiado a diplomáticos norteamericanos[110]).

La segunda ofensiva la están dando en el desarrollo de redes propias de infraestructura, independientes del control de los Estados Unidos y las grandes potencias del mundo. Con esto y con el control de sus propios servidores de datos y software para el manejo de la información, reclaman una parte de la soberanía que, en las primeras décadas del avance de internet , quedó en manos de un puñado de empresas e instituciones fuertemente vinculados con el gobierno y la estructura militar norteamericana. El más ambicioso de estos proyectos es el Brics Cable, que unirá a Brasil, Rusia, India, China y Sudáfrica, enlazando Vladivostock en Rusia, Shantou en China, Chennai en India, Singapur hacia Ciudad del Cabo en Sudáfrica y cruzando el océano hasta Fortaleza, Brasil. Sin embargo, esto no promete una solución totalmente soberana, ya que, de todas formas, si cualquier ciudadano ruso, brasilero o sudafricano utiliza servicios como Facebook o Google, sus datos

[110] Seis meses después de las revelaciones de espionaje masivo realizadas por Snowden, el diario *Folha de São Paulo* informó que la Agencia Brasileña de Inteligencia (Abin) vigiló en Brasilia una serie de salas alquiladas por la embajada de Estados Unidos, además de espiar a diplomáticos Rusia, Irán e Irak. La Presidencia admitió la operación y defendió su legalidad bajo la figura de "contraespionaje".

igual viajarán por servidores de estas empresas, mayormente ubicados en Estados Unidos.

En esta batalla, el avance o el retroceso será también en el plano de la geopolítica, de las negociaciones y alineaciones internacionales, en un mundo que está dejando de tener un solo centro (Estados Unidos) para tener una serie de potencias que lideran en el mundo. Para ellas, dominar las vías de comunicación de la tecnología será estratégico.

Sin embargo, también en los próximos años veremos crecer un nuevo fenómeno: las guerras de la política internacional se dirimirán no sólo con ejércitos reales, en campos de batalla de tierra o mar, sino que también se pelearán en espacios virtuales, de la mano de los ciberejércitos que cada país viene formando en los distintos (ciber)territorios de la Red. Desde las grandes potencias hasta países más pequeños con voluntad de imponerse en la agenda internacional o de producir daños y defenderse de ataques, distintos Estados reclutan y entrenan, desde hace unos años, hackers y expertos en ciberguerra. Más o menos reconocidos oficialmente por los gobiernos, todos ellos dependen de las estructuras militares o departamentos de defensa de cada país y son financiados tanto en su trabajo como en sus sofisticadas infraestructuras por el presupuesto nacional. Las cibermilicias también compran armas, pero en forma de infraestructura de telecomunicaciones: computadoras, servidores y software.

En 2010, Estados Unidos fue uno de los primeros países en hacer público su ciberejército, también conocido como United States Cyber Command, que depende directamente de las Fuerzas Armadas y declara la misión de "velar por los intereses del país y sus aliados, con la protección directa a sus sistemas informáticos o actuando en respuesta a ataques". El Cibercomando trabaja en conjunto con la NSA y ambos tienen su sede en Fort Meade, Maryland, aquel lugar por donde Edward Snowden pasaba por en frente durante la adolescencia y que luego fue su lugar de trabajo hasta revelar la información sobre la Agencia de Seguridad. En su página oficial, arcyber.army.mil, además de detallar sus tareas y noticias, los candidatos a integrar el

cuerpo pueden postularse, bajo un llamado: "Se necesitan cibersoldados. Queremos reclutar y desarrollar a los ciberguerreros del siglo XXI. Apasionados, creativos y determinados a encontrar soluciones a los desafíos que enfrentamos en el siglo". El Comando ya cuenta con cinco mil soldados, que, al ser Estados Unidos el país más atacado —por lejos— por ciberofensivas de otros países, tiene la misión de defender sus territorios virtuales.

El segundo ciberejército más poderoso está en China. Llamado Ejército Azul o "Unidad 61398", depende del Ejército Popular de Liberación (las Fuerzas Armadas del país) y cuenta con unos dos mil integrantes y una infraestructura de fibra óptica provista por la estatal China Telecom. El 80 por ciento de sus ataques están destinados a compañías de Estados Unidos, en especial las de la categoría "blue chip" (grandes corporaciones que cotizan en bolsa), y para defenderse de los ataques a sus instalaciones. En cuestiones defensivas, Israel, Finlandia y Suecia encabezan el ranking de los países más preparados para resistir ataques cibernéticos. Le siguen el Reino Unido, Estados Unidos, Alemania, España y Francia. En el otro extremo, China, Brasil y México se encuentran entre los países con menos defensas para resistir una ofensiva[111].

Desde 2011, la Argentina también conformó un comando para defender al país de ataques cibernéticos y proteger las infraestructuras del sector público. El 28 de julio de ese año, la Jefatura de Gabinete de Ministros dictó la resolución 508 por la cual creó el "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad"[112]. Además de trabajar y capacitar a los organismos del Estado contra ataques, previene vulnerabilidades e implementar tecnologías de seguridad informática.

Si antes las guerras necesitaban dañar u ocupar un territorio, las rutas y las comunicaciones en un país o una ciudad determinada, hoy eso mismo puede hacerse a través de una o miles de computadoras puestas

[111] Según datos de la compañía de seguridad informática McAfee.

[112] http://www.icic.gob.ar.

a trabajar en simultáneo, por ejemplo, atacando las computadoras de un organismo del ejército de un país enemigo o de una empresa con capitales de ese país. Todos los días leemos títulos que lo demuestran: "Hackers paquistaníes atacan la milicia india", "Apple sufrió el mayor ataque de su historia desde China", "Corea del Norte filtra documentos de una compañía norteamericana", "Hackers rusos atacan computadoras de la Otan", "Ciberejército iraní golpea Twitter".

Los ataques tienen orígenes muy diversos. Pueden provenir desde las propias cibermilicias oficiales hasta realizarse cuando distintos grupos de activistas de un país encaran un ataque contra una empresa o un objetivo en otro país. Muchas veces, los ciberejércitos oficiales también reciben ofensivas de parte de activistas virtuales de su propio país. Por eso, es necesario que cuando leamos "ataque de hackers" siempre pensemos que es un término que puede incluir dentro de sí expresiones muy distintas, que van desde hacktivistas más o menos organizados, hasta soldados financiados por un Estado y corporaciones. Ambos son hackers en el sentido amplio de la palabra: una persona que usa conocimientos de informática para penetrar una red. Pero los objetivos pueden ser sumamente diversos: desde el rechazo ideológico a una empresa extranjera, la venganza ante la actitud de una compañía o gobierno, la represalia por un acto puntual haciendo caer el sitio de una empresa, de un municipio o de la policía local. En general, la mayoría de los ataques son para desplomar un sitio o para filtrar una información, o ambas cosas al mismo tiempo. Uno de los procedimientos más sencillos consiste en que muchas computadoras, se pongan de acuerdo para lanzar ataques a un objetivo y colapsarlo. "El más común y más efectivo de los ataques, es el DDoS (ataque de denegación de servicio), el típico que hace que el servidor se sobrecargue y el sitio se caiga", me explicaba hace unos años un hacktivista que participa habitualmente de operaciones desde América Latina. Algunas organizaciones (como Anonymous) desarrollaron programas sencillos para bajarse de internet y sumarse a operaciones.

En una página adictiva de la empresa de seguridad informática Norse (map.ipviking.com) pueden seguirse los ciberataques del mundo, con

origen y destino, y en tiempo real. La mayoría de ellos provienen de China, Rusia o algún país de América Latina y están destinados a algún blanco en Estados Unidos, en general a organismos de defensa (en Washington, Virginia, la costa este, o donde haya bases militares) o a compañías de internet (en general ubicadas en la costa oeste, alrededor de Silicon Valley, aunque también pueden ser grandes compañías de telecomunicaciones como Verizon o AT&T, con sedes en distintas ciudades del país). Pero también ocurren desde Estados Unidos hacia, por supuesto, Rusia y China. Mientras escribo este párrafo, un domingo a la tarde, un día que debería ser tranquilo o de descanso, están ocurriendo 3.854 ataques originados en China, 1.447 desde Estados Unidos, 849 desde Rusia, 568 desde Alemania, 327 desde Japón, 319 desde Mil.gov (es decir, desde los dominios del ejército estadounidense), 289 desde Corea del Sur, 292 desde México, y el resto de la lista lo integran países de Asia y Europa. De todos los ataques, más de ocho mil están dirigidos a Estados Unidos. El segundo país es Rusia, que recibe menos de 300.

Corea del Norte es otro de los países con una cibermilicia poderosa, cuyas acciones llegan con frecuencia a la prensa internacional. El dato no es casual, ya que el país comunista, enemigo declarado de Estados Unidos, posee un porcentaje de personal militar enorme, de 40 soldados cada 1.000 civiles. Su ciberejército ya cuenta con seis mil integrantes, en su mayoría jóvenes con habilidades de *hacking*, cuyo comando central, dependiente de Pyonyang, se ubica en la frontera vecina bajo el mando de Seúl. Dentro de ellos, hay un grupo de elite, la llamada "Oficina 121", que cuenta con 1.800 jóvenes, seleccionados entre los mejores promedios de ciencias de la computación de la Universidad de Mirim y entrenados durante nueve años, en los que viajan a los países que atacarán, estudian su idioma y su cultura. Las cibermilicias de Corea del Norte realizan frecuentes ataques contra su vecino China, pero también contra objetivos de infraestructura de Corea del Sur como bancos, organismos militares, medios de comunicación y cadenas de televisión. Según expertos informáticos de todo el mundo, Pyonyang cuenta con algunos de los hackers más sofisticados del planeta. Sin embargo, y en una de las tantas paradojas

de las guerras de internet, esto sucede en un país donde no existe el acceso a la web para la mayoría de la población. A diferencia de China, que tiene un gran firewall o barrera "alrededor" de su Red y donde sus ciudadanos pueden acceder básicamente a sitios con direcciones IP y contenidos provistos por empresas nacionales, en Corea del Norte sólo existe el acceso para ciertos grupos restringidos, como funcionarios de gobierno y periodistas extranjeros. Ésa es una de las razones por las cuales también es difícil penetrar en sus sistemas informáticos: al estar limitada internet a un ámbito cerrado es menos vulnerable a los ataques externos.

La ciencia ficción que hablaba de los juegos de guerra con enormes computadoras en la década de los 80, se volvió realidad. En internet ocurren y tendrán lugar en el futuro todo tipo de guerras, desde las estratégicas para robar datos sobre ventas de petróleo o filtrar cables diplomáticos sobre negociaciones de paz, hasta las pequeñas batallas de la cultura, los negocios y el entretenimiento. La razón es que la Red ya es otro terreno de la política internacional.

La guerra por la palabra

Libertad de expresión: medios, usuarios y el control de la opinión

La segunda guerra se centra en internet como espacio de opinión. Los sitios, los blogs, los medios *online* y las redes sociales son nuevas plazas de expresión. En ellos comentamos, compartimos, calmamos nuestra sed de fama y ego subiendo una foto o compartiendo la de otros, y aplacamos la necesidad de que nos escuchen. La sensación de que estamos diciendo algo que muchos pueden leer es tan potente que también se hace adictiva: necesitamos decir lo que pensamos. Queremos que otros opinen, y opinar sobre lo que dicen los otros.

Con la masificación de las tecnologías, y en especial de internet, los costos de alcanzar audiencias son cada vez menores. También se amplió la posibilidad de que más personas, dominando algunas herramientas digitales sencillas, participen expresando su voz a través de blogs, medios

digitales, redes sociales, o comentando la información ya disponible. Sin embargo, esto también produjo un exceso de información, que se multiplica exponencialmente todos los días. Para encontrar lo que queremos en ese caos se necesitan una serie de empresas que organizan, ordenan y filtran lo que los usuarios (que también son ciudadanos) buscan[113]. Ellos son los llamados intermediarios de internet, una serie (bastante grande y diversa) de organizaciones que van desde sitios de noticias, plataformas de blogs, redes sociales, buscadores, aplicaciones, sistemas operativos móviles, empresas que prestan conexión a internet o *hosting* (espacio de almacenamiento en servidores). Todos ellos son parte del intercambio diario de contenidos y opiniones, y, a medida que la Red contiene información de todo tipo, son también protagonistas de conflictos que es necesario dirimir.

¿Qué pasa cuando alguien sube, comenta o publica algo que afecta a otro? ¿Quién es responsable: el autor o la plataforma o empresa donde lo hace? ¿A quién y cómo deben responder los intermediarios ante un pedido de un gobierno, de la justicia, de otro usuario o de otra empresa? ¿Qué derechos tiene un usuario frente a ellos? La guerra está intrínsecamente relacionada con la libertad de expresión. Y los intermediarios son fundamentales porque, al mismo tiempo que son un nuevo espacio para volcar nuestras voces, son también dueños de un poder (que también buscan limitar otros poderes, por ejemplo, un gobierno).

Todos los días se producen reclamos para determinar si un contenido que pudo afectar a una persona tiene que ser eliminado de la Red o no. Las razones son diversas: algunas tienen que ver con la reputación o la intimidad, otras con dar de baja el resultado de un juicio que ya caducó o reclamar por derechos de autor. El tema es delicado porque por un lado está el derecho de una persona a que no se diga o se muestre algo que no quiera (por ejemplo, una foto de su intimidad o un dato de su

[113] "Los intermediarios y los desafíos para la libertad de expresión en internet", Ramiro Álvarez Ugarte y Eleonora Rabinovich http://www.cuestiondederechos.org.ar/pdf/numero4/Articulo-8.pdf.

pasado). Pero por otro está la libertad de expresión. La línea es finísima: intervenir sobre los contenidos que se producen en internet puede coartar la libertad de expresión y caer en la censura, pública o privada. "Los intermediarios cumplen un rol esencial para ejercer el derecho de buscar y recibir información en línea", dice Eleonora Rabinovich, abogada de la Asociación por los Derechos Civiles[114]. Y explica: "La función de los intermediarios ha sido asociada frecuentemente a la de *gatekeepers*: actores privados que, por el rol que cumplen dentro de un contexto determinado, tienen poder para controlar o dirigir —en alguna medida— el flujo de las comunicaciones".

Esta guerra tiene nombre: la responsabilidad de intermediarios en internet. Y su pregunta clave es: ¿deben ser estos intermediarios responsables de lo que los usuarios hacen en la web? El conflicto es tan viejo como la expresión libre de la palabra, sólo que ahora está mediada por una complejidad de actores y empresas a quienes confiamos diariamente los contenidos de la Red. Como Google, encargado de filtrar el mayor porcentaje de las búsquedas diarias de internet, o Facebook, donde cualquiera con una cuenta activa puede expresarse, subir comentarios, fotos, links. Todos los países, desde Estados Unidos hasta Europa y América Latina, están comenzando a enfrentarse con casos que involucran la responsabilidad de intermediarios y con jueces a los que se les solicita decidir sobre estos conflictos. Las sentencias, sin embargo, todavía no son unívocas y existen al menos tres caminos que los magistrados están tomando en la resolución de estos problemas.

El caso más conocido en Argentina sucedió cuando una modelo, Belén Rodríguez, demandó a Google y Yahoo por mostrar en los resultados de sus buscadores fotos donde se la vinculaba a sitios de pornografía, por lo que responsabilizó a ambas empresas por lesiones a su intimidad y honor. Luego de un extenso juicio que llegó hasta la Corte Suprema, el máximo tribunal emitió un fallo que establece que no puede conde-

[114] "Internet: la tercera vía", *Bastión Digital*, 4 de noviembre de 2013. http://ar.bastiondigital.com/notas/internet-la-tercera.

narse a Google por lo que sucede en la web. En otros términos: no se puede condenar al bibliotecario por lo que dice el libro. En palabras de la Corte, no puede atribuirse una responsabilidad "objetiva" a los intermediarios de internet, como si ellos estuvieran comprometidos con cada contenido publicado en su plataforma. La razón es que si tuvieran esta responsabilidad tendrían que intervenir en los contenidos, lo que no es sólo técnicamente complejo, sino que violaría otros derechos como la libertad de expresión y la privacidad (porque tendría que monitorearse previamente todo lo que se sube a la web).

Con su resolución, el máximo tribunal argentino tomó lo que Rabinovich denomina como una "tercera posición" respecto de los antecedentes que se vienen desarrollando en el tema en Europa y Estados Unidos. "En Estados Unidos, los intermediarios gozan de una cuasi inmunidad absoluta por los contenidos generados por terceros, pero cuando se trata de infracciones a los derechos de autor deben darlos de baja luego de una simple notificación de un particular", señala Rabinovich, en referencia al sistema conocido como *notice & takedown*, una forma rápida de notificación y retiro extrajudicial que se adoptó en ese país por presiones de la industria del entretenimiento[115]. Sin embargo, el sistema tiene dos grandes riesgos en su funcionamiento. El primero, la eliminación excesiva de contenidos, ya que ante un solo pedido deben darse de baja. El segundo, que tales decisiones quedan en manos de unas pocas empresas que controlan el mayor porcentaje de las búsquedas *online*.

"En Europa, los intermediarios no son en general responsables salvo que hayan sido alertados sobre la actividad ilícita y no hayan actuado en consecuencia", explica la abogada, referente en el debate de los temas judiciales de internet en Argentina. El caso más comentado en Europa se resolvió en mayo de 2014 en España, cuando luego de seis años de litigio el abogado Mario Costeja logró que Google retirara de sus resultados de búsqueda

[115] Con este sistema, las demandas por contenidos de usuarios que violen los derechos de autor pueden ser fácilmente procesadas, quitándolas de circulación ante un pedido sencillo de las corporaciones.

enlaces que lo vinculaban con una deuda inmobiliaria de 1998, que aparecía en el diario *La Vanguardia*. Según ese medio, no se justificaba retirarlo porque era información legal. Pero Costeja entonces fue contra Google, a quien le reclamó que esos eran datos personales de una deuda ya saldada. La Audiencia Nacional de España finalmente le dio la razón, con lo que se generó el precedente del "derecho al olvido", es decir, que frente a un pedido efectuado ante el buscador por un ciudadano para dar de baja un contenido que lo relacione, Google debe dar curso a la petición. En 2014, el Tribunal de Justicia de la Unión Europea siguió el camino del derecho al olvido, declarando que las empresas que gestionan las búsquedas deben acceder a quitar los vínculos a páginas web de terceros que afecten a otra persona[116].

Sin embargo, los especialistas advierten sobre el peligro de que este tipo de decisiones queden directamente en manos de una empresa privada —en este caso, el megabuscador— a través de un simple formulario sin intervención de un juez o una instancia pública que defina el derecho que prevalece. En este punto, el tema es tan delicado como: ¿qué sucedería si quien pide la remoción de un dato es un político acusado de corrupción con una causa ya archivada, pero que luego de diez años se quiere presentar a elecciones? ¿No deberían los ciudadanos, por razones de derecho a la información, tener acceso a esos datos sobre las actividades pasadas de esa persona? ¿Quién determina dónde se pone un límite al pasado? Eduardo Bertoni, abogado y profesor de derechos digitales del Centro de Estudios sobre Libertad de Expresión de la Universidad de Palermo, advierte que, en el caso de los países de América Latina, con una historia de largas y crueles dictaduras, el derecho al olvido tendría serias consecuencias. Bertoni señala que sería un agravio para una región donde, "en lugar de imponer el olvido se ha estado peleando en las últimas décadas por la verdad de lo ocurrido durante los oscuros años de dictaduras militares. Búsqueda de la verdad y olvido son contradictorios".

[116] La información no se borra sino que deja de ser indexada, es decir, reduce su posibilidad de ser tomada en cuenta en futuras búsquedas. Por eso, para algunos especialistas, es más adecuado referirse al "derecho al olvido" como un "derecho a la desindexación".

Como ejemplo, el académico destaca: "Si quienes estuvieron involucrados en violaciones masivas a los derechos humanos pudieran pedir, sin perjuicio del resultado de la solicitud, a un buscador de información en internet (Google, Yahoo, o el que se nos ocurra) que esa información no sea posible de encontrar bajo argumentos, por ejemplo, de que es información extemporánea, resulta, por decirlo suavemente, un insulto a nuestra historia".

El derecho al olvido fue un concepto muy citado desde 2014, con optimismo de un derecho para los usuarios de internet. Sin embargo, tiene consecuencias, en tanto siempre es alguien quien decide. La respuesta no es sencilla. Como dice Bertoni, la solución quizá no sea restringir los contenidos, sino generar mecanismos para que más personas aún opinen sobre ellos, incluso denunciando los que no les gustan o infringen algún otro derecho.

También se ponen en conflicto nuevas soberanías. Al ser internet una herramienta global pero las decisiones tomadas por las justicias locales, ¿qué pasa si un país decide bloquear un contenido que afecta el derecho de otros países a verlo? ¿Qué derecho vale más? Es una cuestión de diseño tecnológico que afecta la palabra, pero también el conocimiento colectivo.

Pero para que internet siga siendo un espacio de libre opinión se necesitan otras condiciones, todavía no garantizadas para todos. La primera es el acceso. Los que tenemos capacidad económica, vivimos en ciudades con buen servicio, e incluso podemos elegir entre varios proveedores, lo damos por sentado. Pero no es todavía un servicio común para gran parte del mundo. En América Latina, cerca del 50% de la población tiene acceso a internet, en el promedio regional. Sin embargo, en países como Haití, Ecuador, Honduras y Paraguay, el acceso llega recién al 10% de la población[117]. Esta brecha digital, que no es más que una brecha social y económica, tiende a cerrarse paulatinamente, aunque todavía existen disparidades.

Pero además del acceso, una vez que "estamos" en internet necesitamos que nuestro derecho a expresarnos esté garantizado. El 5 de julio

[117] Según datos de la Cepal (Comisión Económica para América Latina y el Caribe).

de 2012, el Consejo de Derechos Humanos de Naciones Unidas dictó una resolución donde declara que "los mismos derechos que las personas tienen fuera de internet deben ser protegidos cuando están conectadas". Es decir, que internet es otro espacio donde se ejercen, y también se tienen que defender, los derechos humanos. Y como todo espacio de derechos, también lo es de conflictos. La resolución de Naciones Unidas de 2012 se convirtió en una base para que las justicias nacionales tengan un marco legal para basar sus fallos, protegiendo a sus ciudadanos. "La relación entre derechos humanos e internet es compleja y no está exenta de matices. Si bien el acceso a internet ha potenciado la habilidad para ejercer la libertad de expresión, también es cierto que ha dificultado el ejercicio de otros derechos tales como el de la privacidad", explica Valeria Betancourt, activista ecuatoriana de derechos de internet[118].

Sin embargo, las guerras todavía son muchas, como denuncia la activista: "El bloqueo, control y manipulación de contenidos; el retiro de contenidos en línea por parte de proveedores de servicios sin un debido proceso; la interferencia con la privacidad y la protección de datos personales; la limitación de la calidad del acceso por parte de operadores y proveedores de servicios a fin de dar preferencia a ciertas aplicaciones y contenidos (por ejemplo, violando el principio de neutralidad de la Red); la creciente presión por parte de los gobiernos sobre los intermediarios de internet para controlar el internet; la aplicación radical de la legislación de propiedad intelectual, entre otros aspectos, son prácticas cada vez más frecuentes y sofisticadas".

En cada país, los casos están en los medios todos los días: una celebridad o un ciudadano pide dar de baja un contenido, un legislador exige censurar a los sitios de noticias por "promover la discriminación", una empresa de entretenimientos intimida a un proveedor de internet a censurar sitios de descargas porque pueden afectar sus derechos de autor. El riesgo es que, en pos de proteger un derecho, limitemos otros.

[118] "Derechos humanos en línea: una agenda aún pendiente para la sociedad civil de América Latina y el Caribe", por Valeria Betancourt: http://bit.ly/1Lc4dqB.

En internet esa línea es muy delicada y cada una de esas medidas suele ser desproporcionada según su objetivo inicial. Por ejemplo, para dar de baja una noticia a pedido de una celebridad, los buscadores suelen eliminar todos los resultados de una búsqueda de ese nombre. Eso fue lo que sucedió con Yahoo en Argentina, que suprimió todos los resultados relacionados con las modelos "Valeria+Mazza" o "Julieta+Prandi" para cumplir con órdenes judiciales. Por cuestiones técnicas, un pedido de un privado puede hacer que se borren partes enteras de internet, como sucedió cuando una corte de Pensilvania, Estados Unidos, encontró que un proveedor de servicios de internet borró cerca de 1,2 millones de sitios "inocentes" para responder a un pedido de agencias de seguridad para deshabilitar sólo 400 sitios[119].

Algo similar sucedió el 30 de junio de 2014, cuando el juez argentino Gastón Polo Olivera ordenó bloquear el acceso desde Argentina a las direcciones IP y los nombres de dominio de *The Pirate Bay*, el sitio más conocido de búsqueda y descarga de *torrents*, a pedido de la industria de la música[120]. El magistrado argumentó que *The Pirate Bay* "facilita la violación de los derechos de propiedad" porque "el 25% de los contenidos disponibles en el sitio se corresponde a música, de la cual al menos el 75% está disponible para ser adquirida comercialmente". El problema es que el bloqueo se realizó para todo el sitio de descargas a partir de un pedido concreto. En pocas horas, la comunidad de usuarios reaccionó creando varias copias del sitio[121], que crecieron como cabezas de Hidra: ante cada baja se multiplicaban las páginas.

Pero no sólo los jueces podrían decidir sobre qué podemos ver en internet. Desde sus distintas instancias, los gobiernos también lo hacen[122]

[119] Ejemplo citado en Álvarez Ugarte y Rabinovich, *op. cit*.

[120] Cámara Argentina de Productores de Fonogramas (Capif), la Sociedad Argentina de Autores y Compositores de Música (Sadaic) y seis discográficas (Warner, EMI, Universal, Leader Music, Sony, Epsa).

[121] Y publicaron el sitio de denuncia chupalacapif.com.

[122] Para un informe completo, ver Freedom of the Net 2014, de Freedom House http://bit.ly/1rGAp00.

con diversas medidas. Algunos limitando el acceso desde la infraestructura, con barreras para bloquear sitios o aplicaciones, o la salida de las conexiones hacia otros países. Otros, limitando los contenidos que pueden verse desde el país, con filtros o distintos tipos de censura a sitios o medios *online*, o usando internet para detectar activistas opositores y perseguirlos. Y también, violando los derechos a través de la vigilancia masiva y la intromisión en la privacidad. Entre los primeros países, los más conocidos por sus prácticas son China, Rusia, Cuba, Irán, Turquía, Ucrania y Angola. En términos de vigilancia, Estados Unidos es el país líder en este tipo de violaciones, pero no existe casi ningún gobierno (de Alemania a Brasil) en el mundo que no recurra a estas herramientas de intromisión para monitorear a sus ciudadanos, ya sea con la excusa de la lucha contra el terrorismo, o de amenazas internas a la seguridad, o menos explícitas pero practicadas, como el espionaje político contra adversarios.

También existen propuestas de algunos legisladores que, intentando proteger ciertas libertades, atentan contra la libertad en la Red. En septiembre de 2014, el diputado argentino Remo Carlotto presentó un proyecto de ley donde proponía luchar contra la discriminación multando y clausurando sitios web con comentarios maliciosos. Entre ellos, incluía "páginas, blogs, redes sociales, agencias de noticias, medios de prensa, diarios *online*, revistas electrónicas y otros sitios de internet que admiten que los usuarios publiquen contenidos, opiniones o dejen mensajes en sus respectivos dominios". El problema de este proyecto es que delega a organismos especialmente creados facultades judiciales que ya existen en otras leyes. Es decir, que con un reclamo judicial podrían resolverse. Otros planes van más allá y proponen el riesgo de cerrar sitios completos para "prevenir" lo que algunos usuarios puedan expresar, lo cual es una medida claramente desproporcionada. Otro proyecto que generó polémica provino del diputado del PRO Sergio Bergman, que se sumaba a las entonces recientes iniciativas de derecho al olvido europeas proponiendo una ley que permitiera a empresas, organizaciones no gubernamentales y partidos políticos reclamar y obtener una rápida baja de contenidos por parte de los buscadores. El problema con estas

ideas es que, ante un pedido de este tipo, las empresas siempre optan por dar de baja a una cantidad mayor de contenidos de los que son estrictamente necesarios.

Pero no sólo es con leyes y la censura de sitios o contenidos como se puede afectar la libertad de internet. También hay conflictos que, partiendo de lo técnico, pueden implicar grandes riesgos a la forma en que hasta ahora la conocimos.

La guerra por la cultura

Copyright: creación, monopolios y el control de la innovación

La cuarta guerra es quizá la primera que se presentó como tal —cronológicamente hablando— en la era digital. Se origina también en una posibilidad técnica que ofrece internet: la de copiar y distribuir contenidos de forma sencilla y barata, sin necesidad de dominar tecnologías complejas o costosas. Y enfrenta a quienes dominan la industria del entretenimiento con los millones de usuarios que gracias a las herramientas digitales pueden acceder a ellas más fácilmente. Pero además, pueden modificarlas, remixarlas y distribuirlas. Responde a una pregunta vieja que renació en la era de internet: ¿quién es el dueño de la cultura? O, más lejos: ¿de quién son las ideas que circulan en la Red? El gran inconveniente de esta guerra es que se presenta como un problema de internet en relación con el mundo del arte, la cultura o el entretenimiento. Sin embargo, sus consecuencias afectan a toda internet, es decir, a ese espacio donde hacemos algo más que consumir entretenimientos.

En julio de 1999, Sean Parker y Shawn Fanning[123] crearon Napster[124], un programa que permitía compartir archivos de música en formato

[123] Parker, nacido en 1979, después fue uno de los fundadores de Facebook y actualmente es uno de los accionistas del servicio de música por *streaming* Spotify.

[124] Para una historia de Napster, ver el documental *Downloaded* (2013), dirigido por Alex Winter.

MP3. Fue la primera gran red de *peer-to-peer* (P2P), es decir, de intercambio de archivos entre usuarios de internet. Y fue un éxito. En los primeros nueve meses, Napster tenía 10 millones de usuarios registrados; dos años después, eran 26 millones. Sus inventores habían unido, por medio de un código, a la música que ya estaba disponible en la Red con gente que ya la compartía. Sin embargo, la industria discográfica cargó contra ellos rápidamente. En diciembre de 1999, los tribunales de Estados Unidos cerraron Napster por violación de derechos de autor. También vertiginosamente, aparecieron otros programas de intercambio de archivos P2P (Kazaa, Ares, eMule), demostrando que Napster simplemente funcionaba como un motor de búsqueda e intercambio de datos que ya estaban allí. Desde su creación, internet se trataba justamente de eso: de compartir información. El problema es que algunos —muy poderosos— no querían que sucediera. O, al menos, que no se hiciera sin pagarles.

Todo lo que existe en internet se puede tomar y modificar, y por lo tanto compartir. Como escribió el profesor de computación Lev Manovich en *El lenguaje de los nuevos medios de comunicación*[125], la característica fundamental de todos los objetos *online* es que son divisibles, combinables, capaces de variar. Esto es porque están hechos de pequeñas partes, los bits (caracteres de texto, música, imágenes), que podemos editar y combinar. Pero, además, lo que permite internet es la capacidad de distribuir los datos por nuestros propios medios. Antes, había que tener una imprenta, saber editar, tener máquinas costosas, dominar un circuito de distribución. Por eso la cultura circuló, desde Gutenberg hasta internet, dominada por monopolios, que también pusieron el precio a las obras, porque se encargaron al mismo tiempo de estipular y hacer cumplir los derechos de autor.

Con el nacimiento de la Red, la distribución está potencialmente en manos de mucha más gente. Con ello, la cultura, la música, el cine, el video, los libros, tuvieron una época dorada de creación. Pero entonces las corporaciones y la industria, que dominaron gran parte de la cultura

[125] Manovich, Lev. *El lenguaje de los nuevos medios de comunicación*, Barcelona, Paidós, 2006.

durante siglos, empezaron a perder su monopolio. Como dice el escritor y ensayista italiano Alessandro Baricco en *Los bárbaros*[126], estos poderes se encontraron con "una revolución tecnológica que rompe de repente con los privilegios de la casta que ostentaba la primacía del arte".

Las grandes corporaciones no sólo reclaman que se les pague por derechos de autor a quienes hagan circular "sus obras", sino también a quienes las exhiban, aunque no las hayan subido ellos mismos. Es decir, también inician demandas contra intermediarios de internet como YouTube, por ejemplo, por alojar un video o una canción (o partes de ellos) de su propiedad[127]. Por estos litigios, muchas veces un usuario de Argentina no puede escuchar canciones o ver videos cuyos derechos de autor no se negociaron localmente y entonces aparece una pantalla negra que nos advierte que dichos contenidos "no están disponibles para la región" o "infringen derechos de autor".

La industria del entretenimiento, una de las más poderosas del *copyright*[128], declaró la guerra. Napster fue uno de los primeros capítulos. Los grandes estudios, las discográficas y las editoriales se enfrentaron a cualquier novedad tecnológica: apuntaron contra los programas de intercambio de música, contra los primeros reproductores de DVDs alegando que se podrían copiar las películas, contra los libros y lectores de ebooks suponiendo que iban a terminar con los libros en papel, contra los servicios de películas por *streaming* que harían que nadie más fuera al cine. También limitaron, o directamente cooptaron, a las plataformas a través

[126] Baricco, Alessandro. *Los bárbaros*, Barcelona, Anagrama, 2008.

[127] Uno de los casos más resonantes fue el del megajuicio que inició Viacom (compañía dueña de canales como MTV) contra YouTube/Google en 2007, por el que reclamaba mil millones de dólares en concepto de daños por "violación masiva internacional de *copyright*". En 2013 la justicia de Estados Unidos falló a favor del sitio de videos, alegando que, en su condición de intermediario, no era responsable de los contenidos (protegidos o no por *copyright*) que subieran sus usuarios.

[128] Junto con la medicina y la salud (industria de los medicamentos, vacunas, avances médicos), y la alimentación (soja, transgénicos, Monsanto), la tecnología y el software (Microsoft, Apple).

de las cuales se consume la cultura en internet, por ejemplo, servicios de video *online* como YouTube, con quien las discográficas y los estudios de cine y televisión realizaron acuerdos para que les pagasen por exhibir sus contenidos y para que estuvieran disponibles o no en ciertos países.

Esta industria está dominada por grandes corporaciones transnacionales y apoyada por artistas y autores locales, algunos muy enfáticos para reclamar sus derechos[129]. Las primeras patentes de propiedad intelectual las dictaron, en el Renacimiento, reyes que querían mantener para sí mismos el monopolio de lectura de ciertas obras. Trescientos años después, las grandes compañías de entretenimientos se basan en el mismo sistema porque su negocio principal es ganar dinero con las licencias de lo que compran y patentan. Entre ellas se encuentran las dos asociaciones más grandes: la Motion Picture Association of America (MPAA) y la Recording Industry Association of America (RIAA), que impulsaron, en octubre de 2011, la ley SOPA (Stop Online Piracy Act) ante el Congreso de Estados Unidos. En ese país, el paraíso de los *lobbies*, la ley SOPA proponía una pena máxima de cinco años de cárcel por cada diez canciones o películas descargadas. También que se bloqueara la financiación de sitios, sin probar delito, tal como le pasó a WikiLeaks cuando empresas como Visa o MasterCard le cortaron los fondos.

En Argentina, las guerras por el *copyright* y la cultura se dieron con otros casos muy resonados en la prensa, como los de Taringa, Cuevana y la plataforma colectiva de películas Popcorn Time (que recoge datos de intercambios de archivos *torrent*) y del sitio The Pirate Bay (sus direcciones IP locales). Los litigios fueron impulsados por la industria del entretenimiento y los autores locales, nucleados en Sadaic, Capif, Argentores y la Cámara Argentina del Libro. En el caso de Taringa, el segundo sitio de intercambio social más visitado de la Argentina después de Facebook, el 6 de mayo de 2011, la Cámara Nacional de Apelaciones en lo Criminal y Correccional envió a juicio a sus propietarios por supuesta infracción de

[129] Lars Ulrich, baterista de la banda Metallica, dijo sobre el juicio que siguieron contra el sitio de descargas: "Napster nos jodió, entonces nosotros los jodimos a ellos".

derechos de autor, argumentando que eran "partícipes necesarios" por las acciones que realizan los usuarios dentro de la página, fundamentalmente el intercambio de libros y manuales de computación protegidos por derechos editoriales. Tras dos años de juicio, los querellantes decidieron retirar la demanda, declarando: "Internet debe mantenerse como un espacio libre de censura, colocando el derecho a la libertad de expresión por sobre cualquier otro derecho social o económico". El portal de películas Cuevana también sufrió un cierre preventivo, en su caso por ofrecer series y películas de Warner, una de las empresas demandantes. Luego volvió a estar activo. Pero el debate siguió y continuará ante cada novedad que altere a la industria del entretenimiento[130].

La guerra del *copyright* fue la primera en dividir moralmente las aguas entre los "buenos y malos" de internet, que desde entonces fueron llamados despectivamente "piratas". Es también una de las guerras que ha tenido consecuencias fatales en la vida de algunas personas. Entre ellos, el programador y activista Aaron Swartz que, acusado por la justicia norteamericana por descargar documentos académicos, reseñas y publicaciones protegidas por leyes de derechos de autor de la base de datos JSTOR en el MIT, decidió terminar con su vida en enero de 2013. Swartz era un miembro destacado de la comunidad digital, no sólo como militante de la cultura libre, sino como programador que había realizado contribuciones destacadas, como el desarrollo de la primera versión del código XML, que aún permite compartir contenidos en internet. Perseguido por una demanda desmesurada, señalado por pertenecer al lado "del mal", se suicidó a los 26 años.

También, en esta guerra, Gottfrid Svartholm, Fredrik Neij y Peter Sunde, los fundadores del sitio sueco de descarga de archivos *torrent*

[130] En marzo de 2014, el director de cine argentino ganador de un Oscar, Juan José Campanella, atacó a la aplicación de películas Popcorn Time. "Te felicito Sebastián, creador de Popcorn Time. Sos un chorro argentino más en nuestro larga lista", dijo el cineasta desde tu cuenta de Twitter, generando una polémica que finalmente ayudó a publicitar el sitio, que en sus 6 primeros días de vida tuvo 150 mil descargas de la aplicación.

The Pirate Bay sufrieron consecuencias. Desde 2005, sus oficinas fueron allanadas, con la acusación de que allí se encontraba el centro de datos que alojaba contenidos ilegales (que estaban siendo compartidos por los usuarios). Luego de confiscar todos sus servidores, los tres administradores del sitio, que entonces tenían 22, 24 y 28 años, fueron arrestados y luego liberados. En protesta, 600 personas se manifestaron en las calles de Estocolmo y Gotemburgo. Al mes siguiente, el sitio estuvo de nuevo *online*. Pero en 2006 la justicia sueca inició un juicio en el que pidió un año de cárcel para los responsables de The Pirate Bay, acusados de piratería y violación a los derechos de autor. El tribunal los declaró culpables, les impuso un año de cárcel y una multa de casi un millón de dólares. Desde ese momento, el juicio continúa, con avances y retrocesos, los dueños del sitio continúan enfrentando detenciones y la página (y sus réplicas en el mundo) sigue siendo dada de baja periódicamente en distintos países (entre ellos Argentina) por violar derechos de autor.

La lucha entre los innovadores que lanzan al mercado nuevas tecnologías que habilitan la copia y los titulares de derechos de *copyright* es parte de una larga historia de tensiones que suma capítulos cada vez que las tecnologías corren límites[131]. El problema es que la historia del arte, la cultura, pero también de la innovación, siempre creció en base a desarrollos e ideas anteriores. Y a "los nuevos" siempre se los llamó piratas y se los acusó de piratería, es decir, de robar. Como señala el abogado y activista de internet Lawrence Lessig: "Si la piratería significa usar la propiedad creativa de otros sin su permiso, si lo de 'si hay valor, hay derecho' es verdad, entonces la historia de la industria de contenidos es una historia de piratería. Cada uno de los sectores importantes de los grandes medios

[131] El concepto, de Jane Ginsburg (2001), está desarrollado en detalle en el artículo "Libertad de expresión, cultura digital y derechos de autor", de Beatriz Busaniche, en *Cuestión de Derechos* Nº 4, primer semestre de 2013: http://www.cuestiondederechos.org.ar/pdf/numero4/Articulo-3.pdf.

hoy día (el cine, los discos, la radio y la televisión por cable) nació de una forma de piratería, si es que la definimos así"[132].

Un argumento en contra de la copia es que se trata de un robo. Pero es fácilmente rebatible: a diferencia de un libro o una película en sus versiones físicas, en el caso de internet, copiar y distribuir una obra no implica tener un objeto menos para vender. Por supuesto, no se trata de que los autores o creadores no reciban una compensación por su trabajo, ni de estar a favor del robo. Sin embargo, Lessig advierte que una cosa es proteger los derechos de los autores y otra dañar a toda internet para proteger a una industria[133].

La historia después de Napster comprobó dos cosas: que quienes usan las redes para intercambiar distintos tipos de obras también son quienes más consumen cultura, y que la industria también encuentra otras formas de financiamiento y pago para la música y las películas. La cultura siempre estuvo y estará sustentada en el conocimiento, de lo nuevo y de lo clásico. Si miramos en nuestros muros de Facebook, *timelines* de Twitter o cuentas conectadas a servicios de música como Spotify, gran parte de lo que compartimos son formas del arte. El entretenimiento tiene en internet su mejor socio. Ningún fenómeno masivo hoy lo es sin la ayuda de la Red, la primera ventana por donde los artistas o las grandes empresas de entretenimientos muestran sus productos, con campañas millonarias y hasta "filtraciones" (planeadas, por supuesto) de películas o discos antes de que se lancen oficialmente. Pero los mismos artistas tardan en comprenderlo. Neil Gaiman, uno de los escritores de

[132] Lessig, Lawrence, *Cultura Libre*. Disponible en español en: https://www.derechosdigitales.org/culturalibre/.

[133] El académico diferencia cuatro tipos de usuarios que comparten contenidos en la Red: quienes la usan como sustituto de compra de contenidos (cuando sale un disco o una película, lo bajan en vez de comprarlo); los que usan la Red para "probar" la música antes de comprarla (y luego la compran o no); quienes la usan para acceder a materiales con *copyright* que ya no están a la venta o que no habrían comprado porque tienen un precio muy elevado fuera de internet; y los que usan el intercambio *online* para acceder a contenidos que no tienen directamente *copyright*.

ciencia ficción más vendidos del mundo, confesó: "Yo tenía la idea de que si subían mis cosas a la web me estaban pirateando. Hasta que me di cuenta de algo más importante: en los lugares donde los usuarios me pirateaban o traducían mis libros, vendía más. Porque me descubrían y querían comprar mi nuevo libro. Fue fascinante. Entonces puse mi libro *online* gratis por un mes. ¿Y saben lo que pasó? Las ventas aumentaron 300%. Por eso, la otra pregunta que les hago a mis amigos es: ¿Cuánto de lo que descubriste y después compraste en los últimos cinco años fue porque lo viste en internet?".

Por otro lado, la industria de la música y del cine también idearon otras formas de venta *online*, algunas más independientes y otras haciendo acuerdos con compañías discográficas, con estudios de televisión o con artistas independientes. Lo demuestran los casos más que exitosos de Netflix y Spotify, que ya son grandes empresas en sí mismas.

Más que hacer un favor a los artistas, la guerra por controlar lo que se comparte en internet le produce un gran perjuicio a una parte mucho más grande de la gente: la que usa la Red. El escritor, periodista y activista Cory Doctorow lo explica: "No hay una solución para el tema del *copyright online* sin que se dañe la salud de internet". Y argumenta: "Ser artista siempre fue un mal negocio. Estadísticamente, pueden vivir de ese trabajo unos pocos privilegiados, una fracción de 0,0000000000001%. ¿Cuál es el verdadero problema? Que las guerras del *copyright* erosionaron la resistencia de internet en un tiempo en que la Red se necesita desesperadamente. Hoy internet está integrada en nuestras vidas de maneras que sobrepasaron hasta los pronósticos más salvajes de 1980. Es la forma a través de la que inscribimos a los chicos en la escuela, pagamos el gas, publicamos videos de violencia policial, le mandamos dinero a nuestros familiares, reservamos vacaciones, escribimos un trabajo para la escuela, nos ganamos la vida, hacemos las compras y todas las otras actividades de nuestra vida pública". Doctorow destaca que todas estas actividades de la vida diaria funcionan "dentro de internet", por lo tanto, ya no puede determinarse la libertad y el control por parte de empresas privadas, porque es un espacio público esencial de nuestras vidas. Su idea central es:

no tiremos la bomba atómica para resolver un problema del tamaño de una hormiga. Porque la Red es más que entretenimiento. Es nuestra vida.

¿Cuál es entonces la solución para esta guerra? La respuesta de Doctorow es precisa, contundente: "La misma solución que necesitamos para la regulación de la prensa, para la guerra contra el terrorismo, para las guerras contra la vigilancia, para las guerras contra la pornografía: entender que internet es el sistema nervioso de la era de la información y que preservar su integridad y su libertad de la vigilancia, la censura y el control es el primer paso esencial para asegurarnos otras metas"[134].

La guerra de los datos

Privacidad y vigilancia: huellas digitales, gobiernos y empresas

La quinta guerra afecta nuestra privacidad. Su base es una combinación compleja de posibilidades técnicas, codicias económicas y la necesidad creciente de "seguridad" en un mundo a veces más amenazado o simplemente menos predecible. Su consecuencia es que estamos perdiendo, cediendo o dejando en manos de otros (empresas, gobiernos, otros usuarios) gran parte de nuestra información privada.

En el mundo hay 1,5 mil millones de computadoras y en 2014 se vendió ese mismo número de dispositivos móviles. Los aparatos son tan vitales en nuestra vida que ya no sólo enloquecemos si nos olvidamos el celular al salir de nuestra casa: no podemos siquiera estar adentro de ella sin llevar la conexión con nosotros en todo momento. Vamos al baño con el celular, lo llevamos para ver videos o chatear desde la cama, *trackeamos* desde nuestro consumo de calorías hasta los kilómetros que caminamos en la semana, le preguntamos a Google en voz alta dónde queda tal negocio mientras vamos por la calle, dejamos registro de cada búsqueda, palabra e información en nuestros buscadores. Cada una de

[134] Doctorow, Cory. "Copyright wars are damaging the health of the internet", *The Guardian*, 28 de marzo de 2013.

esas actividades va dejando una huella. Debido a la arquitectura de internet, la información se copia muchas veces hasta llegar a su destino y pasa por muchos "lugares", donde van quedando partes de ella. Pero, al contrario de las migas de pan que dejan Hansel y Gretel para marcar su camino de vuelta, las huellas que dejamos *online* no son siempre voluntarias. Para preservar nuestros datos personales de terceros, buena parte de la información que circula en la Red está encriptada. Pero, aún así, hay otra que no lo está, otra a la que puede accederse igual, otra que cedemos voluntariamente y otra que simplemente no consentimos compartir pero que igual se comparte.

Las amenazas a la privacidad de nuestros datos provienen de distintos actores, con objetivos diversos, por lo que es casi imposible determinar un sólo "responsable". El primer grupo de amenazas proviene de motivos económicos: las empresas que se valen de los datos que les dejamos voluntaria o involuntariamente en nuestro uso cotidiano, para luego vendernos cosas. El segundo grupo tiene que ver con el avance de la tecnología, a la que confiamos voluntariamente ciertos procesos para hacernos la vida más fácil: sería ridículo perder tiempo en ir a un negocio a comprar un producto si podemos tenerlo a un clic, hacer la fila para pagar un impuesto o hacer una transferencia si lo podemos hacer *online*, o perder dos horas para sacar un turno en una dependencia púbica si podemos resolverlo en un minuto en una página web; también, sería necio que si existen formas de comunicarnos con otras personas que están lejos a través de un programa sencillo lo evitemos, o que no usemos incluso algunos servicios de citas de internet si nos resultan una buena opción. El tercer grupo de amenazas se relaciona con la intromisión que realizan los Estados, ya sea porque realizan un espionaje abierto contra sus ciudadanos, porque cumplen con funciones legítimas pero a través de métodos que violan otros derechos, o porque eligen herramientas inadecuadas o excesivas para proteger la seguridad.

Cuando se habla de la pérdida de privacidad a causa de la tecnología, caemos en dos extremos. El primero es darle una confianza ciega como solución a todos los problemas. El segundo es temerle hasta la

paranoia en su capacidad de entrometerse en nuestra vida. Sin embargo, ni internet ni la tecnología son —todavía— máquinas autogobernadas para actuar en contra de los humanos. Hay algo cierto: la pérdida de la privacidad es y será inevitable. Pero, antes de darnos por vencidos, es posible comprender en manos de quién están las responsabilidades y qué herramientas tenemos en nuestras manos como ciudadanos para defendernos. Porque en internet, además de consumidores, también podemos ser ciudadanos.

¿Ciudadanos o consumidores?

Internet creció en etapas y, con el tiempo, se sofisticó: permitió que los sitios tuvieran imágenes, audio, videos, contenidos interactivos. Con esto, la Red también se masificó y llegó a la vida cotidiana, con sitios de noticias, entretenimientos, luego foros, blogs, clasificados y hasta redes sociales[135]. Pero con su avance, también necesitó construir un modelo de negocios, una forma de financiar ese gran mercado universal donde se crean y comparten contenidos. Ese modelo fue —y sigue siendo— la publicidad. Ese sustento económico fue también su riesgo futuro.

"Queríamos construir una herramienta fácil para todo el mundo, para compartir conocimientos, opiniones, ideas y fotos de gatitos lindos"[136], explica Ethan Zuckerman, profesor del MIT, activista de internet y ex fundador de Tripod.com, una de las primeras (y entonces pocas)

[135] La web como la conocemos —gran espacio universal donde se crean y comparten contenidos minuto a minuto— existe como tal desde hace unos diez años. Los blogs y las redes sociales como Facebook y Twitter tienen menos años de los que imaginamos: los primeros tuvieron su año de gloria en 2008 y las grandes redes sociales tuvieron su momento de gran expansión hacia 2010.

[136] "Internet's original sin", publicado en *The Atlantic* el 14 de agosto de 2014: theatln.tc/1sZ4DZW.

empresas exitosas de la llamada "burbuja puntocom"[137]. Sin embargo, dice con autocrítica: con el tiempo las compañías de la Red necesitaron (y pudieron, gracias a la tecnología) recabar cada vez más información de los usuarios para "*targuetizar*" mejor los avisos. En otras palabras: si el software y los algoritmos le permiten a las empresas conocer cada movimiento de quienes visitan un sitio, cada clic que realizan, cómo navegan, qué temas, productos y servicios les interesan, lo van a usar en su beneficio, para generar una serie de ofertas acordes para cada consumidor y maximizar las posibilidades de venta. El modelo de las empresas es utilizar bases de datos cada vez más personalizadas con las preferencias de los usuarios, que les permiten ofrecer lo que cada persona quiere. Con exactitud científica y a un solo clic de esfuerzo.

Sin embargo, pasado el momento de la comodidad del consumo, el modelo de negocios de internet basado en la publicidad y la recolección permanente de datos pone en riesgo nuestra privacidad. Nos convierte en usuarios vigilados. Nos transforma en productos: valemos lo que valen nuestros datos, como dice la repetida frase "el producto sos vos" o "nada es gratis en internet, porque se paga con tus datos". El problema es que esos datos valen muy poco, comparados con los derechos que perdemos en el camino.

Para Zuckerman, éste es el gran pecado original de la Red. ¿La razón? No hay forma de que una internet basada en la publicidad, en recabar crecientemente más datos de los usuarios para venderles productos y servicios, funcione sin niveles de vigilancia cada vez más detallados de cada acción de los usuarios. Los buscadores *online*, las redes sociales y los sitios de comercio electrónico crean herramientas progresivamente más sofisticadas para saber qué buscan, cliquean y compran cada segundo que

[137] La "burbuja puntocom" fue un período, entre 1997 y 2001, donde se fundaron, crecieron y alcanzaron grandes niveles de rentabilidad en la bolsa de valores de una serie de compañías de la entonces "nueva" internet. Sin embargo, luego del rápido crecimiento y ganancias, muchas de esas empresas quebraron o cerraron, y, aunque no llegaron a provocar una crisis económica, marcaron un período de recesión en la economía internacional y una etapa de crecimiento más moderado en las empresas de internet.

están conectados. También sostienen departamentos de investigación y *Big data* que construyen perfiles minuciosos ("*targets*") de los usuarios/consumidores. "La publicidad sin vigilancia es posible, pero es difícil de imaginar. Porque el principal beneficio de la publicidad *online* es la habilidad para ver quién está viendo un aviso", advierte Zuckerman.

Con el tiempo como usuarios y con la multiplicación de internet para todo tipo de operaciones y compras *online*, también nos vamos dando cuenta de cómo funciona este mecanismo de intercambiar comodidad y rapidez por privacidad. Sabemos, o al menos nos damos cuenta, de que cada clic que realizamos en una publicidad implica una ganancia para alguna empresa de la web o que nos llegan o vemos ofertas cada vez más personalizadas para nuestro perfil de consumo. En cierto punto, sabemos que nuestras acciones están siendo "vistas" y "esperamos" que se nos vigile. Sin embargo, muchos todavía no son conscientes de cómo funcionan estos mecanismos y el cuidado de la privacidad todavía es una batalla perdida frente a la "comodidad" de usar la web tal como se nos presenta: dar aceptar a todas las condiciones de uso de sitios y dispositivos, navegar, buscar y comprar rápido y fácil, y olvidar (o más bien, ignorar a sabiendas) las consecuencias de nuestras acciones. El experto en seguridad informática finlandés Mikko Hypponen lo resume así: "Somos brutalmente honestos con nuestros motores de búsqueda. Somos más honestos con ellos que con nuestras familias. Los motores de búsqueda saben más de ti que tu familia"[138].

La investigadora norteamericana Rebecca MacKinnon explica este mecanismo de la era digital como "el consenso de los conectados", es decir, todos los problemas que preferimos no ver a cambio del "beneficio mayor" de utilizar las posibilidades de la web: comunicarnos, hacer amigos, comprar, opinar, apoyar una causa social o política, encontrar el amor, todo rápido con un clic. Para realizar cada una de esas acciones mudamos nuestra vida a plataformas digitales, servicios y dispositivos

[138] Mikko Hypponen: How the NSA betrayed the world's trust, charla TED, http://bit.ly/1ChbT9N.

que hoy mediatizan todas nuestras relaciones. Y el problema, dice MacKinnon, es que esos espacios digitales van ganando un creciente poder, pero, al contrario del control que le reclamamos a otros espacios públicos de nuestras vidas (el barrio, la ciudad, el país, una escuela o un aeropuerto) todavía no nos ocupamos demasiado del poder que le damos a la nueva esfera *online*. "En nuestra dependencia, tenemos un problema: entendemos cómo funciona el poder en el mundo físico, pero todavía no tenemos un entendimiento claro de cómo funciona el poder en la esfera digital"[139], explica la académica. "La realidad es que las corporaciones y gobiernos que construyen, operan y gobiernan el ciberespacio no están siendo lo suficientemente responsables de su ejercicio de poder sobre las vidas y las identidades de la gente que usa las redes digitales. Hay soberanías operando sin el consenso de los que están conectados"[140].

En favor de los usuarios, en este caso también consumidores, ya existen (en cada país y en algunos continentes como Europa) leyes que van regulando el uso de los datos personales en internet y defendiendo a las personas de los abusos por parte de las empresas. La razón es que internet cada vez ocupa un espacio más grande en nuestra vida, como un nuevo espacio "público" donde todos interactuamos. Sin embargo, cada espacio de la web se rige por "leyes" de empresas privadas: los términos y las condiciones de las redes sociales o de los sitios de comercio electrónico, las fórmulas o los algoritmos de los buscadores (el software, o lo que está programado, también es una forma de ley que determina qué datos se retendrán de nosotros, por ejemplo), la forma en que operan las "cookies" (pequeñas piezas de información que sirven para identificar los rastros del usuario) en los sitios, entre otras leyes del ciberespacio. Como los usuarios también son ciudadanos, existen leyes de tratamiento de datos personales para regular su uso.

Un gran riesgo que deberá definir esta guerra es si el ecosistema de internet será cada vez más privado, al punto de que para conservar

[139] Rebecca MacKinnon, *Consent of the Networked*, Basic Books, 2012, p. 13.
[140] Rebecca MacKinnon, *op. cit.*, p. 23.

la intimidad debamos pagar. Algunos ya lo señalan: la privacidad, en el futuro, será un bien más de cambio, si no nos ocupamos hoy de que las leyes del mercado no la tomen en sus manos.

Ciudadanos espiados y controlados

Las empresas no son las únicas que aprovechan la tecnología para intervenir en la vida de la gente. Los gobiernos —de países, pero también de ciudades de todo tamaño— también se valen de la interconexión total de nuestras vidas para espiar a sus ciudadanos y ejercer un control ya no sólo de sus acciones, sino también de sus cuerpos. En efecto, el uso de la tecnología por parte de los gobiernos a veces se realiza con resultados positivos: ayuda a protegernos o está al servicio de procesos más eficientes, fáciles o rápidos en el Estado. Otras veces, la vigilancia o el espionaje son necesarios: para atrapar un asesino, un narcotraficante, evitar un abuso a un menor o el intento de poner una bomba en una escuela. Sin embargo, en otros casos, en nombre de vivir más seguros o modernizar nuestras vidas, se violan los derechos de los ciudadanos en el mundo digital.

No solemos pensarlo, pero en cada dispositivo que usamos o llevamos con nosotros, tenemos un arma de vigilancia. Los datos que circulan en los aparatos (cuando mandamos un mail, usamos una aplicación, hacemos una llamada, chateamos, publicamos una actualización en Facebook, una foto en Instagram o una frase en Twitter) pueden interceptarse, leerse y controlarse. Lo demostraron las revelaciones de Edward Snowden en 2013: desde Estados Unidos, la NSA accedía a la información de ciudadanos de todo el mundo. Lo hacía habilitada por su ley de seguridad nacional, que le permite espiar a los extranjeros cuando sus conexiones o datos entren en su país o pasen por él. El problema, como señala el informático Mikko Hypponen, "es que todos somos extranjeros, el 96% del planeta es extranjero", porque las infraestructuras de internet pasan por el territorio de Estados Unidos.

Intervenir en "los cables", los "caños" o los datos es una de las formas

de la vigilancia. Para hacerlo, se necesita de la cooperación de las empresas por donde circula la información, tal como Snowden demostró en su denuncia. Otra forma de lograrlo (la legal) es pedir a las compañías privadas que entreguen los dados de los usuarios con una orden legal. Pero eso no siempre sucede, como quedó demostrado en que la NSA y su par inglesa intervinieron también las redes privadas que conectan los centros de datos de Google y Yahoo en todo el mundo[141]. Quedó así claro que la intención no sólo era buscar la información de casos puntuales que pusieran en riesgo la seguridad nacional, sino un mecanismo complejo de vigilancia generalizada y masiva, cuyas víctimas son todos los ciudadanos del mundo. La propia infraestructura de la NSA lo demuestra: "El centro de datos de la NSA en Utah es cinco veces más grande que la tienda más extensa de muebles Ikea. Son 140 mil metros cuadrados que albergan supercomputadoras y *datacenter*s que gastan decenas de millones de dólares al año en electricidad, capaces de guardar información prácticamente para siempre", señala Hypponen.

Cuando estalló el escándalo de la NSA, un comentario común fue "bueno, pero ya sabíamos que nos espiaban". Es cierto: suponíamos que sucedía. Pero tal vez lo más impactante fue confirmar la cooperación entre los gobiernos y las empresas con el objetivo de espiar. "Es como que se puedan meter en los códigos de las alarmas de todas las casas del mundo porque en algunas de las casas viven algunos tipos malos", explica Hypponen. Otro argumento fue que otros países también espiaban a su vez a Estados Unidos o a sus propios ciudadanos. También es cierto. "Pero la realidad es que no es equilibrado. Si Estados Unidos tiene derecho a espiar todas las comunicaciones que pasen por su territorio, entonces tiene derecho a espiar todo, porque todos de alguna forma usamos Windows, Skype, Dropbox, Linkedin, webmails y servicios en la nube. Si todos los servicios están en Estados Unidos, ellos tienen la ventaja de espiarnos. Los suecos usan los servicios de empresas estadounidenses, pero los estadounidenses no usan los servicios suecos".

[141] ¿Cómo nos vigilan en internet?, Fundación Karisma, http://bit.ly/1Hlu4hH.

El argumento que esgrime la NSA para defender sus operaciones es la lucha contra el terrorismo. Sin embargo, expertos y organismos internacionales advierten que, en nombre de combatir ese mal, se están violando otros derechos fundamentales, empezando por las convenciones de derechos humanos internacionales y las constituciones de cada país, que consagran el derecho a la privacidad como base de la democracia. En mayo de 2014, más de 400 de organizaciones del mundo presentaron los "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones"[142], un documento que explica "cómo aplicar el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y de los cambios que están teniendo las tecnologías y técnicas de vigilancia de las comunicaciones". En el mismo, señalan que la intimidad es un derecho humano fundamental, porque si no estamos seguros de que no estamos siendo vigilados, es probable que no nos expresemos libremente, que no consultemos ciertos medios o que no nos reunamos con otras personas o protestemos contra algo que consideramos injusto. Por eso, la vigilancia de las comunicaciones sólo se justifica cuando es prescrita por ley, es necesaria para lograr un objetivo legítimo y es proporcional al objetivo perseguido. Siempre debe precederse de estas preguntas: ¿existe una causa que justifique invadir la intimidad de esta persona[143]?, ¿es proporcional respecto de lo que se busca (por ejemplo: no es necesario espiar masivamente a todo un grupo ante la sospecha de un delito de una persona[144]?

[142] En: https://es.necessaryandproportionate.org/text.

[143] "Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición", se señala en el documento Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

[144] Por ejemplo: no es necesario vigilar a todos los de un grupo o un país ante la posibilidad del delito de una persona. También el documento establece que sólo debe realizarse cuando se hayan agotado otras instancias menos intrusivas, y que "cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con

Las organizaciones advirtieron además en su documento sobre el gran crecimiento no sólo del espionaje, sino también de la información que guardan los Estados y los privados: "La frecuencia con la que los Estados procuran acceder tanto al contenido de las comunicaciones como a los metadatos de las comunicaciones aumenta drásticamente, sin controles adecuados". El riesgo, escriben, es que esa gran cantidad de datos se conviertan en perfiles de los ciudadanos, "a partir de sus condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones".

A partir de este riesgo creciente, que se repite sin excepción en todos los países del mundo, los Estados también han ido dictando normas para proteger los datos personales de los ciudadanos. En la Argentina, la ley 25.326 de Protección de Datos Personales[145], sancionada en el año 2000, se encarga de proteger esta información asentada en archivos, registros, bancos de datos, públicos o privados, y cuenta con un órgano de control para hacer cumplir dicha ley: la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia de la Nación. En la Ciudad Autónoma de Buenos Aires, desde 2005, existe una ley similar (la 1.845[146]) y un organismo que se ocupa de tutelar a los vecinos en caso de violaciones a ésta, el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires[147]. Otros países, ciudades y regiones del mundo (como la Unión Europea) también cuentan con normas y organismos de defensa.

Sin embargo, muchas veces existe una "gobernanza" de facto por parte de las empresas a quien confiamos nuestros datos, que tienen sus propias leyes (términos y condiciones de uso) que los usuarios aceptan,

prontitud", y que "la información será accesada sólo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización", entre otras cosas.

[145] Consultar la ley en http://bit.ly/datosperson.

[146] Consultar la ley en http://www.protecciondedatos.com.ar/ley1845.htm.

[147] http://www.cpdp.gob.ar/.

quedando sus derechos en manos de esas legislaciones y tribunales que ni siquiera están en sus países. En ese punto volvemos al viejo problema: si la mayoría de los servicios web que utilizamos tienen su sede en empresas estadounidenses, estaremos finalmente sometidos a esa ley. Sin embargo, también hay antídotos que se pueden aplicar contra esa situación: usar programas de código abierto, seguros, comunicaciones encriptadas, tratar de salir de los servicios residentes en Estados Unidos. Es un camino que requiere informarse, leer los términos y las condiciones con los que se maneja nuestra información y aprender ciertas herramientas técnicas. En síntesis: demanda que entendamos más la tecnología. Pero, hoy, si no lo hacemos, estaremos dejando nuestras vidas digitales en manos de otros; será como no haber leído la Constitución o como no comprender cuáles son nuestros derechos.

En los países de América Latina, además del terrorismo, existe otra excusa para intervenir en la intimidad de los ciudadanos: la inseguridad. Para combatir esta amenaza, los gobiernos de todo signo político están invirtiendo presupuestos millonarios en armarse con cámaras y centros de operaciones donde pueden ver, en tiempo real, qué hacen sus ciudadanos. Repletos de camaritas, funcionan las 24 horas como Ministerios de la Verdad, como panópticos de ciudades que se pueblan con ojos electrónicos que no vemos, aunque sabemos que están. Pero las imágenes no sólo son usadas por los gobiernos, sino que también son fuente de horas interminables de materiales para noticieros y canales de televisión que usan lo que se capta en la vía pública para mostrarlo a quien quiera verlo. De esa forma, el círculo de los medios que muestran ciudades inseguras se retroalimenta con ciudadanos que demandan más seguridad y Estados que entonces llenan los techos con cámaras, porque "la gente lo pide". El problema es que esas imágenes no siempre son tratadas con los requisitos legales y de respeto de derechos humanos establecidos por los tratados internacionales que la mayoría de los países deberían cumplir.

Quedan cada vez menos espacios libres en las ciudades sin vigilar. Basta con mirar hacia arriba en cualquier calle y ver cómo las cámaras nos filman. Las instalan las ciudades, los gobiernos nacionales o municipales. Lo hacen sin preguntar, alentados por el "reclamo ciudadano" de más seguridad. Si vivimos en Buenos Aires, los porteños convivimos con más tres mil cámaras distribuidas en distintos barrios, es decir, una cámara cada mil habitantes. En el resto del país, cada provincia y municipio avanza con sus propios programas de vigilancia. También lo hacen los sistemas privados, con circuitos cerrados de televisión en shoppings y edificios, y en una creciente cantidad espacios públicos como plazas, escuelas, hospitales y aeropuertos. Sin embargo, todavía no existen estadísticas que confirmen que vivir rodeados de cámaras reduzca efectivamente el delito en general.

En ese intercambio, también vamos perdiendo privacidad. Muchas veces, incluso, lo aceptamos. Otras veces, también somos responsables, cuando la tecnología nos convierte en policías del otro: queremos saber a qué hora se conectó, qué foto subió, con quién habló. Como escribe Julian Assange: "No sólo vivimos en un estado de vigilancia; también vivimos en una sociedad de vigilancia. La vigilancia totalitaria no está sólo encarnada en nuestros gobiernos; está incrustada en nuestra economía, en nuestros usos mundanos de la tecnología, en nuestras interacciones diarias"[148]. La naturaleza misma de internet y la tecnología permite la vigilancia. Por eso, prestarle atención a la privacidad es relevante.

"Yo no tengo nada que esconder": ése es un argumento común de quienes no se preocupan por la privacidad o de quienes honestamente no sienten que tienen que protegerla. También lo utilizan las empresas o gobiernos para justificar sus prácticas de vigilancia diciendo que sólo observan a quienes cometen delitos. Pero, si la información no tuviera ningún valor, ¿por qué es tan importante para empresas como Google o para los gobiernos? La razón es que sí es valiosa, ya sea con objetivos comerciales o con otros relacionados a la vigilancia estatal. En *Nada que*

[148] "Who should own the internet?", Julian Assange, *The New York Times*, 4 de diciembre de 2014. http://nyti.ms/1yUMFe4

esconder. El falso intercambio entre privacidad y seguridad[149], el profesor de derecho de la Universidad de Washington Daniel Solove señala que ese argumento es el más utilizado, justamente, por quienes violan la privacidad. Supone que si no hicimos nada malo no deberíamos temer, con lo cual nos supone previamente culpables y nos genera una culpa si no admitimos "cooperar" con quienes quieren "saber" sobre nosotros.

Solove ofrece varios argumentos para responder contra esa presión. El primero: "¿Por qué deberíamos justificar cada acto previamente? Yo no tengo nada que justificar. En todo caso, si tienen algo que me incrimine, vuelvan con una orden judicial". El segundo: "No tengo nada que esconder, pero tampoco tengo nada que quiera compartir con usted". El tercero: "Si no tenés nada que esconder, entonces no tenés una vida". El cuarto: "Mostrame lo tuyo, entonces te muestro lo mío". El quinto: "No se trata de tener algo que esconder, sino de no formar parte del negocio de otro". Solove dice que las razones podrían seguir hasta el infinito, porque la privacidad es tan compleja que está en cada acción de nuestras vidas. Si no, no tendríamos cortinas en las ventanas, iríamos desnudos por la calle o no nos molestaría que alguien lea nuestros mails. Pero la verdad es que si eso nos sucede, nos enojamos. Que la tecnología esconda la vigilancia no significa que ella no exista. O, como dice otra frase famosa: "Que yo no sea paranoico no significa que no me estén vigilando".

Los argumentos anteriores tienen que ver con lo individual. Pero la privacidad también es un derecho colectivo. Y allí reside otra de sus dimensiones más importantes. Incluso cuando no nos preocupe mantener nuestra intimidad, ella tiene un valor fundamental para la democracia. Como decíamos, es un valor en sí, porque permite la libertad, desde el pensamiento hasta la protesta. Nos permite ser iguales, al menos para expresarnos. Por eso, cada vez que admitimos dejarla en manos o no pedir su debido control a empresas o a gobiernos, también estamos dañando la libertad de toda la sociedad. Si hoy no nos importa que se

[149] *Nothing to hide. The false trade off between privacy and security*, Yale University Press, Estados Unidos, 2011.

espíen las comunicaciones de un político o un periodista con el que no acordamos, permitirlo también es abrir la posibilidad de que mañana se espíe a cualquier otro, incluidos nosotros. Si mañana hay un golpe de Estado o nuestro país se convierte en una dictadura, y no defendemos hoy nuestra privacidad, cualquier parte de nuestra información puede ser utilizada para encarcelarnos, porque sí, porque a alguien no le gustó lo que dijimos. Ese es el riesgo de la "justicia selectiva": todos tenemos información que puede ser usada en nuestra contra. Aún más los activistas políticos, los periodistas, o cualquier ciudadano que participe en la vida pública.

Ante estos riesgos, todavía estamos a tiempo de protegernos, de cuidar y reclamar nuestra privacidad, y de pedir a gobiernos y empresas que la respeten. Para eso, primero es necesario conocer quiénes y cómo nos vigilan, cómo nos espían y qué hacen con nuestros datos.