Este artículo es copia fiel del publicado en la revista Nueva Sociedad Nº 269,
mayo-junio de 2017, ISSN: 0251-3552, <www.nuso.org>.

La trampa del «Nada que ocultar»

Democracia, capitalismo y privacidad

Las críticas al uso masivo de servicios digitales fuertemente centralizados y de sus bases de datos gigantescas suelen despertar una respuesta unívoca: no tengo nada que ocultar. A punto tal que esta frase se convirtió en un ya viejo y conocido desafío argumental, según el cual solamente quienes realizan actividades ilícitas podrían tener alguna objeción respecto a que se guarde un registro de todas sus actividades digitales. Esta frase también implica la aceptación tácita de los nuevos modelos de negocio de los servicios web y la negación de la relevancia de los problemas políticos involucrados. Por eso vale la pena detenernos en los contraargumentos y en las estrategias que conllevan.

Lucas Domínguez Rubio

Continuamente, quienes piensan los problemas de la privacidad en internet dicen algo respecto al «Nada que ocultar», de manera que se estableció todo un género de intervenciones para intentar desactivarlo a través de blogs, charlas y libros. ¿Existe una respuesta categórica y concluyente? Claramente, no. Analizar los distintos contraargumentos propuestos

Lucas Domínguez Rubio: es licenciado en Filosofía y becario doctoral del Consejo Nacional de Investigaciones Científicas y Técnicas (Conicet) de Argentina, en el Centro de Documentación e Investigación de la Cultura de Izquierdas (cedinci).
Palabras claves: democracia, encriptación, internet, políticas de software, privacidad.
Nota: durante su desarrollo, este trabajo fue presentado por el autor junto con Ramiro Uviña en el Festival Latinoamericano de Instalación de Software Libre (flisol) 2016 y en el iv Simposio de la Red Latinoamericana de Vigilancia, Tecnología y Sociedad (lavits), Buenos Aires, 21 a 23 de noviembre de 2016.

en intervenciones tanto periodísticas como académicas permite evaluar sus supuestos, alcances, límites y similitudes, como así también a quiénes se dirigen y qué cambios buscan lograr.

Con este objetivo, las páginas siguientes recorren los contraargumentos utilizados por los principales referentes sobre estos temas. Como marca común, todos ellos han buscado responder al «Nada que ocultar» revalorizando de distintas formas la idea de privacidad. En buena medida, esto se debe a que el desafío ya está planteado de este modo por la misma pregunta que contiene. Y, de hecho, este ha sido el enfoque desarrollado, entre otros, por el principal referente académico sobre el tema, Daniel Solove.

Nada que ocultar / *Nothing to hide* / *Rien à cacher*

En sus distintas formas, el argumento «Nada que ocultar» sostiene que los programas de acumulación masiva de datos no constituyen un serio problema social ni personal. El argumento toma la forma de un dilema: si estos programas descubren actividades ilegales, cumplen su objetivo, ya que la persona que comete tales actividades no tiene derecho a mantenerlas en privado. Mientras tanto, quienes no usen las distintas plataformas para llevar a cabo actividades ilícitas no deberían tener inconveniente en que su información inocua sea filtrada sistemáticamente.

Actualmente, más de 80% del tráfico de internet pasa por los servidores de cinco corporaciones estadounidenses. Estas empresas generan bases de datos y análisis de manera despersonalizada con fines comerciales para, entre otras cosas, brindar servicios de publicidad dirigida. Como sostiene la hipótesis vigente, se trata del nuevo modo de acumulación de capital propio de lo que va del siglo XXI. Este nuevo capital tiene su origen en el tiempo mismo de las actividades laborales y recreativas de todos los usuarios de plataformas digitales, quienes producen información permanentemente de manera espontánea y se transforman así –sin ningún gasto de tiempo extra– en una suerte de *data-entry* colaterales, a cambio de los servicios «gratuitos» que necesitan. Resultaría ya ocioso detallar la cantidad de rastros digitales que dejamos en nuestras actividades cotidianas.

Aparentemente, se trata de una situación en la que todos ganan (*win-win*). Por un lado, hay un ofrecimiento implícito de servicios de calidad a cambio de la información recolectada por cada perfil de usuario. Por otro lado, estas bases de datos brindarían mejores herramientas para luchar contra el terrorismo, la

pornografía ilegal o el narcotráfico. Con lo cual, el «Nada que ocultar» se torna más sólido de lo que parece. No solo no es perjudicial, sino que además genera varios beneficios para el propio usuario. Aunque, así y todo, según la legislación de varios países, esta comercialización de datos y metadatos también toma muchas veces un cauce clandestino e ilícito.

El *big data* no trata información considerada privada y, en teoría, solo procesa datos de manera impersonal ■

La clave del asunto radica en que, *por default*, el *big data* no trata información considerada privada y, en teoría, solo procesa datos de manera impersonal. Y, también en teoría, solo se enfoca en un determinado individuo ante un pedido judicial, mientras que, en la práctica, también puede acceder a esa información quien pueda comprarla. Como está demostrado, en estos casos esa acumulación de datos se personaliza de una manera increíblemente minuciosa. En este contexto, ¿por qué resulta central el argumento conocido como «Nada que ocultar»? De manera preliminar, al menos determinamos tres motivos.

En primer lugar, porque efectivamente funciona de manera tácita. Abrir el interrogante pone en discusión el uso cotidiano que se hace de internet. En rigor, puede pensarse que no se trata de un argumento, sino más bien de un supuesto adoptado de manera implícita por prácticamente todos los usuarios de internet. Desde el principio de la década de 2000, la cuestión quedó planteada como un problema entre la seguridad nacional y la privacidad personal. Y ya hace años el asunto se estableció como la aceptación de manera tácita de una determinada relación entre comodidad o usabilidad versus privacidad.

¿Tantas contraseñas para resguardar datos que no le importan a nadie? La verdad es que son cansadoras y resguardan información de escaso valor. La calidad del contenido compartido no amerita mayores esfuerzos. Además, los servicios de uso masivo son por lejos los más fáciles de usar y los más eficientes. Por esto, tematizar el «Nada que ocultar» implica problematizar una serie de implicancias de los términos y condiciones de los servicios digitales utilizados que aceptamos sin mirar.

En segundo lugar, cuando hoy en día alguien habla sobre por qué importa la privacidad, en algún momento tiene que cuestionar el «Nada que ocultar». A punto tal que varios periodistas, académicos y activistas establecieron todo un género de respuestas a través de blogs, charlas y libros a cargo de, por ejemplo, Julian Assange, Jakob Appelbaum, Jérémie Zimmerman, Glenn Greenwald,

Daniel Solove, Marta Peirano y Natalia Zuazo, entre otros. Quienes lo enfrentaron suelen mostrarse convencidos de sus argumentos, aunque no haya habido mayores modificaciones en las prácticas generales.

Tercero: sucede que una buena respuesta al «Nada que ocultar» constituye al mismo tiempo un argumento a favor de usar de manera cotidiana software libre, herramientas de encriptación o determinados servicios de internet y no otros. Por esto, sofisticar estos contraargumentos involucra pensar cómo darles más difusión a las luchas llevadas a cabo por los activistas de la criptografía, el software libre y la conformación de redes descentralizadas. Y la pregunta por el «Nada que ocultar» involucra también otros interrogantes: ¿sería conveniente utilizar sistemáticamente herramientas de encriptación para nuestras comunicaciones diarias? ¿Por qué? ¿O software libre? ¿O servicios de internet descentralizados?

¿Sería conveniente utilizar sistemáticamente herramientas de encriptación para nuestras comunicaciones diarias? ¿Por qué?

Una sensibilidad liberal-libertaria: objetivos y alcances de los contraargumentos

Como señalamos, muchos referentes en esta clase de temas (Jérémie Zimmermann, Jakob Appelbaum, Richard Stallman), protagonistas de procesos en curso (Julian Assange, Edward Snowden), periodistas (Glenn Greenwald, Natalia Zuazo, Marta Peirano) y algunos académicos (Daniel Solove), entre otros, han atacado el llamado «Nada que ocultar». Al recorrer sus intervenciones, los contraargumentos se repiten a punto tal que han establecido un pequeño canon.

Hay que señalar que muchas de estas intervenciones surgieron de entrevistas, charlas TED y videos disponibles en internet. Es decir: se trata de material de divulgación que sus autores pensaron con el objetivo principal de lograr alcance y difusión.

a) Por ejemplo, una de las primeras respuestas que surgen afirman cosas como «Si no tienes nada que ocultar, ¿para qué usas cortinas en tu casa?»[1]. O: «Bueno,

1. V., por ejemplo, J. Zimmerman: «Rien à cacher», video, 2014, disponible en <https://archive.org/details/RienNCacherJrrJmieZimmermannEtLaParisienneLiberLeenglishSpanishHungarianSubtitles>.

entonces anótame en este papel todas tus contraseñas de redes sociales, correo electrónico, etc.»[2]. O también: «Si no tienes nada que ocultar, ¿por qué no dejas que pongan cámaras en el baño de tu casa, o en tu cuarto?»[3]. U otra muy habitual: «Es falso, todos tenemos algo que ocultar a alguien: a nuestros compañeros, a nuestros jefes, etc.»[4]. Desde esta perspectiva, se considera el argumento «fácilmente rebatible». Por un lado, como señaló Solove, todas estas intervenciones apuntan a combatir una versión exagerada del «Nada que ocultar». Por otro lado, con el objetivo de ampliar su poder persuasivo, apelan a despertar algo así como una sensibilidad liberal-libertaria, muy intuitiva, de espanto frente a una excesiva intromisión en la vida personal. Más allá de esto, es indudable que la solución no es tan obvia y estas son consideradas respuestas irreales que no cambian el comportamiento digital de nadie.

b) Una vez abandonadas estas respuestas, otro segundo conjunto de contraargumentos toma la forma de un experimento mental para preguntarse qué pasaría si todo tu historial-perfil digital de repente se viera bajo condiciones políticas adversas. Aquí aparecen los ejemplos típicos que refieren a experiencias concretas de militantes políticos en países de Oriente Medio[5]. O, sin ir tan lejos, situaciones habituales de peligro en las que por un error o mala suerte podrías verte involucrado, como sostiene Peirano: «Hay mil maneras de estar en el sitio equivocado en el momento equivocado»[6]. Por lo general, el problema con estos contraargumentos es que no consiguen convencer a un público que no solo se piensa en un sistema político estable, sino que habitualmente no se vería en peligro de caer en situaciones de riesgo político.

c) Otra táctica radica en limitar el destinatario del contraargumento y publicar algún manual de autodefensa para activistas o para periodistas, como si el público al que estuviese dirigido quedara de esta manera restringido, sin preguntarse por qué no ampliarlo, o por qué no deberían interesarse usuarios amplios con prácticas inocuas[7]. En buena medida, estas intervenciones no discuten las implicancias prácticas del «Nada que ocultar», sino que,

2. V., por ejemplo, G. Greenwald: «Why Privacy Matters», charla TED, 2014, <https://vimeo.com/108845353>.
3. V., por ejemplo, J. Zimmerman: ob. cit.
4. V., por ejemplo, «Richard Stallman Snowden & Assange Besieged By Empire But Not Defeated», entrevista, 2013, disponible en <https://archive.org/details/RichardStallmanSnowdenAssangeBesiegedByEmpireButNotDefeated>.
5. Por ejemplo, v. J. Appelbaum: «The Tor Project, Protecting Online Anonimity», charla TED, 2014, disponible en <https://archive.org/details/JacobAppelbaumAtTEDxFlanders>.
6. M. Peirano: «¿Por qué me vigilan, si no soy nadie?», charla TED, 2015, <https://archive.org/details/PorQuuMeVigilanSiNoSoyNadieiPorMartaPeiranoTEDxMadrid>.
7. Por ejemplo, M. Peirano: *El pequeño libro rojo del activista en la red*, Roca, Barcelona, 2015.

por el contrario, parecen respetarlas para el «usuario común» de internet y pensar que un determinado conjunto de personas sí puede tener cosas que ocultar.

d) Otra serie de argumentos sostiene la importancia de la privacidad y el secreto como base de la libertad de expresión y la democracia[8]. Por lo general, quienes desarrollaron esta perspectiva postulan la privacidad como un derecho que debe ser respetado, aunque, en todo caso, después queda la dificultosa tarea de definir en términos legales la privacidad. Además, sostienen, se trata de una condición de posibilidad de la democracia y la república. Desde esa premisa, especulan con distintos miedos que son producto del uso hegemonizado de la minería de datos, como la posibilidad de censuras programadas o de coartar cualquier acción indeseada en regímenes políticos de control. Aunque, en definitiva, ni la posibilidad de verse en situaciones contrafácticas ni los potenciales peligros producto de la acumulación de la información parecen hacer temer cambios fundamentales en el actual sistema político-económico[9].

e) Por último, otros textos parten de un ambiente de peligrosidad tácita respecto al cual quieren funcionar como un aviso de incendio. Desde esta perspectiva, no justifican mayormente por qué se debería utilizar encriptación de manera cotidiana, por lo que parecen dirigirse a una comunidad de activistas ya convencidos.

El libro de Assange utiliza un lenguaje bélico e impulsa la idea de una guerra de guerrillas de armas criptográficas

En esta dirección, por ejemplo, *Cypherpunks*, el libro de Assange, utiliza un lenguaje bélico e impulsa la idea de una guerra de guerrillas de armas criptográficas[10]. De alguna manera, estos textos podrían parecer contraproducentes. Una de las primeras formas que se buscaron de limitar la circulación de criptografía fue darle el tratamiento de «municiones de guerra». Por lo que este lenguaje bélico continuaría estigmatizando lo que, en definitiva, solo es un pequeño complemento en nuestro gestor de correo electrónico con software

8. Por ejemplo, E. Snowden: «Why Privacy is the Most Important Human Right», 2016, <https://archive.org/details/WhyPrivacyIsTheMostImportantHumanRight> y N. Zuazo: «Escritora Natalia Zuazo habla sobre su libro *Guerras de internet*», video, disponible en <https://archive.org/details/EscritoraNataliaZuazoHablaSobreSuLibroGuerrasDeInternet>.
9. Efectivamente, las prácticas del uso de internet no vieron mayores cambios después de las revelaciones de Snowden. Al respecto, v. por ejemplo Sören Preibusch: «Privacy Behaviors After Snowden» en *Communications of the* ACM vol. 58 Nº 5, 5/2015.
10. J. Assange, J. Appelbaum, Andy Müller-Maguhn y J. Zimmermann: *Cypherpunks*, OR Books, Nueva York, 2012. [Hay edición en español: *Cypherpunks. La libertad y el futuro de internet*, Deusto, Barcelona, 2013].

capaz de manejar una compleja algoritmia matemática. Esta discusión se enmarca en lo que se llama la «segunda guerra criptográfica» en la carrera entre los desarrolladores de herramientas de encriptación y quienes intentan romperlas y restringir su uso para poder desactivarlas. Si bien existen claras campañas para neutralizar el uso de la criptografía, puede parecer que esta «guerra» nunca empieza si no hay antes una tematización argumental sobre por qué y cuándo usar criptografía.

En definitiva, la táctica de todos los contraargumentos frente al «Nada que ocultar» radica en revalorizar de distintas maneras la sensación y noción de privacidad, probablemente porque para promover interés en el tema el camino más fácil sea despertar miedo frente a un posible peligro personal. Pero estos argumentos fracasan o bien por simplistas o bien por la certeza de que estamos inmersos en un sistema democrático con ciertas garantías perdurables. Contra esta perspectiva, buscamos sostener que en la práctica este enfoque no funciona. Principalmente, porque nadie cree violada su privacidad por el uso cotidiano que hace de los servicios que utiliza[11].

En busca de la metáfora literaria: estalinismo, neoliberalismo y ciberpunk

Si bien el «Nothing to hide» constituía ya un género de contraargumentos que desordenadamente se expandían en distintas páginas web aun antes de las revelaciones de Snowden en 2013, quien observó su relevancia desde el ámbito académico fue Daniel Solove[12]. Solove realizó un minucioso trabajo en el que rastreó la presencia del «Nada que ocultar» en la arena pública estadounidense y británica. Contra esto, ha realizado un análisis similar de estos contraargumentos, y su propio proyecto consiste en desarrollar una teoría sobre la privacidad para su protección legal. De esta manera, Solove es uno de los que de manera más decidida marcan la importancia de revalorizar socialmente la noción de privacidad. Para lo cual, de hecho, además de su rol como académico, fundó una empresa de seguridad digital, cuya tarea principal es brindar cursos sobre cómo resguardar información personal y corporativa. Pero su caso como referente del tema se vuelve especialmente claro en la metáfora literaria

11. Este texto, lejos de querer posicionarse críticamente frente a los más importantes activistas de las problemáticas políticas ligadas a internet y el software, busca contribuir a mejorar los argumentos que usamos.
12. Sus últimos trabajos al respecto son: «I've Got Nothing to Hide and Other Misunderstandings of Privacy» en *San Diego Law Review* Nº 44, 2007; *Nothing To Hide: The False Tradeoff Between Privacy and Security*, Yale University Press, New Haven, 2011.

que escoge pare pensar los problemas alrededor del «Nada que ocultar». Gran parte de los trabajos sobre privacidad no dejan de proponer alguna metáfora literaria para pensar el asunto, en un tema en el que por momentos se torna difícil escribir en formato académico, mientras que la ciencia ficción permitió plantear *conspiranoias* sin necesidad de mayores justificaciones. La metáfora del Gran Hermano no va más, sostiene Solove: la opresión no es tan explícitamente cruenta. En su lugar, propone tomar como referencia el tipo de dominación presente en *El proceso* de Franz Kafka. Allí el protagonista se mueve bajo la fuerza de un poder abstracto e ininteligible contra el que se encuentra desorientado. Lo destacable es que la militancia liberal-libertaria que mueve las intervenciones de Solove hace que deje de lado la necesidad de comprender mejor este nuevo tipo de relación entre individuo y sociedad, para lo cual tiene que dejar de lado también la metáfora literaria más actual sobre el tema, brindada por el ciberpunk.

La batalla cultural de la Guerra Fría tuvo su inicio simbólico en las continuas rediciones de la novela filotrotskista *1984* de George Orwell, publicada en 1949. Al menos desde allí, los totalitarismos han dado lugar a pensar la posibilidad de un engaño sistemático e incluso de una realidad paralela. Así por ejemplo, en su paso postorwelliano en *El hombre en el castillo* (*The Man in the High Castle*, 1962), Philip K. Dick lleva esto a un grado espectacular: qué tal si para asentar definitivamente la dominación, el *Reich* ganó la Segunda Guerra Mundial pero el modo más efectivo de ejercer el control consiste en hacer creer a todos los estadounidenses que viven libres y felices en sus hogares... Sin alejarse mucho de estas preguntas, el ciberpunk nació como un subgénero de la ciencia ficción a principios de la década de 1980, con sus propias marcas estéticas y políticas. A través de los *mirrorshades* de protagonistas en un combate quijotesco contra gigantescas corporaciones rivales de ambivalente existencia, vemos ambientes ecológicamente devastados y socialmente decadentes. La distopía funciona en un orden político determinado por distintos poderes económicos indescifrables, escondidos unos tras otros de manera tal que se vuelven insondables detrás de la mercancía y herramienta de dominio que ellos mismos controlan: la información. Los trabajadores informáticos, aquellos capaces de manipularla y robarla, bajo la ansiedad punk de destruirlo todo, no encuentran vías posibles para ello y viven bajo la paradoja del *hacker*: el último héroe romántico con la capacidad potencial de implosionar el sistema, pero cuya vida se encuentra disminuida tras su propia herramienta de combate.

La metáfora política del ciberpunk que aquí nos interesa remarcar es la constante e imposible determinación de la respuesta final sobre quiénes son los

actores corporativos y políticos en juego. Esta literatura avanza a través de falsas certidumbres y revelaciones para descubrir que el horizonte se movió: había otros elementos por tener en cuenta, una dimensión nueva que cambia todo, un actor social mayor y más poderoso que parece aunar al resto y unificar intereses aparentemente contradictorios. Del *ciberpunk* al *cypherpunk*, el libro citado de Assange mantiene ciertos rasgos de este subgénero de la ciencia ficción: el miedo a la distopía, el combate quijotesco, la ambigüedad potencial de las herramientas de emancipación y control de la información.

Donde no se puede reponer quiénes son los dueños de tales compañías, quiénes son sus inversores, cuáles sus intereses y sus relaciones, donde no se puede reponer la cadena de producción de un bien de consumo y las tercerizaciones de compañías que involucra, no se puede mejorar nuestro conocimiento sobre el mundo. De manera que frente a un neoliberalismo múltiple dentro del cual se vuelve imposible determinar actores y flujos de capitales, se dibuja la figura de un Leviatán acelerado que deviene único Gran Hermano respecto a la inexistencia de otros leviatanes. Entonces: ¿es posible que se trate solo de empresas en libre competencia por la información? ¿Se trata de punks en lucha contra el Gran Hermano? ¿O de un único Gran-Gran-Hermano-Leviatán acelerado? ¿No hay intereses geopolíticos atrás de la financiación de estas empresas?

El estallido mediático de las revelaciones de Snowden no trajo mayores consecuencias. Dentro de Estados Unidos, la disputa se abrió a partir de un debate acerca de si Snowden debía ser considerado un héroe o un traidor. Celosos de las libertades individuales frente al Estado, los llamados liberal-libertarios (una suerte de anarquistas de derecha) fueron los que más levantaron su voz. En el exterior, una de las razones por las que la Universidad de Rostock (Alemania) reconoció académicamente a Snowden fue porque «nos ayudó a pensar nuevamente la democracia», en el marco del gran conjunto de cambios que involucran las reformulaciones del liberalismo como neoliberalismo y las relaciones entre sociedad, Estado, individuos, empresas y corporaciones, y en el momento mismo en que los marcos legales de internet están comenzando a discutirse.

El estallido mediático de las revelaciones de Snowden no trajo mayores consecuencias ■

Al igual que muchos textos sobre esta temática, el análisis y la propuesta de Solove dejan en claro que su objetivo es solamente problematizar de manera general «los peligros de la vigilancia estatal» y reducir el papel político de las

empresas de contenidos digitales a que solo cumplan los contratos acordados con sus usuarios. Frente a esto, la mirada ciberpunk permite mantener abierta la pregunta sobre los vínculos de empresas de una misma bandera y su gobierno. Mientras tanto, el lema cypherpunk –«transparencia para los poderosos, privacidad para los débiles»– deja en claro que ciertas empresas transnacionales manejan un capital mayor que el PIB de muchos países. Aunque esta tarea parezca difícil, contra Solove, se trata de identificar a los actores responsables de la infraestructura y los contenidos detrás de internet.

Prácticas conscientes en torno de una nueva agenda política

Desde un principio, el «Nada que ocultar» plantea el problema como una trampa. Al intentar desactivarlo en sus propios términos, el conjunto de los contraargumentos busca generar cierto temor por potenciales inconvenientes personales para mostrar la importancia de reactualizar la privacidad como un valor social.

Por el contrario, otra vía de análisis aún poco explorada requiere una interpretación de la coyuntura política, que en definitiva únicamente puede consistir en un diagnóstico sobre los actores responsables de brindar servicios digitales. «¿Quién construyó Tebas?» es una pregunta que interroga a los estudios históricos, pero no extiende su poder hacia el presente, como si el panorama actual resultase transparente. Como ya señalamos, hoy en día identificar actores e intereses presenta gran dificultad, en tanto usamos plataformas y consumimos productos que, por la complejidad de sus cadenas de producción y estrategias de marketing, se nos aparecen neutros. En este contexto, identificar actores e intereses se vuelve una acción en sí política. La difusión de análisis de este tipo podría romper varios niveles de ingenuidad, o al menos correrno s de las actitudes iniciales de desestimar el carácter político de las herramientas informáticas hegemónicas.

De hecho, esta perspectiva contra el «Nada que ocultar» es la que nos ayuda a plantear mejor el problema. No se trata de pensar en algo que tengamos que ocultar, sino más bien en las implicancias de los usos que hacemos de internet y del software y en las empresas utilizadas. El desafío consiste en pensar cómo politizar estos contraargumentos para buscar elementos que interpelen, quizás no a un usuario cualquiera, sino al menos a quienes tengan ciertas convicciones político-sociales. Por ejemplo, es posible esbozar contraargumentos que apelen al consumo responsable –dentro de lo que podrían entrar los llamados a boicot que hace Stallman–. O, con un correcto diagnóstico, ampliar

los contraargumentos según sus implicancias antimonopólicas. O sugerir las ventajas de utilizar servicios cooperativistas o autonomistas también en el mundo digital.

Si el *big data* plantea problemas políticos todavía inescrutables, los grupos activistas abren dos frentes: uno referido a sus regulaciones legales y otro que promueve herramientas como la criptografía. En cualquier caso, difundir y volver masivas estas discusiones no solo contribuye a hacer más conscientes nuestras prácticas digitales. Al mismo tiempo, permite descubrir una nueva agenda política que hasta ahora era en buena medida invisible[13]. Y también, por ejemplo, da lugar a considerar algunas de las discusiones en curso promovidas por los activistas: sobre el alcance político de las nuevas licencias y el software libre, sobre los modos de habitar/conformar internet, sobre la llamada gobernanza de internet y la soberanía digital.

13. Por ejemplo, v. Eben Moglen: «Libertad en la nube, libertad del software, privacidad y seguridad para la web 2.0 y computación en la nube» en *En Defensa del Software Libre* Nº 0, 2010.