

ATRIO

www.flacsoandes.edu.ec

Habitar las redes: las controversias sobre la privacidad en Facebook

María Belén Albornoz

FLACSO Ecuador

© 2020 FLACSO Ecuador
Octubre de 2020

Cuidado de la edición: Editorial FLACSO Ecuador

ISBN: 978-9978-67-545-8 (pdf)
<https://doi.org/10.46546/20209atrio>

Flasco Ecuador
La Pradera E7-174 y Diego de Almagro, Quito-Ecuador
Telf.: (593-2) 294 6800 Fax: (593-2) 294 6803
www.flasco.edu.ec

Albornoz, María Belén

Habitar las redes : las controversias sobre la privacidad en
Facebook / María Belén Albornoz. Quito : FLACSO Ecuador,
2020

viii, 288 páginas : ilustraciones, figuras, gráficos, mapas, tablas.
- (Serie Académica Atrio)

Bibliografía : p. 271-287

ISBN: 9789978675458 (pdf)
<https://doi.org/10.46546/20209atrio>

REDES SOCIALES ; MEDIOS DE COMUNICACIÓN ;
INDUSTRIA DE LA COMUNICACIÓN ; PROTECCIÓN
DE DATOS ; TECNOLOGÍAS ; SOCIOLOGÍA TECNO-
LÓGICA ; FACEBOOK ; PROBLEMAS SOCIALES

302.30285 - CDD

Editorial  FLACSO
Ecuador

A Manuel, por su lectura crítica,
su paciencia y cariño.

A Javier y Mónica, por introducirme en
el mundo del CTS de manera irremediable.

A Roberto, por su guía generosa
por los laberintos del ciberespacio.

Índice de contenido

Introducción	1
------------------------	---

SECCIÓN I

ORÍGENES Y CONTROVERSIAS SOBRE LA PRIVACIDAD

Capítulo 1. Las raíces europeas y americanas del derecho a la privacidad	5
La tradición francesa de la vida privada	8
La tradición del derecho alemán a la privacidad	10
El sistema europeo	12
El sistema estadounidense	14
Lo que el derecho ha excluido	16

Capítulo 2. Controversias acerca de la privacidad desde el siglo XIX: su co-construcción	20
Autonomía en la toma de decisiones	25
Un nuevo actor dentro de la controversia: el Estado	33
La autodeterminación y las expectativas de privacidad	35
La información como forma de clausura de la privacidad	38
Datos personales	41

Capítulo 3. Ciberespacio y redes sociales	46
Origen de las redes sociales	54
El nuevo fenómeno de las redes	59
Información que se publicaba en los perfiles personales	65

SECCIÓN 2

FACEBOOK

Capítulo 4. El artefacto sociotécnico	71
La sociedad en red: Silicon Valley y los visionarios.	74
Imaginando Facebook. El valor del código	78
Capítulo 5. Transformando la red en una empresa	96
Nuevas alianzas para reinventar la publicidad en Facebook	99
La economía política de Facebook	108
Capítulo 6. Construyendo historias personales y dossiers digitales	115
El perfil.	116
La construcción del <i>Social Graph</i>	120
Interactuando en Facebook	123
<i>Timeline</i> y las historias de vida.	126
<i>Dossiers</i> digitales	129

SECCIÓN 3

LA PRIVACIDAD EN FACEBOOK

Capítulo 7. La construcción de la privacidad en Facebook	132
Organizaciones dedicadas a la privacidad	135
La trayectoria de la privacidad en Facebook	138
Fetichismo de la privacidad en Facebook	139
Privacidad y economía política de Facebook	141
Capítulo 8. La privacidad desde una mirada sociotécnica	146
Privacidad y publicidad	162
El marco tecnológico de Facebook	168
Problemas y soluciones de los grupos sociales relevantes	177

SECCIÓN 4

CONTROVERSIAS Y EMSAMBLAJES

Capítulo 9. Las controversias sobre la privacidad en Facebook.	182
<i>News Feed</i> : la primera controversia sobre la privacidad en Facebook	187
<i>Beacon</i> : la segunda controversia sobre la privacidad en Facebook	198
Términos de servicio, año 2009: la tercera controversia sobre la privacidad en Facebook	209
Demanda de la Comisaría de Privacidad de Canadá a Facebook: la cuarta controversia sobre la privacidad	222
<i>Everyone</i> : la quinta controversia sobre la privacidad en Facebook.	241
Ensamblajes sociotécnicos	257
Conclusiones	259
Referencias	271
Sobre la autora	288

Figuras

Índice de gráficos

Gráfico 1. Surgimiento de las redes sociales	56
Gráfico 2. Mapa de relaciones personales entre redes vinculadas a Facebook	78
Gráfico 3. Características de Thefacebook	80
Gráfico 4. Inversionistas de Facebook	99
Gráfico 5. Exposición de la información de los usuarios 2005-2010.	148
Gráfico 6. Posibilidades de ejercer el control de la información	161
Gráfico 7. Porcentaje de consumidores que consideran importante la privacidad	166
Gráfico 8. Responsables de salvaguardar la privacidad	167
Gráfico 9. Confianza en los términos de privacidad.	167
Gráfico 10. Niveles de controversia CIPPIC vs. Facebook	225
Gráfico 11. Número de palabras utilizadas en Facebook sobre privacidad	246
Gráfico 12. Actores de la controversia <i>Everyone</i>	252

Mapas

Mapa 1. Posición de las redes sociales en el mundo a junio de 2009 . .	57
Mapa 2. Posición de las redes sociales en el mundo a junio 2010.	58
Mapa 3. Posición de las redes sociales en el mundo a junio de 2011 . .	58
Mapa 4. Posición de las redes sociales en el mundo a junio de 2012 . .	58

Índice de tablas

Tabla 1. Controles de privacidad <i>vs.</i> posibilidades de control.	155
Tabla 2. Flexibilidad interpretativa de News Feed	193
Tabla 3. Controles de privacidad a raíz de Beacon	203
Tabla 4. Nociones de privacidad a raíz de Beacon	204
Tabla 5. Flexibilidad interpretativa de los Términos de servicio de Facebook	214
Tabla 6. Acciones de los actores.	239
Tabla 7. Flexibilidad interpretativa en la controversia Everyone.	256

Índice de ilustraciones

Ilustración 1. Thefacebook, 2005	79
Ilustración 2. Mini Feed, 2006	86
Ilustración 3. Engagement Ads	106
Ilustración 4. Perfil en Facebook, 2008	117
Ilustración 5. Perfil en Facebook, 2010	120
Ilustración 6. Foto con comentarios	125
Ilustración 7. Timeline	126
Ilustración 8. Controles de privacidad en octubre de 2009	153
Ilustración 9. Controles de privacidad en enero de 2010	154
Ilustración 10. Ausencia de la opción “rehusar”, uso de información en aplicaciones	156
Ilustración 11. Ausencia de controles para optar por “no compartir información sobre mí”	156
Ilustración 12. Nuevos controles no permiten ver qué se muestra a los otros usuarios	157
Ilustración 13. Sistema <i>opt-out</i> de personalización instantánea.	158
Ilustración 14. Escalamiento de controles de configuración de cuenta	159
Ilustración 15. Sitio de Gobernanza de Facebook	216
Ilustración 16. Notificaciones del sitio de Gobernanza de Facebook	218
Ilustración 17. Captcha de reconocimiento facial	223
Ilustración 18. Visualización presencial en el f8, abril de 2010	250
Ilustración 19. Autorización para entregar número de teléfono celular y dirección a los desarrolladores de aplicaciones	250

Introducción

Hasta hace pocas décadas no era evidente la relación entre política, privacidad y tecnología. Luego de que Cambridge Analytica y Facebook probaran que se podía influenciar campañas electorales a través del uso de algoritmos, esta relación parece obvia. Ahora escuchamos cómo a través de la psicometría se cuantifican los comportamientos sociales, se reconocen los estilos de vida de las personas mediante códigos informáticos (psicográficos) y se usa *machine learning* para combinar datos personales, datos demográficos y tipos de personalidades e identificar grupos de votantes que puedan ser influenciados a través de Facebook.

De igual manera, las controversias sobre la privacidad que ahora nos parecen incuestionables todavía no se habían establecido sino hasta mediados del siglo XIX. Esto debido a que la literatura sobre privacidad poco aporta a explicar cómo la privacidad evoluciona en relación con el cambio tecnológico. Por tanto, en este libro se estudia la relación entre cambio social y cambio tecnológico para explicar cómo los artefactos y los códigos informáticos co-producen la privacidad en las redes sociales.

La novedad de este trabajo es dejar de estudiar la privacidad desde lo puramente social e introducir la tecnología en los procesos de construcción de lo privado desde un abordaje sociotécnico. Una primera entrada es mostrar cómo los debates sobre la privacidad se vuelven parte de la esfera pública el momento en que ciertos artefactos tecnológicos se masifican. Cada artefacto que se incluye en este libro muestra por qué las tecnologías de la mano de las regulaciones han contribuido a configurar la privacidad.

Este texto intenta responder varias interrogantes. La primera tiene que ver con una arqueología de la privacidad en Occidente y con su

relación con el cambio tecnológico: ¿cómo se ha construido la noción moderna de privacidad en Occidente? ¿de qué modo estos procesos se relacionan con el cambio tecnológico? ¿cuáles son las nociones de privacidad que se estabilizan? La segunda cuestiona la capacidad que tiene el artefacto sociotécnico de diseñar condiciones de privacidad y de transformar la norma social: ¿qué se entiende por privacidad en los mundos virtuales, más allá del derecho de la privacidad? ¿qué agencia tienen las redes sociales virtuales en la construcción de espacios virtuales públicos estandarizados? ¿de qué modo estos espacios públicos en línea promueven la naturalización de la exhibición del sujeto? Y la tercera se enfoca en las controversias de la privacidad: ¿cuáles son los procesos de negociación entre los usuarios y Facebook? ¿quiénes intervienen en las controversias? ¿cuál es la relación entre el código y la norma social que permite la co-construcción de las nociones de privacidad en línea? ¿qué consecuencias tiene la constante exhibición del sujeto sobre los imaginarios que se desarrollan acerca de la privacidad?

El punto de partida de este trabajo se centra en los debates sobre la privacidad que se inician en la segunda mitad del siglo XIX, cuando en el campo del derecho se intenta construir una teoría sobre la privacidad y un sistema de protecciones legales del individuo. Para ello, se describen los orígenes legales de la privacidad en Estados Unidos y en Europa y de los artefactos tecnológicos que han acompañado los debates sobre la privacidad en ambos lados del mundo. Así, se sigue el rastro de las cámaras fotográficas, las nuevas tecnologías de la prensa, el teléfono, las bases de datos, la internet y las redes sociales para develar la importancia del cambio tecnológico en la construcción de la privacidad como un valor social.

En este libro se incorpora a la tecnología como un actor en los procesos de construcción de la privacidad, procesos que hasta ahora han sido pensados en términos estrictamente sociales y no sociotécnicos. Así, los lentes de los estudios sociales de la ciencia, tecnología y sociedad (CTS) ofrecen una oportunidad para explicar cómo se produce el cambio de las normas sociales a partir de la agencia que tiene el artefacto tecnológico de Facebook. Solo de este modo es posible mostrar que la sociedad está tecnológicamente estructurada y que la tecnología está socialmente construida (Thomas 2008).

El análisis sociotécnico contribuye también a reconstruir el ámbito en que los artefactos tecnológicos se vuelven parte constitutiva de las relaciones sociales, culturales, económicas y políticas, al mismo tiempo que estas relaciones se materializan en artefactos y sistemas tecnológicos. Tal enfoque permite entender la estabilización de Facebook como artefacto de socialización virtual y como estructurador de conductas y de formas de entender lo privado; un sitio donde la arquitectura del código informático para diseñar formas de poder que condicionan los comportamientos de los sujetos en línea acontece en “el lugar más regulado que el ser humano haya habitado jamás” (Lessig 2006, 39).

Cuando Thefacebook inició, todavía no había llegado la era de la postverdad ni era el momento de reclamar la propiedad y control de los datos como un derecho humano. Sin embargo, Thefacebook es parte del origen de las tecnologías invasivas y del momento en que los ciudadanos reconocen que su privacidad está en riesgo debido al cambio tecnológico. Por ello, vale la pena entender la génesis de por qué los algoritmos empezaron a moldear nuestras vidas.

SECCIÓN I
ORÍGENES Y CONTROVERSIAS
SOBRE LA PRIVACIDAD

Capítulo 1

Las raíces europeas y americanas del derecho a la privacidad

La noción de privacidad es una idea moderna, hija del Iluminismo. Separa la esfera privada y la esfera pública como espacios autónomos y diferenciados (Bloustein 1964; Rule 2007; Schoeman 1984; Solove 2008; Warren y Brandeis 1890). Este capítulo tiene el propósito de analizar cómo se han construido las diferentes concepciones de privacidad en Occidente y relacionar dicha trayectoria con el cambio tecnológico. Para ello recupero los debates sobre la privacidad surgidos en Europa desde el derecho francés, vinculado con la imagen y con el honor, y desde el derecho alemán, relacionado con la dignidad y con la personalidad. Estas nociones son retomadas en los Estados Unidos por los abogados Warren y Brandeis en su artículo “The Right to Privacy” (1890) y dan lugar a la propuesta norteamericana de la privacidad basada en el derecho a “ser dejado en paz”.

Uno de los hallazgos más importantes en este capítulo es que las versiones de la privacidad, que surgen en el seno del derecho, están estrechamente ligadas a coyunturas de cambio tecnológico; en ellas, los artefactos sociotécnicos son utilizados de forma masiva dentro de la sociedad, lo que genera controversias sobre qué es la privacidad en los distintos grupos sociales relevantes. Así, se muestran las trayectorias de la *snap camera*, la prensa amarillista, el teléfono, los anticonceptivos, los sistemas de monitoreo, las bases de datos y, finalmente, el ciberespacio y sus redes sociales.

En este recorrido he acopiado las doctrinas más relevantes sobre la privacidad, producidas por los sistemas legales y la sociología jurídica en el siglo XX, como la autonomía en la toma de decisiones, el acceso limitado

a uno mismo, las razonables expectativas de privacidad, el control de la información personal/autodeterminación informacional, el fetichismo de la privacidad y la privacidad en red. Acompaño este análisis con el de las relaciones entre sujeto, tecnología y norma social para explicar cómo la privacidad es un producto social móvil donde se co-construyen relaciones entre actores humanos y no-humanos en la red.

Las trayectorias europeas y norteamericanas responden a diferentes culturas de privacidad, las cuales albergan sensibilidades intuitivas¹ distintas y producen dos sistemas de derecho únicos. El derecho europeo, a diferencia del norteamericano, se basa en un sistema de valores que data de los siglos XVII y XVIII, donde el honor y el respeto fundamentan lo que hoy se conoce como vida privada.

Las leyes sobre la privacidad en Europa derivan de protecciones más amplias del respeto interpersonal: la ley sobre el discurso odioso² y la ley sobre el insulto. Ambas se basan en cuerpos legales muy antiguos de protección del honor personal individual. A pesar de que se ha asociado la producción de la noción de dignidad continental a una reacción europea contra el fascismo, en particular a los actos derivados del nazismo, para Withman este concepto es, más bien, una construcción de los siglos XVII y XVIII. La Europa de hace trescientos años contenía una sociedad fuertemente jerárquica, monárquica y aristocrática, en la que solo las personas de clase alta tenían el *derecho* a que se respete su honor personal en la corte. La evolución del derecho europeo tiene como objeto nivelar esta inequidad, por lo que extiende las normas destinadas a los aristócratas y nobles al resto de la población.³ Así pues, la privacidad

¹ Hablo de sensibilidades intuitivas porque los sujetos tienen intuiciones que están moldeadas por los sistemas legales y los valores sociales de las sociedades en que viven. Tenemos intuiciones “juridificadas”, esto es, intuiciones que reflejan nuestro conocimiento y nuestro compromiso con los valores legales básicos de nuestra cultura (Withman 2004, 1160).

² El marco legal que da origen a la protección de las minorías puede rastreararse en la «ley del duelo». En el siglo XIX, las cortes solo protegían el derecho al respeto únicamente en casos de duelo. En Europa este cuerpo legal se ha extendido a la protección del derecho al respeto para los presos en las cárceles (Withman 2004).

³ Incluso las formas de ejecución de los sujetos se diferenciaban dependiendo de la clase social a la que pertenecían; a los nobles los decapitaban, y a los plebeyos los colgaban. Una manera más de lograr la nivelación de clases que encuentra la Revolución francesa es el invento de la guillotina, donde todos eran decapitados por igual. Así, el privilegio de la nobleza se extendió al resto del pueblo (Withman 2004).

européa está muy ligada a las leyes sobre el respeto que se desarrollan en la época cortesana, y a su sistema de etiqueta que más tarde sería utilizado por el conjunto de la sociedad.⁴ Las leyes sobre la privacidad protegen normas de dignidad que son “reglas de civilidad”, tales como las normas de etiqueta, sin las cuales ninguna sociedad podría mantener alguna forma de comunidad (Post 1995).

La relación entre el derecho a la privacidad y la personalidad tiene que ver con la capacidad de controlar lo que Goffman (1981) denomina “la presentación del ser”. La habilidad del individuo para moldear, mantener y controlar una imagen pública, así como el poder de la ley de interpretar y ordenar lo que la sociedad considera la propia imagen. “Las normas de civilidad están lejos de ser universales, varían dramáticamente de una comunidad a otra” (Post 1995, 51). La privacidad, en tanto control de la propia imagen, tuvo éxito en Europa porque encajó en las tradiciones sociales continentales, en una cultura cotidiana del respeto y en la diaria presentación de la persona. Esta versión de la privacidad es un fenómeno históricamente situado, que funciona porque es apropiado dentro de la cultura europea. En el viejo mundo, la privacidad tiene que ver con el derecho del sujeto a que su rostro público no se desprestigie; así, dentro de este sistema de valores, su primer enemigo son los medios de comunicación (Withman 2004).

A diferencia de los valores de libertad de expresión y de propiedad privada distribuida a través del mercado, que predominan en la sociedad norteamericana, la historia del derecho continental europeo de la vida privada tiene como núcleo el honor. En Francia, las regulaciones que se vinculan al honor se ubican entre 1790 y 1900, en Alemania entre 1880 y 1960.

⁴ Los autores europeos continentales muchas veces consideran la etiqueta y la privacidad como temas relacionados; tal es el caso de Alemania, donde encontramos que ciertos asuntos relativos a la privacidad son tratados también como problemas de «buenos modales» (Gerhard y Stefen, citados por Withman 2004).

La tradición francesa de la vida privada

La tradición francesa de la privacidad se establece en relación con los recurrentes periodos de licencia sexual. En Francia del siglo XIX había dos cosas que amenazaban el honor de una persona: las habladurías y el bajo mundo de la compraventa; así, es frente a estos problemas que el derecho a la privacidad se fortalece. Durante siglos, por ejemplo, la nobleza francesa evitó registrar sus propiedades y dar cuentas públicas de su fortuna, apelando a su sentido de privacidad.

La historia moderna de la protección de la vida privada en Francia empieza más bien con la revolución y con la introducción de la libertad de prensa, la cual ponía nerviosos incluso a los franceses más liberales (Withman 2004). La Constitución de 1791 estableció protecciones a la libertad de prensa, pero al mismo tiempo, añadió salvaguardias contra “calumnias e insultos relativos a la vida privada”.⁵ Reconoció que estas libertades amenazaban la privacidad de las personas y contradecían las ideas del antiguo régimen.⁶ En el *nuevo orden*, el honor de “todos” podía ser protegido, con lo cual se ampliaban a toda la población los códigos de honor que regían en las clases aristocráticas. En 1819 pasó la primera ley que levantó la censura, lo que permitió una prensa más libre; ello originó una reacción incluso de los más liberales defensores de la nueva ley, como Royer-Collard, quien sostuvo que la vida privada debe ser tapiada (*murée*) –Barante (1863)–. El término se convertiría en un lema continental que se repetiría hasta bien entrado el siglo XX.

Si bien la protección de la privacidad no estuvo codificada en ley alguna hasta 1830, fue ejercida a través de mecanismos de protección del honor como el del duelo. No obstante, hacia mediados del siglo XIX empezó a desaparecer esta costumbre y las demandas sobre la vida privada pasaron al ámbito de los tribunales; apareció entonces lo que se conocería como el centro del derecho a la privacidad en Francia: el “derecho

⁵ Constitución del 3 de septiembre de 1791, tit. III, cap. V, art. 17 (“Les calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée, seront punies sur leur poursuite”).

⁶ Término utilizado como sinónimo de feudalismo. Tocqueville, sin embargo, lo emplea para referirse al siglo XVIII, al momento en que crece el comercio y la burocracia administrativa al lado de los privilegios feudales (Sennett 1977, 47).

a la propia imagen”. Los casos de Dumas padre⁷ y del pintor Ingres⁸ sirvieron de jurisprudencia, entre otros, para sostener que existe un “principio sagrado e inalienable sobre uno mismo y, en consecuencia, sobre la reproducción de la propia imagen” (Dumas, citado por Withman 2004, 1177). El derecho a la propiedad intelectual entró en tensión con el derecho a la propia imagen, lo cual afectó también la liberalización de la prensa. Así, en 1868 se creó una política de prensa que protegía la privacidad; de esta manera se reconocía como contravenciones graves (delitos), cualquier atentado contra la vida privada, la difamación y el insulto. Se prohibía, por ejemplo, que un escritor utilizara en su novela eventos revelados en la corte (Contamine-Raynaud 1978).

A pesar de los avances en las cortes, todavía se consideraba que el derecho a la vida privada no resolvía del todo el daño moral ocasionado a las personas. Dos años antes de que Warren y Brandeis publicaran su artículo “The Right to Privacy”, el filósofo legal Émile Beaussire (1888) sostenía que el derecho a la privacidad debía formar parte de los derechos del honor y tenía que ser defendido a través del duelo, y no por medio del derecho: “cuando mi honor es atacado, no gano nada demandando a mis calumniadores [...] la gente se ha burlado de la máxima ‘la vida privada debe ser tapiada’” (372-73).

El valor de la protección de la privacidad “honorable” se mantuvo en Francia muy cercano a la ortodoxia hasta finales de 1890 y se extendió

⁷ Alexandre Dumas, padre, tuvo un romance con una actriz norteamericana, Adah Meken, y ambos se tomaron fotografías atrevidas para la época (en algunas imágenes Meken aparece en ropa interior). Era 1867 y Dumas no había acordado nada con el fotógrafo sobre los derechos de publicación, por lo que este intentó registrar el derecho de propiedad intelectual de lo que consideraba podían ser fotos muy valiosas en el mercado. Las autoridades le otorgaron el derecho de propiedad intelectual, pero le prohibieron publicar únicamente las fotos en que Meken aparecía en ropa interior. La publicación del resto de las fotos fue un escándalo en Francia. Dumas apeló a la corte en París que sentenció a su favor con el principio de que la vida privada de las personas debe ser “tapiada”. La corte privilegió el derecho a la privacidad de Dumas por sobre el derecho de propiedad intelectual que poseía el artista que lo fotografió con su amante, obligándolo a vender sus derechos de propiedad intelectual al demandante. “La propia privacidad, como otros aspectos del honor, no es una mercancía que pueda ser simplemente comerciada o vendida” (Withman 2004, 1176).

⁸ Jean-Auguste-Dominique Ingres realizó un retrato de la señora Moitessier desnuda. Él utilizó dos modelos: una para pintar el desnudo y Moitessier para el rostro. Al morir el pintor se encontró la obra y uno de sus ejecutores intentó venderla, ante lo cual el señor Moitessier presentó una demanda legal. La corte le otorgó los derechos de propiedad intelectual a los herederos de Ingres, pero también reconoció el derecho a la privacidad del señor Moitessier: el derecho a la imagen de su esposa, sentenciando que se venda la pintura al señor Moitessier.

a lo largo del siglo XX, a través de códigos de etiqueta que, a su vez, se transformaron en protecciones al derecho a la privacidad, tal es el caso de los reportes de crédito.

La tradición del derecho alemán a la privacidad

La tradición germánica se desarrolla de modo más lento que en Francia y se vincula, particularmente, a los sucesos acaecidos durante y después del periodo nazi. La protección de la vida privada en ese lado del Rin tiene raíces filosóficas en el concepto de “personalidad”. En tal sentido, la ley sobre la personalidad es una norma sobre la libertad y el espacio interior del sujeto, donde la noción de libertad se concibe sobre todo opuesta al determinismo. En la tradición alemana, la libertad no está en relación con el Estado o el libre mercado sino más bien con el “libre albedrío”, con la capacidad de concebir al sujeto como criatura única, capaz de alcanzar su potencial a través de sus poderes y facultades. Reinterpretando de forma excepcional la antigua ley romana del insulto o *injuria*,⁹ y combinándola con la ley de propiedad artística, crearon la ley sobre la personalidad.

El derecho romano es estudiado desde el enfoque hegeliano de la historia del castigo. En esta perspectiva, la ley del talión de “un ojo por un ojo” produce gradualmente un concepto de proporcionalidad más sofisticado al incluir valores inmateriales. La evolución de la ley romana del insulto refleja, así, el paso de la reivindicación monetaria del honor a su protección contra insultos verbales y otras formas de falta de respeto; se da paso, entonces, a la versión alemana del derecho al buen nombre y la propia imagen.

La ley de propiedad artística reconoce los derechos del creador artístico o intelectual, y parcialmente fundamenta los derechos de propiedad intelectual (*copyright*), pero, lo que es más importante, abarca el derecho

⁹ La ley del insulto es una norma muy compleja de reinterpretar porque cubría muy diversos fenómenos. Se aplicaba contra el lanzamiento de hechizos, propinamiento de lesiones corporales o el insulto público. También se extendió a la protección de las mujeres respetables de comentarios lascivos y a garantizar que las personas de alto estatus no insultaran a sus inferiores. El trabajo de los juristas alemanes ejerció gran influencia en académicos como Warren y Brandeis (Withman 2004).

que tiene el autor de controlar el uso de su obra, con el fin de proteger la propia reputación del artista (*droit moral de l'auteur*). El artista es considerado el actor libre paradigmático, y no el consumidor (Krieger 1957).

De esta manera, hacia principios del siglo XX el derecho alemán incluyó un amplio espectro de derechos a la personalidad. El derecho de prensa contenía a su vez el derecho a réplica. El Código Civil protegió el nombre y la capacidad de crédito de los sujetos. Se creó la Ley de competencia desleal, protegiendo así a las empresas alemanas de declaraciones falsas que puedan afectar su crédito. Además, el Código criminal incluyó una prohibición al insulto. A pesar de todos estos avances, en ningún corpus legal apareció propiamente el “derecho a la personalidad” (Withman 2004).

En el primer tercio del siglo XX, el régimen nazi estaba muy comprometido con la protección de la personalidad y proclamaba la importancia del “honor”, en particular, el honor de las personas de bajo estatus (mientras fueran racialmente alemanas).¹⁰ La reivindicación del honor de los alemanes se realizaba en contra del deshonor de los otros: los enfermos y los extranjeros. En cuanto a la doctrina, los nazis ratificaron el derecho a la personalidad y garantizaron el honor de las clases bajas alemanas. En este sentido, las leyes nazis son un antecedente a la Constitución alemana de posguerra, que en su artículo 2.º garantiza que “cada persona tiene el derecho al desarrollo libre de su personalidad, mientras no lastime los derechos de los otros” (Grundgesetz [Constitución] 1949, artículo 2.º, párrafo 1).¹¹

No es raro entonces que las tradiciones francesa y alemana del derecho a la privacidad se encuentren en Estrasburgo a mediados del siglo XX. Desde la Corte Europea de los Derechos del Hombre, la jurisprudencia del Tribunal de Estrasburgo ha contribuido enormemente a la evolución del derecho a la privacidad en Europa.

¹⁰ Esto llevó a insistir en normas de respeto para los empleados en su lugar de trabajo.

¹¹ Traducción libre, véase texto original en <https://bit.ly/34w0CVu>

El sistema europeo

El *principio de evaluación normativa* se basa en el criterio de proporcionalidad. Implica, así, una ponderación de los intereses privados de las personas y opera, *a priori*, en la sociedad y, *a posteriori*, en los debates de legisladores y jueces. Este principio se encuentra en el artículo 8.º del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma en 1950.

Art. 8. Derecho a respetar la vida privada y familiar

No podrá existir ninguna interferencia en el ejercicio de este derecho por parte de una autoridad pública, a menos que dicha injerencia esté contenida en la ley y sea necesaria dentro de una sociedad democrática, para proteger la seguridad nacional, la seguridad pública o el bienestar económico del país, la prevención del delito, la protección de la salud o moral públicas, o para la protección de los derechos y libertades de los demás.

En tal sentido, en las sociedades occidentales actuales se ha convertido en un imperativo ético y jurídico *respetar* la autonomía individual de los sujetos, porque intentar crear las condiciones necesarias para el desarrollo de autonomía de los ciudadanos (*self government*) y la democracia deliberativa colectiva es una condición de legalidad y de legitimidad de la ley.¹² Si bien la ley se centra en el desarrollo de la personalidad del sujeto, insiste en ubicarlo dentro de una sociedad democrática en constante interacción:

el valor del respeto a la vida privada supera su utilidad al ayudar a los individuos a salvaguardar su dignidad y a desarrollar sus relaciones personales. La mayoría de expertos sobre temas de privacidad insiste en la necesidad de respetar la vida privada. Yo sostengo que es igualmente importante para la sociedad que exista el respeto a la privacidad porque el respecto a esta sirve no solo a los intereses individuales, sino también los fines comunes, públicos y colectivos (Regan 1995, 321).

¹² Sin embargo, la autonomía y la autodeterminación no pueden ser reconocidas como derechos en estricto sentido jurídico, pues el Estado no puede proporcionarlos a los individuos. Y la simple abstención del Estado a inmiscuirse o interferir en los asuntos privados o íntimos de las personas, no es suficiente para que los sujetos se vuelvan autónomos.

En la jurisprudencia del Tribunal de Estrasburgo se pueden rastrear sendos momentos del derecho a la privacidad: el derecho de la persona a ser dejada sola (un derecho a la opacidad) y el derecho a la autodeterminación. Estos dos momentos han marcado, igualmente, dos visiones del Estado muy diferentes respecto de la vida privada de los individuos: uno negativo, vinculado a los límites del Estado de inmiscuirse en los dominios reservados de las personas; y otro positivo, que vuelve al Estado posibilitador de las condiciones materiales y psíquicas para el florecimiento individual. La protección de la vida privada es, por tanto, híbrida: es *defensiva* en tanto protege a la persona de las intromisiones del exterior, y es *ofensiva* en cuanto exige del Estado las libertades individuales necesarias para el desarrollo de la personalidad, tomando en cuenta las concepciones individuales del buen vivir y la organización de un ambiente lo suficientemente heterogéneo. Se trata entonces de la consagración de una libertad,

pero de una libertad diferente de otras libertades públicas, puesto que concierne a cada individuo y a su propia subjetividad y singularidad. Así, esta toca igualmente a las ciencias humanas: psicología, antropología, sociología, filosofía y los valores éticos. Toca todo a la vez, lo real, lo imaginario y lo simbólico, impacta todo aquello que se encuentra en la base de los comportamientos de los hombres. Por tanto, no es por azar que la Corte Europea de los Derechos del Hombre haya escogido explícitamente renunciar a definir su contenido (Meulders-Klein 2005, 308).

Frente a la concepción normativa, Ruth Gavison (1984) propone la concepción neutral, en la que se define a la privacidad como la medida del acceso que otros tienen a los datos de una persona a través de la información, atención y proximidad física. Así, la privacidad depende de que la información sobre la persona sea secreta o conocida. El beneficio de la concepción neutral es que permite reconocer estados crecientes o decrecientes de privacidad sin (juicios de valor moral) tener que recurrir a la concepción normativa: esto es bueno o es malo. El problema de quién tiene discreción o control sobre determinado nivel de acceso representa un área importante de negociación entre las personas y las sociedades donde viven (Nissenbaum 2010, 68-70). Para esta propuesta, la concepción normativa se basa

en una capa de la concepción neutral, al establecer cuánta privacidad es buena o es requerida en términos generales, y al especificar con qué condiciones variables y en qué nivel se puede asegurarla.

Otro problema que se toma en cuenta es el desplazamiento de las nociones de privacidad a los ámbitos de la propiedad y de los bienes comerciales. A Cohen (2000) le preocupa particularmente el giro que tomó el debate sobre la privacidad en la segunda mitad del siglo XX. La autora insiste en que la privacidad merece un lugar al lado de valores como los de igualdad y libertad, porque resulta crucial para el desarrollo de la autonomía moral (Cohen 2000). El espacio de lo privado permite, así, el fortalecimiento de la construcción consciente del sujeto, gracias a él las creencias y los deseos de las personas se salvan de caer dentro del espectro de lo corriente. Sin embargo, la crítica que ha tenido esta definición apunta que “la privacidad no es idéntica al control del acceso a uno mismo, porque no toda la privacidad puede ser escogida. Algunos tipos de privacidad son accidentales, compulsivos e involuntarios” (O’Brien 1979, 15-6).

El sistema estadounidense

El sistema legislativo estadounidense centra el derecho a la privacidad en el valor de la libertad, en especial, en la libertad de los ciudadanos frente a su propio Estado. Del mismo modo, la privacidad está íntimamente asociada a la noción de propiedad. Por ello, el derecho a la privacidad se enfoca en la libertad que los sujetos practican dentro de los muros de su propio hogar. Las expectativas de privacidad se ejercen dentro de la soberanía del hogar; por tanto, mientras la persona más se aleja de su casa más desprotegida está. Son las paredes del hogar las que le proporcionan su legítima expectativa de privacidad, del mismo modo que su ropa le ayuda a conservar la privacidad sobre su propio cuerpo.

Sin embargo, en la tradición estadounidense, el hecho de que las personas compartan información financiera no se considera un atentado contra el derecho a la privacidad. Todo lo contrario, un buen reporte de crédito hace la vida de las personas más fácil, un mercado con información es un mercado que ofrece los bienes y los servicios que la ciudadanía necesita de forma más eficiente.

Al contrario de la trayectoria europea, en Estados Unidos ni las normas sociales ni las regulaciones o el derecho parecen considerar a la prensa como el gran enemigo de la privacidad. En 1886, el presidente Grover Cleveland se casó con Frances Folsom; a partir de ese momento, la prensa y los anuncios publicitarios empezaron a utilizar la imagen de la popular primera dama de forma indiscriminada: en ceniceros, jabones, pastillas para el hígado, entre otros productos. Ante ello, el legislador John Thomas intentó pasar una ley que prohibía el uso de cualquier imagen femenina (viva o muerta) y proteger de este modo el derecho a la propia imagen de las mujeres. Sin embargo, esta ley no fue aprobada, lo que incrementó todavía más el uso del rostro de la primera dama (Lane 2009).

Otro ejemplo es el de Warren y Brandeis, quienes escribieron su artículo en respuesta a las publicaciones de un periódico local sobre la fiesta dada por los Warren. Así, reconocieron, en el chisme de la prensa amarillista, un nuevo fenómeno de intrusión en la vida familiar: “La prensa está sobrepasando, en todas las direcciones, los límites de la propiedad y la decencia [...] ocupando columna tras columna con chisme ocioso, producido a partir de intrusión del círculo doméstico” (Warren y Brandeis 1890, 196). En su artículo “The Right to Privacy”, ambos abogados proponen proteger a los individuos no solo de la prensa, sino también de fotógrafos y de las publicaciones no autorizadas por los ciudadanos.

¿Por qué esta primera propuesta del derecho a la privacidad no logra tocar el centro mismo de la cultura de la prensa libre? Si seguimos la línea de razonamiento de Warren y Brandeis, veremos que parte de la propuesta se basó en las ideas europeas sobre privacidad y, por tanto, apelaba a sensibilidades intuitivas que no funcionaban en el sistema estadounidense.¹³ A pesar de iniciar el artículo señalando que Estados Unidos carece de las protecciones a la privacidad que tiene Europa, los autores mantienen un hilo explicativo que recurre tanto a la tradición alemana, como a la francesa. Usan las fuentes alemanas sobre la personalidad —una de las vertientes más ortodoxas de la tradición¹⁴— y el honor— a través

¹³ Brandeis era hijo de inmigrantes de Bohemia que llegaron a Estados Unidos después de 1948; creció en una comunidad alemana, en Louisville, y estudió la secundaria en Alemania durante 1870; fue un gran admirador de la cultura alemana.

¹⁴ El autor citado es Salkowski, uno de los académicos alemanes que reinterpretan el antiguo derecho romano por medio de la filosofía alemana.

de la ley del insulto—. Del mismo modo, usan la legislación francesa de 1868¹⁵ para explicar la protección del buen nombre y la propia imagen. Y, finalmente, tratan de desarrollar estos valores, de la mano de los derechos de propiedad intelectual (*copyright*) y extenderlos a la protección de la privacidad de las personas.¹⁶ Su aporte a la literatura internacional fue muy importante —todavía hoy es citado por académicos europeos—, pero no logró fundamentar el derecho norteamericano desde los valores europeos. En gran medida porque no era posible trasladar a América la tradición de la ley del insulto o las ideas sobre honor personal que funcionaban al otro lado del Atlántico. También porque atentaba contra dos estructuras norteamericanas fundamentales: la prensa libre y el valor del libre mercado.

Para entender cómo funciona la protección de la propia imagen en Estados Unidos frente a la libertad de prensa, Nimmer (1954) desarrolla la invención doctrinal del derecho a la publicidad a mediados del siglo XX. Según esta doctrina, las personas tienen el derecho de propiedad sobre su propia imagen, pues la imagen misma debe considerarse, en términos propietarios, como una mercancía. Por tanto, si eres dueño de tu propia imagen puedes venderla, la imagen es protegida en relación con la propiedad, pero no con respecto al honor. Esta noción de la propia imagen es completamente diferente en la tradición europea, donde forma parte del derecho a la vida privada.

Lo que el derecho ha excluido

Los estudios antropológicos sobre la privacidad (Geertz 1976; Murphy 1984; Westin 1984) se han centrado en analizarla como un constructo social que intenta armonizar las necesidades de interacción de los individuos en sociedad y la búsqueda de espacios para sí mismos. Si bien las nociones contemporáneas occidentales sobre la vida privada estaban

¹⁵ El caso de Dumas padre era muy reciente. Según Withman (2004), Godkin utilizaba la jurisprudencia francesa para mostrar el derecho que tenían las personas de defender su propia imagen. “En Francia, un hombre puede prevenir o castigar la mera mención de su nombre, incluso si no es político o artista [...] existe un sentido del ridículo y del insulto que jamás ha existido en ningún país anglosajón” (Godkin 1890).

¹⁶ En la jurisprudencia de Estados Unidos ya se empezaba a reconocer el daño moral y el sufrimiento mental, al mismo tiempo que las invasiones a la propiedad, tanto física como metafórica.

ausentes en casi todas las culturas primitivas, esto no significa que no existieran otras formas de relación entre la necesidad de privacidad, de exposición y de control dentro de cada sociedad.¹⁷

Entre los factores comunes de las sociedades investigadas están las *normas de privacidad individuales y grupales*, para organizar la necesidad de privacidad que afecta varias áreas de la vida individual, familiar y comunitaria. Las personas buscan la compañía tanto como la posibilidad de estar solos, y estas normas ayudan a establecer los grados de distancia con los otros en ciertos puntos de la cotidianidad. Aunque las normas varían de una cultura a otra, lo que sí permanecen son las distinciones entre áreas de la vida social.

La configuración de estas normas también puede ser muy novedosa para nuestros parámetros. En sus estudios sobre Java, Geertz relata que

excepto por el sitio donde se cambian la ropa, ningún lugar de la casa es realmente privado [...] los javaneses no tienen, literalmente, ninguna protección física contra el mundo exterior. El resultado es que sus defensas son más bien psicológicas. Las relaciones dentro de la casa son muy restringidas; las personas hablan suavemente, escoden sus sentimientos e incluso, en el seno de una familia javanesa, uno siente que está en el centro la plaza pública donde uno debe comportarse con decoro. Los javaneses crean distancia con los otros a través de la etiqueta –sus patrones de cortesía son muy desarrollados– (citado por Westin 1984, 64-5).

El miedo al aislamiento, junto con la sensación de no estar totalmente solos en el mundo, es otro de los factores que los estudios antropológicos traen a colación en sus trabajos sobre privacidad. La necesidad de comunicarse con los espíritus o los dioses produce otras formas de *privacidad y reclusión* que podemos presenciar incluso en sociedades como las nuestras (en torno a la vida espiritual de las personas o las comunidades).

La predisposición a invadir la privacidad de los otros a través de la *curiosidad o la vigilancia* es otro elemento presente en estos análisis. Se encuentra que el chisme, una forma de obtener información privada de

¹⁷ Los trabajos realizados en Yale en 300 sociedades de distintas partes del mundo, integradas por 4000 personas analfabetas, muestran que existen algunos aspectos de la privacidad que están presentes en cada uno de los grupos humanos investigados; ello puede ser muy relevante para estudiar qué es la privacidad hoy en día (Westin 1984, 61).

los otros, está presente en prácticamente todas las culturas; en gran parte de ellas se establecen límites a dicha curiosidad. Así, existe una serie de mitos que ilustran las consecuencias de la curiosidad exacerbada, como la caja de Pandora o Eva y la manzana. Más allá de la curiosidad individual están también los procesos de control y de vigilancia que las autoridades ejercen sobre las personas y la capacidad de crear mecanismos sociales consensuados de invasión de la privacidad de los individuos para proteger al resto de miembros de la sociedad.

La literatura antropológica sugiere que el *paso de las sociedades primitivas a las modernas* aumenta las oportunidades de privacidad de las personas, tanto las físicas como las psicológicas. Los fenómenos vinculados a la Revolución industrial, como la familia nuclear viviendo en casas individuales, el anonimato y el crecimiento de las ciudades, la movilidad en el trabajo y en los lugares de residencia, así como el debilitamiento de la autoridad religiosa sobre las personas, ofrecen nuevas oportunidades de privacidad—física y psicológica— que no poseían los sujetos primitivos. Sin embargo, el refinamiento del orden social moderno también ha producido otras barreras, hasta no hace mucho desconocidas, como la capacidad del Estado de crear un control orwelliano sobre la vida de los otros, con sus capacidades militares, tecnológicas y económicas.

La privacidad ha sido abordada también como un *mecanismo de distanciamiento social*. Los trabajos de Robert Murphy son muy importantes para explicar cómo es reconocida e institucionalizada en todo tipo de sociedades, y lo esencial que resulta para mantener las relaciones con los otros y con uno mismo. Desde esta perspectiva, la privacidad es operativa y significativa no solo para los individuos, sino también para la propia sociedad, tanto en los vínculos íntimos como en las relaciones cotidianas. La novedad de la propuesta de Murphy es que concibe la privacidad como una precondition de los roles públicos y no solo como la simple antítesis de la acción en el campo público. Él observa cómo algunos roles públicos de las personas entran en conflicto con los más personales y la manera en que la privacidad resuelve el mantenimiento de los roles públicos de la persona.¹⁸ Un área de la privacidad es, entonces, mantenida por todos,

¹⁸ Su trabajo se basa en el marco conceptual propuesto por Simmel (1950, 312) de autorrevelación y autocontrol como cualidades necesarias para toda relación social. Para Simmel, la distancia está inversamente relacionada con la cantidad de conocimiento que otros puedan tener sobre uno.

y la reserva y moderación son factores comunes, aunque no constantes, en todas las relaciones sociales. La sociedad no podría perdurar si la gente supiera demasiado sobre el otro, y uno podría preguntar, siguiendo a Simmel, si el individuo pudiera perdurar como persona social bajo el peso de una completa conciencia del sí (Murphy 1984, 35).

Si la distancia se encuentra de manera pronunciada en las relaciones sociales ambivalentes, debemos encontrar otros sectores del sistema social y analizar la función de la distancia en la manutención del orden social.

Las autorrevelaciones de los actores están filtradas para producir lo que él llama “un teleológico no-conocimiento del otro”.

Capítulo 2

Controversias acerca de la privacidad desde el siglo XIX: su co-construcción

Aunque podría pensarse que la idea de la vida privada como la concebimos actualmente se remonta hacia muy atrás en la historia, esta noción es más bien una consecuencia de la Revolución industrial del siglo XIX que permitió hacer una distinción entre las esferas pública y privada de la vida de los individuos (Jolicoeur 2005, 6). A partir de ello se marcan los momentos históricos en los que es necesario redefinir la privacidad en relación con el cambio tecnológico.

En el siglo XIX, dos acontecimientos marcaron el ingreso de la tecnología en la vida cotidiana, lo cual afectó para siempre a la privacidad: el surgimiento de la *penny press* en 1830, en Inglaterra, y la aparición de la *snap camera*, hacia 1884, en Estados Unidos.

Los periódicos de un *penny* inglés masificaron el consumo de la prensa de un modo muy peculiar: eran más baratos y la gente podía pagarlos, a la vez que sus contenidos sensacionalistas estimularon la curiosidad de la población sobre la vida personal de los *otros*, dando paso al periodismo amarillista. El concepto de la *penny press* salta muy pocos años más tarde a Estados Unidos con el periódico *Sun* (1833), lo que dio lugar a la publicación de escándalos de todo tipo. Si tomamos en cuenta que antes de la Guerra civil no existía una amplia circulación de periódicos, el fenómeno que provocó esta prensa barata fue de gran importancia. En cuatro meses alcanzó una circulación equivalente a todos los periódicos de Nueva York. Entre 1850 y 1890, el tiraje de los periódicos aumentó en un mil por ciento; se pasó de 100 periódicos con un total de 800 000 lectores, a 900 periódicos con más de ocho millones de lectores.

En Estados Unidos la aparición de la *snap camera*, producida por la compañía Eastman Kodak, revolucionó el *acceso* a la fotografía para

miles de personas en el mundo. Robert Ellis Smith apunta: “en los años anteriores al desarrollo de la fotografía, a mediados del 1800, incluso los espejos no eran parte del mobiliario de las casas en Inglaterra o Estados Unidos. Imaginen el efecto que causó que, por primera vez, la esencia de la persona —su rostro— pudiera ser capturado por alguien y usado y controlado por cualquiera” (Smith 2004, 108). Seis años más tarde, la prensa hacía uso regular de las *snap cameras* para retratar tanto a personajes públicos como a las personas en la calle; ello sin necesidad de que el fotógrafo haga explícito su deseo de retratarlos y de mantenerlos en pose por momentos interminables.

Un famoso abogado y comentarista social, Edward Lawrence Godkin, cayó en la cuenta de que estos avances se habían tornado en un atentado contra la privacidad y sostuvo que “la curiosidad en sí misma se ha convertido en la mayor enemiga de la privacidad en la vida moderna”. Sostuvo, asimismo, que a diferencia de antes, cuando el chisme era expresado en forma oral y hería de forma tan solo superficial e individual, en la actualidad el chisme se imprime y esto provoca que la víctima, con todas sus imperfecciones, sea conocida a miles de millas de su lugar de origen (citado por Solove 2008, 108). El mismo Godkin sostiene que la privacidad es un producto moderno, “uno de los lujos de la civilización” (citado por Solove, Rotenberg y Schwartz 2006, 10).

El primer elemento que utilizamos para describir esta controversia son los artefactos sociotécnicos constituidos por la *penny press* y la *snap camera*. ¿Qué es lo que estos artefactos cambian con respecto a lo que los sujetos consideraban lo privado? Con las nuevas tecnologías aparecen grupos sociales relevantes, vinculados a las empresas de prensa y de fotografía, que intervienen en la modificación de las costumbres y de las formas de representación de lo privado. Los periódicos publican chismes, asesinatos, robos, que involucran tanto a la clase alta como al pueblo en general, mostrando datos e imágenes sin previa autorización de las personas involucradas. El segundo elemento es la reconfiguración de las normas sociales de la mano de la tecnología, el modo en que el estigma funciona de forma amplificada y, sobre todo, queda registrado en dos tipos de soportes tecnológicos: el papel y la fotografía, modificando así de manera radical la noción de vida privada.

En este contexto, grandemente influidos por los artículos de Godkin, en 1890 dos abogados jóvenes de Boston, preocupados por las consecuencias que estaban provocando tanto la prensa sensacionalista como la tecnología fotográfica y sus usos comerciales, escribieron un artículo en *Harvard Law Review* llamado “The Right to Privacy”.¹ A diferencia de Godkin, quien no reconoce una posible solución a los problemas de privacidad, Warren y Brandeis apelan al derecho para proteger la privacidad. Por lo visto, Warren tenía una motivación personal para escribir el artículo, pues el periódico *The Saturday Evening Gazette* constantemente publicaba artículos sobre las cenas que se ofrecían en casa del abogado, y otros datos acerca de su vida social (Solove 2008).

Que el individuo deba ser protegido en su persona y en su propiedad es un principio tan viejo como la ley; pero encontramos necesario, de tiempo en tiempo, definir de nuevo la naturaleza exacta y la extensión de dicha protección. Aunque en tiempos muy tempranos la ley remediaba solo problemas de interferencia física sobre la vida y la propiedad [...], el derecho a la propiedad aseguraba a los individuos su tierra y su castillo. Más tarde, vino el reconocimiento de la naturaleza espiritual del hombre, de sus sentimientos y de su intelecto. Gradualmente, el alcance del derecho se amplía; y ahora el derecho a la vida se ha convertido en un derecho a disfrutar de la vida –el derecho a ser dejado en paz–. El derecho a la libertad asegura el ejercicio de privilegios civiles extensivos, y el término “propiedad” llega a comprometer toda forma de posesión –intangible como tangible–. [...] Recientes invenciones y métodos de negocios nos llevan a dar el siguiente paso en lo que respecta a la protección de la persona, para asegurar al individuo lo que el juez Cooley denomina “el derecho a estar solo”. Las fotografías instantáneas y la empresa de los periódicos han invadido los sagrados recintos de la vida privada y doméstica; y los numerosos artefactos mecánicos amenazan con hacer cumplir la predicción de “lo que es murmurado en el closet será proclamado desde lo más alto de la casa”. [...] Es nuestro propósito considerar si la ley actual permite un principio que puede ser adecuadamente invocado para proteger la privacidad de los individuos; y si es así, cuál es la naturaleza y alcance de dicha protección (Warren y Brandeis 1890, 193-98).

¹ El artículo más influyente en la historia del derecho norteamericano (Mason 1946).

Ambos abogados reconocían que la ley no protegía a los ciudadanos frente al sufrimiento y al estrés que provocaban estas nuevas prácticas. El artículo referido llama la atención en el ambiente jurídico de la costa este de Estados Unidos y su concepto de privacidad es utilizado, tres años más tarde, por el Tribunal Supremo norteamericano para sentenciar a favor de un actor que demandó a un medio de prensa escrita por publicar una fotografía suya sin su consentimiento, basando su veredicto en el derecho del demandante a ser dejado en paz.

El tercer elemento de la controversia es la extensión de la privacidad, hasta el momento limitada a los ámbitos sociales, tecnológicos y culturales, a la esfera del derecho. Ello produce un nuevo cambio sociotécnico: *the right to be left alone*. La privacidad empieza a delinarse como el *derecho a la soledad* a partir de la obra del juez estadounidense Thomas Cooley, *The Elements of Torts* (1895) donde define la privacidad como el derecho de cada individuo a permanecer aislado, solo y no ser arrastrado a la publicidad;² y también a partir del artículo de Warren y Brandeis “The Right to Privacy”. Ambos textos serán citados más tarde como referencia para las sentencias de las cortes y los alegatos de los abogados, produciendo una acción a distancia que se reflejará en los cambios de legislación de la siguiente década:

1903 - La legislatura de Nueva York crea una acción de responsabilidad civil sobre privacidad por estatuto.

1905 - Georgia es el primer estado que reconoce una ley común de responsabilidad civil para las invasiones a la privacidad.

Por una parte, la tecnología y el cambio social producen regulaciones para tecnologizar el derecho a la privacidad; por otra, la regulación pasa a definir qué es lo privado y las expectativas sobre privacidad que los sujetos pueden tener. La *penny press* y la *snap camera*, la reconfiguración de la norma social y la extensión de la privacidad a la esfera del derecho son parte del proceso sociotécnico de co-construcción entre elementos heterogéneos, actores, artefactos, regulaciones y normas sociales (Oudshoorn y Pinch 2005; Thomas 2008; Vercelli y Thomas 2007).

² Cooley asocia el derecho a la soledad con todo aquello que se vive en privado, de espaldas al exterior, a lo público.

Si bien la noción del derecho a ser dejado en paz se estabiliza en la legislación norteamericana, este significado de la privacidad no hace otra cosa que abrir un debate sobre el concepto en sí. Ello ocurre a fines del siglo XIX y se extiende al siglo XX, configurándose un cuarto elemento de la controversia: las reflexiones sobre la privacidad. Como se verá, la privacidad es objeto de una flexibilidad interpretativa muy importante. La noción norteamericana original es aplicada, más bien, contra las intrusiones del Estado, tales como la inviolabilidad de domicilio y de la correspondencia. El respeto a la privacidad se considera una condición para el libre desarrollo de la personalidad y la protección de la vida íntima familiar y doméstica entre las paredes del domicilio (o dentro de un sobre cerrado). El *lugar privado* diferencia la vida pública de la vida privada de las personas, en este los sujetos pueden liberarse de los roles que juegan en público para construir su vida íntima. Y es en tal sentido que *el derecho a la opacidad* es una condición necesaria para la formación de la personalidad. En una época de transparencias y de sobreexposición del sujeto como la de finales del siglo XX, este derecho a la opacidad se vuelve particularmente relevante.³

Otra de las derivaciones importantes que ha tenido el derecho a la privacidad, como lo plantearon Warren y Brandeis, es la privacidad como una forma de protección de la *personalidad*. Desde la publicación de su artículo, se la relaciona con la inviolabilidad de la personalidad.

Sin embargo, no solo los juristas utilizan esta noción, lo hacen también varios filósofos, Reiman (1984, 300-14), por ejemplo, quien considera que la personalidad es un componente de la privacidad: “el derecho a la privacidad [...] protege el interés personal en convertirse, ser y permanecer como una persona”. Esta acepción de la privacidad se centra en la protección de la integridad personal y muchas veces ha sido utilizada para reforzar otros significados del término, en particular aquellos cuyo centro es proteger al individuo de la interferencia del Estado.

La privacidad ha sido conceptualizada para salvaguardar aquello que puede ser protegido. Así, desde sus primeras facetas, la vida privada se

³ El derecho de la persona a la opacidad ha sido considerado, en ciertos casos, negativo, en particular en la literatura jurídica feminista; así, esta ha denunciado la violencia doméstica que han sufrido las mujeres y la incapacidad del Estado de protegerlas, pues al respetar la vida privada y familiar, se ha abstenido de tomar acción (Mackinnon 1989).

vincula con la noción de *intimidad*, y con ello se intenta garantizar las circunstancias que la posibilitan. La privacidad como intimidad es lo que desborda la personalidad moral más allá de la simple autonomía racional (Denning 2010), porque valoramos la privacidad para mantener diferentes niveles de intimidad con los otros y desarrollar nuestras relaciones personales. La intimidad permite compartir, con aquellos que escogemos, la información sobre nuestras propias acciones, credos y emociones. El derecho a la privacidad crea «el capital moral que invertimos en la amistad y el amor» (Fried 1970, 142). Así, el énfasis hecho en el contexto de amor o amistad en que se comparte la información íntima es lo que permite distinguirla de otros tipos de relación personales; por ejemplo, la información que una persona pueda compartir con su psicoanalista no necesariamente convierte esta relación en una relación íntima (Reiman 1984).

La controversia analizada tuvo lugar en los Estados Unidos en la segunda mitad del siglo XIX; por tanto, se trata de un proceso socio-técnico situado, en el que intervienen una serie de actores, tecnologías, regulaciones y normas sociales concretas. La privacidad se co-construye entre las tecnologías que intervienen en la controversia,⁴ los actores sociales que toman posturas y reaccionan contra las nuevas formas de exposición pública de las personas,⁵ y las doctrinas y sentencias que juristas y jueces empiezan a diseñar con respecto al derecho a la privacidad.

Sin embargo, esta controversia está lejos de cerrarse. Como he expuesto, los significados que adquiere la privacidad, en vez de contribuir a formular definiciones, amplían el espectro.

Autonomía en la toma de decisiones

La segunda controversia acerca de la privacidad está vinculada con el desarrollo de las comunicaciones y los artefactos tecnológicos que las acompañan. En este acápite analizo cómo el uso del teléfono por parte

⁴ En este caso, las técnicas de masificación de la prensa escrita y la tecnología fotográfica de la cámara portátil de Kodak.

⁵ El crítico social Godkin, los abogados Warren y Brandeis, el juez Cooley y los sujetos que iniciaron acciones legales contra las empresas de prensa.

de los granjeros estadounidenses, a principios del siglo XX, ayudó a visibilizar la flexibilidad interpretativa sobre lo público y lo privado, que deviene del cambio tecnológico de las comunicaciones, y cómo el debate jurídico acompañó la construcción de lo que la sociedad fue considerando privado.

La introducción del teléfono en Estados Unidos implicó grandes desafíos comerciales, tecnológicos y sociales. La nueva tecnología era significada por los actores sociales de forma muy diversa y su estabilización como un medio de comunicación común del siglo XX atraviesa los debates sobre lo público y lo privado, del mismo modo que sobre la aceptación o resistencia a la tecnología.

El fenómeno urbano de la telefonía involucró varios tipos de intromisión en la privacidad. El primero, el cambio de la visita personal anunciada a la llamada telefónica imprevista, puso en discusión las características intrusivas de la nueva tecnología ante las posibilidades de invasión del domicilio por parte de quienes hacían la llamada. El segundo fue la falta de privacidad sobre el contenido de la llamada, pues la conversación estaba mediada por un sistema de escuchas de las operadoras que posibilitaban la comunicación. El tercero, las normas sociales que deben desarrollarse en la resistencia y domesticación de la tecnología, así como los cambios que esto implica en la construcción de lo privado.

La resistencia de los usuarios a la tecnología⁶ es un aspecto común del proceso de creación técnica y del cambio social. A través de la resistencia, los beneficiarios negocian, de forma interactiva, el cambio sociotécnico con los otros actores sociales (mediadores, productores). La resistencia se visibiliza, según Kline (2005), a través de la oposición a la introducción de la nueva tecnología en la comunidad, la no-compra de esos aparatos y en el uso de la tecnología de manera no-prescrita.

De esta forma, la incorporación de la telefonía en las ciudades operó bajo las dos primeras formas de resistencia. Para las compañías

⁶ Por ejemplo, la resistencia de los artesanos luditas en Gran Bretaña, en las primeras décadas del siglo XIX (Bauer 1995); de los esclavos (Dew 1994), de los artesanos (Randall 1986), de los granjeros (Scott 1985) y otros grupos marginales que se resistieron a ser explotados por la tecnología. Los granjeros del centro-oeste norteamericano destrozaron maquinaria en la crisis económica de 1870 (Argersinger y Argersinger 1984) y los amish, en Pensilvania, todavía se rehúsan a la introducción del teléfono dentro de sus casas (Kraybill 1989).

teléfónicas vencer esa reticencia de la población consistía en lograr negociar socialmente el uso masivo a la tecnología bajo el precepto de *una línea de teléfono por casa*. Tanto productores como mediadores lograron que el teléfono funcionara en esta modalidad dentro de la ciudad. En este modelo, si bien la privacidad estaba comprometida por la intermediación de la operadora, no existía la posibilidad de que la conversación fuera escuchada en tiempo real por otras personas. Así, la segunda negociación es vencer la resistencia a que un tercero escuche aquello que debía ser dicho en privado.

En el campo norteamericano, en cambio, se presentó la tercera forma de resistencia: el uso de la tecnología de manera no prescrita. El modelo de una línea por casa no iba a funcionar, pese a no existir gran resistencia a la compra del artefacto por parte de los granjeros. Así, cuando las compañías operadoras del servicio, como AT&T (American Telephone and Telegraph Company), eran lentas para ofrecer telefonía, fueron los propios granjeros quienes empezaron a construir sus propias líneas de teléfono, comprando los equipos y organizando cooperativas para establecer sistemas de comunicación en los vecindarios. Incluso cuando las compañías comerciales empezaron a construir líneas de teléfono rurales, tuvieron que subdividir cada línea en 10 y hasta en 20 compartidas.

Mientras las personas de la ciudad usaban el teléfono de manera individual y se cuidaba la privacidad de las conversaciones, en el campo del centro-oeste norteamericano se privilegiaba un sistema de escuchas en el que participaba cada vecindario. La resistencia se encuentra, de este modo, justo al centro de la flexibilidad interpretativa, pues no todos los usuarios de telefonía conciben la tecnología del mismo modo: “Los grupos sociales relevantes no ven simplemente los diferentes aspectos de un artefacto. Los sentidos otorgados por un grupo social relevante ‘constituyen’ el artefacto. Hay tantos artefactos cuanto diferentes grupos sociales relevantes” (Bijker 1995, 77).

Así, grupos de granjeros norteamericanos concibieron al teléfono de un modo completamente diferente que los usuarios urbanos; por ello, además de no asumir el rol de “simples consumidores” de la tecnología, fueron capaces de convertirse en mediadores, al formar cooperativas para tener el servicio pronto, y se convirtieron en creadores de tecnología

autónoma al inventar la posibilidad de compartir líneas de teléfono, aun cuando las compañías no habían diseñado la tecnología para hacerlo. Mientras, en la ciudad las compañías comerciales se encargaban de desarrollar la tecnología en una relación de uno a uno con las familias interesadas.

De esta manera, la norma social del campo se sofisticó en un “extraño código de etiqueta que defendía las escuchas [...] lo que explica por qué muchos granjeros se negaban a contratar un servicio estrictamente privado” (Kline 2005, 56). De alguna manera, el sistema de escuchas trasplantó la costumbre rural de las visitas a la línea telefónica en muchas comunidades hasta bien entrados los años cuarenta del siglo XX. Lo que en la ciudad se consideraba una intromisión en el hogar por parte de la tecnología, en el campo se recibía como una reinención de la socialización entre vecinos. El contenido de las llamadas no se consideraba privado sino público, y se aceptaba la participación de la comunidad en un sistema diseñado, en principio, para excluir a los otros.

Productores y mediadores habían estructurado un sistema de uso del teléfono que se cumplía en la ciudad, pero que no lograba estabilizarse en el campo. Ello obligó a las compañías de teléfonos, en 1909, a rediseñar la tecnología de las zonas rurales.⁷ Si bien muchas empresas se encargaron de aumentar las trabas para las escuchas, otras decidieron no interferir con esta práctica social; más bien, desarrollaron tecnología que la volviera más eficiente, en un claro ejemplo de co-construcción sociotécnica.⁸

La telefonía en Estados Unidos ha sido definida a través de los sentidos sociales generados por los grupos en la interacción con sus artefactos tecnológicos (líneas, regulaciones, corporaciones, etc.). Su estabilización se ubica en la década de los cuarenta como un medio de comunicación

⁷ En 1910 se llevaron a cabo pruebas de baterías, donde se sugería aumentar el valor de la cuenta de teléfono si las baterías se acababan antes de 10 meses. Asimismo, se introdujeron, sin éxito, aparatos que detectaban las escuchas con el fin de intimidar a quienes compartían sus líneas. En 1914 se diseñaron sistemas de señalización que permitían hacer sonar solo al teléfono que tenía contratada la línea y no a los otros teléfonos compartidos (Kline 2005, 57).

⁸ L. Spalding de la compañía Bell de Pensilvania propuso al jefe de ingenieros de AT&T el cambio de las bobinas de inducción # 13 por unas de calibre 10. Ello mejoró el volumen de las líneas rurales en el supuesto de que “es muy probable que exista gran cantidad de escuchas en los circuitos por terceras personas” (Kline 2005, 58).

individual y privado (no sujeto a sistemas de escuchas). El teléfono terminó desempeñándose de una manera bastante homogénea entre los grupos sociales, pero su funcionamiento “no debe ser considerado la causa de su éxito, sino el resultado de haber sido aceptado por grupos sociales relevantes” (Bijker 1993, 119).

Sin embargo, hasta el día de hoy, los usos rurales del teléfono no han terminado de estabilizarse de acuerdo con las intenciones de inventores, usuarios y mediadores. Un ejemplo de la no clausura de esta tecnología y de su relación con lo privado es el uso del teléfono en la comunidad amish. En otras palabras, la construcción social del artefacto no ha logrado una clausura total, porque tal proceso significa la disminución de su flexibilidad interpretativa. Aunque en el resto de la sociedad eso aconteció hace más de setenta años, para los amish, el teléfono tiene un sentido totalmente distinto. Por tanto, aunque el consenso sobre el sentido del teléfono es muy alto y adquiere mayor estabilización en términos macro, en esta comunidad aún es un artefacto en controversia. En el caso de este grupo etnorreligioso, el uso no prescrito del teléfono tiene que ver con el no-uso de otras tecnologías ya estabilizadas desde hace décadas en el resto de la sociedad, como la electricidad, la radio o la televisión. Así, para los amish proteger el hogar del teléfono tiene el objeto de preservar el orden social de su comunidad.

Los amish se organizan a través de comunidades de agricultores que mantienen una tradición oral muy fuerte y una comunicación cara a cara. Sus distritos no son más grandes que el número de personas que una casa pueda albergar para sus reuniones. Por tanto, el uso del teléfono no es considerado una necesidad para la comunicación entre su gente, sino como una facilidad para hacer negocios y evitar viajes innecesarios a la ciudad. Su “estilo de vida” los lleva a revisar la innovación tecnológica con mucho cuidado, como un modo de controlar su propia “evolución estructural para enfrentarse a cada grupo significativo de posibilidades tecnológicas” (Winner 2008, 101). El teléfono estuvo detrás de la división de la iglesia amish en 1910, en la que se perdió a una quinta parte de sus miembros⁹ (Kraybill 1989). Los pastores de la

⁹ A quienes abandonaron la antigua orden amish, en 1910, se los conoció como los *Beachy Amish*, y aceptaron con el tiempo otras tecnologías todavía prohibidas por los amish: los carros y la electricidad.

antigua orden sostenían que el teléfono no era una necesidad y, puesto que venía de afuera, los miembros de la comunidad tendían a relacionarlo con los forasteros, lo cual contribuía a fomentar el orgullo y el individualismo. Lo interesante del caso amish es que no se prohíbe el uso del teléfono, sino que se impide que sea instalado *dentro* de la casa. Es esta “intrusión” en el hogar y en la privacidad de las familias amish lo que se protege incluso con el riesgo de perder gran número de miembros de la comunidad.

El uso del teléfono tiene la peculiaridad de ubicarse en pequeñas casetas denominadas *shanties*, al lado de los graneros o cerca del garaje de un vecino no-amish. Las *shanties* son compartidas entre seis o siete familias y manejadas cuidadosamente por los líderes de su iglesia. La segunda singularidad de este uso es que no se permite recibir llamadas, solo es consentido hacerlas:

Si se posee un local de negocios y se necesita un teléfono, este debe instalarse fuera del local, y si se instala en la granja, tiene que ser público para poder compartirlo con otros. Es solo que no está permitido dentro de la casa, sino ¿dónde terminaría esto? Nos preocupamos por mantener las cosas pequeñas y la familia unida (descripción del uso del teléfono por un miembro de la comunidad amish, citado en Kraybill 1989, 149).

La flexibilidad interpretativa del caso amish revela que una tecnología no tiene un sentido universal hasta que no es construida o negociada socialmente. Además, la negociación de la aceptación y el uso del nuevo artefacto reestructura también la interacción social de los grupos (Zimmerman Umble 1992). Aunque han transcurrido más de cien años, la privacidad del hogar sigue siendo un factor fundamental de la cultura amish y es defendida ante la intromisión de tecnologías que puedan afectar el orden social de la comunidad. Las reglas sobre la propiedad del teléfono resaltan la lucha por quién tiene autoridad sobre qué campos del conocimiento y de la información. Su debate continúa poniendo a prueba a los pastores de la Iglesia amish y su capacidad de regular las prácticas sociales

una ‘cosa’ aparentemente no-ambigua (un proceso técnico, una condición material del metal, etc.) es mejor comprendida al ser considerada como diferentes artefactos. Cada uno de estos artefactos, ‘oculto’ dentro

de la misma 'cosa', puede ser rastreado (*traced*) a fin de identificar los sentidos atribuidos por los diferentes grupos sociales relevantes (Thomas 2008, 234).

En tal sentido, qué es privado y qué es público dentro de la comunidad se acuerda entre todos los miembros, tratando de ser fieles al estilo de vida escogido. Ello incluye opciones como la de prohibir tecnologías que podrían naturalizar prácticas sociales inaceptables.

La concepción de la privacidad como el derecho a ser dejado en paz se resignifica con el uso del teléfono de las zonas rurales, donde no se diferencia entre comunicaciones privadas y públicas como sí se hace en la ciudad. El teléfono se domestica integrándose en la vida cotidiana, es decir, pasa de su estadio desconocido y hasta amenazante, a formar parte de la cultura, las prácticas y las rutinas de todos los días.

Tanto en el campo como en la ciudad, la domesticación del teléfono implicó un trabajo simbólico en el que los sujetos crearon sentidos del artefacto y adoptaron o transformaron los sentidos inscritos en la tecnología (a través de usos no prescritos, por ejemplo). Mediante un trabajo práctico, desarrollaron patrones de uso para integrar el teléfono a su vida cotidiana y, gracias a una labor cognitiva, aprendieron sobre la tecnología (y en ciertos casos rediseñaron su modelo de negocios, como en las cooperativas de telefonía rurales en Estados Unidos). De esta manera, la domesticación fue un proceso de dos vías: cambiaron los sujetos y también el artefacto tecnológico. "El uso del aparato puede cambiar el sentido y la función simbólica del artefacto, y puede permitir o impedir *performances* de identidad, negociaciones de estatus y posición social" (Oudshoorn y Pinch 2005, 14).

De acuerdo con Silverstone (1992), quien acuña el término de domesticación de la tecnología, esta implica su apropiación, objetivación, incorporación y conversión. La apropiación del artefacto tecnológico *teléfono* se ejerce a través de la propiedad del aparato en las zonas urbanas, y compartiendo líneas en ciertos ámbitos rurales. La objetivación del teléfono revela las normas, los principios y el sentido que se le confiere como nueva tecnología, de forma situada dentro del espacio familiar. Según Silverstone, la objetivación otorga al artefacto tecnológico su lugar en el mundo; mientras que la incorporación lo vuelve parte

de la rutina cotidiana, naturalizando la tecnología hasta llegar al máximo estadio de la domesticación: la conversión, donde el uso del objeto tecnológico modela las relaciones entre usuarios y personas fuera de la casa. La domesticación me ayuda a explicar cómo funciona la apropiación tecnológica dentro de la economía moral de la casa, por medio de un proceso multidinámico en el que el artefacto debe ser ubicado en un espacio concreto, tiene que ser interpretado –esto es adquirir valor simbólico– y debe ser integrado a las prácticas sociales.

El teléfono es una de las nuevas tecnologías que contribuye al debate sobre el derecho a la privacidad en la primera mitad del siglo XX, en particular en lo referente al establecimiento de las libertades que tienen los sujetos sobre la comunicación que consideran privada.¹⁰ Así, se cuestiona qué informaciones deben ser protegidas y se reconoce el derecho que tienen los individuos de que su propiedad y su vida privada sean protegidas. La privacidad en este punto se acerca al estereotipo del propietario, en el que su hogar y la propiedad de la línea de teléfono contribuyen a configurar el espacio de lo privado y, por extensión, la información que en este espacio se produce como privada.

La noción jurídica del derecho a la privacidad se desarrolla en paralelo al concepto del acceso limitado a uno mismo. Este hace referencia al deseo de la persona de mantener sus asuntos fuera del alcance de los demás. Se diferencia así del derecho a la soledad, porque no es equivalente a ninguna forma de reclusión (Poulet y Rouvroy 2009). En el caso de la telefonía urbana vemos que el acceso limitado a uno mismo es muy importante en el desarrollo de las comunicaciones telefónicas, mientras que en las zonas rurales, este concepto no es aplicado a las llamadas de teléfono porque los usuarios no las consideran de carácter privado.

Esta controversia de la privacidad se organiza alrededor de otros actores: empresas telefónicas, consumidores, diseñadores de tecnología y las regulaciones. Entonces, ¿qué se entiende por privado en el uso del teléfono en Estados Unidos de fines del siglo XIX y principios del XX?

¹⁰ El derecho a la vida privada no se aplica a las publicaciones realizadas por un organismo público o destinado para el público, como es el caso de un cuerpo legislativo, una corte de justicia, una asamblea municipal, por ejemplo. Del mismo modo, si un individuo decide volver pública una comunicación, no podrá ampararse en su derecho a la vida privada porque está renunciando a él implícitamente (Warren y Brandeis 1890).

Esta percepción, en su incorporación a la economía moral de la casa, variará notablemente entre los sujetos urbanos y algunos sujetos rurales durante más de cuatro décadas (en la comunidad amish, incluso durante una centuria). La flexibilidad interpretativa de la privacidad está atravesada por la resistencia y domesticación de la nueva tecnología, del mismo modo que por el valor social que se le atribuye al teléfono como forma de relacionamiento social. La resistencia urbana está marcada por el carácter intrusivo de la tecnología dentro del hogar; mientras que la resistencia rural, por una forma de apropiación no prescrita de la tecnología. Los diseñadores responden de forma heterogénea a ambos tipos de resistencia: en la ciudad ofrecen una tecnología más individual (una línea por casa), en el campo una tecnología más comunitaria (permiten la línea telefónica para varios usuarios). El acceso limitado a uno mismo y la protección a la información que los sujetos consideran de carácter privado son algunos de los significados que adquiere la privacidad dentro de la controversia.

Un nuevo actor dentro de la controversia: el Estado

Hasta ese momento el Estado había permanecido ausente de esta segunda controversia de la privacidad, en gran medida porque las tecnologías que habían acompañado el cambio social (*penny press*, fotografía, teléfono) se consideraban “neutras”: por sí mismas, no ponían en riesgo la moral y la ética ciudadanas.

Ello, sin embargo, cambia notablemente con el desarrollo de otras tecnologías más sensibles en términos morales: los métodos anticonceptivos. La autonomía en la toma de decisiones fue una versión de la privacidad que tuvo que decidirse en la corte de Estados Unidos para proteger a la persona de las injerencias del Estado. Fue necesario definir una dimensión de inmunidad del sujeto que le permitiera vivir como le pareciera y encargarse de sus asuntos a su manera. El respeto a la faceta de inmunidad de la vida privada pone en escena la noción de libertad. El propio Estado debe respetar que las personas vivan según sus propias preferencias y esquemas de valores, siempre y cuando sus prácticas no sean ilegales.

El primer precedente jurídico que ratifica el respeto del Estado por la privacidad de los ciudadanos fue el caso *Griswold vs. Connecticut*.¹¹ La Corte Suprema invalidó una ley del Estado de Connecticut que prohibía a las parejas casadas el uso de anticonceptivos y consagraba el derecho a la vida privada como un derecho constitucional. Estelle Griswold y Lee Buxton¹² habían sido declarados culpables en primera instancia, según la ley de Connecticut, por ofrecer información sobre métodos anticonceptivos a parejas casadas, y prescribir anticonceptivos a varias mujeres, lo cual era considerado un crimen bajo dicha legislación, en 1961. En la sentencia, la Corte Suprema estableció que la ley de Connecticut era inconstitucional, porque la cuarta y la quinta enmiendas protegen la vida privada de los individuos frente a la interferencia gubernamental.

En este caso, la decisión del juez Douglas se basó en dos factores que él reconoció inquietantes. El primero es la intrusión en la esfera privada, que la policía entrara en la habitación de la pareja para constatar una eventual violación a la prohibición de usar métodos anticonceptivos. El segundo es la intrusión del Estado en los espacios privilegiados del matrimonio. Su sentencia, entonces, tuvo dos interpretaciones; por un lado, la de los conservadores cuya prioridad es proteger la institución del matrimonio; por el otro, la de los liberales quienes consideraban que la intromisión de la policía en la habitación es un tema periférico y que el centro de la sentencia es la autonomía en la toma de decisiones sobre temas individuales existenciales.

Los anticonceptivos son el segundo artefacto sociotécnico que me permite analizar cómo la privacidad se configura a mediados del siglo XX en la sociedad estadounidense, ya no solo a través de la interacción entre pares, diseñadores y corporaciones, sino mediante el involucramiento de las cortes, la academia, las organizaciones no gubernamentales y los ciudadanos. El caso *Griswold vs. Connecticut* es particularmente relevante porque presenta la privacidad como un bien que debe ser defendido incluso del propio Estado. La flexibilidad interpretativa de la privacidad por parte de la ley de Connecticut y la jurisprudencia

¹¹ Número de expediente 281 US 479 (1965).

¹² La primera, directora ejecutiva de la Liga de Planificación Familiar; el segundo profesor y médico de la Universidad de Yale y director médico de la Liga de Planificación Familiar.

que asienta la Corte Suprema resulta fundamental, porque visibiliza versiones muy diferenciadas de qué es la privacidad desde dos instancias jurídicas del mismo Estado, ambas capaces de organizar y estructurar a la sociedad de acuerdo con sus propios principios. Este caso es paradigmático porque sienta un precedente sobre las atribuciones que el Estado norteamericano se toma sobre sus ciudadanos, así como de las diferencias de su trayectoria sociotécnica con respecto a la de otros países.

La autodeterminación y las expectativas de privacidad

A mediados del siglo XX, el cambio tecnológico empieza a tocar otros aspectos de la vida privada de los ciudadanos. En la década de los sesenta, los Estados adquieren la capacidad de reunir información sobre los individuos a través de bases de datos, se desarrollan sistemas de vigilancia y de escuchas más sofisticados y la jurisprudencia de las cortes sienta las bases de lo que se considera “privado” no solo en la retórica, sino también en la práctica.

A pesar de las diferencias entre la cultura jurídica europea y la estadounidense, la *autodeterminación* y la *construcción autónoma de la personalidad* son los valores esenciales que fundamentan el respeto a la privacidad en ambos lados del Atlántico. La esencia del respeto a la vida privada es “la pretensión de la existencia de una parte del espacio que no será destinado al uso público del control” (Konvitz 1966, 272). Ello no solo por parte del Estado sobre la ciudadanía, sino en las relaciones *entre* ciudadanos.

Sin embargo, Europa y Estados Unidos, frente a los mismos retos del cambio tecnológico, desarrollan regulaciones y principios legales muy diferenciados. Por esta razón, analizo la trayectoria sociotécnica de la privacidad en cada lugar. Estados Unidos opera según el principio sociológico de legítimas expectativas de privacidad, mientras que Europa lo hace con el de evaluación normativa.

El sistema de valores sobre el que se fundamenta el desarrollo de la legislación norteamericana acerca de la privacidad tiene como centro la libertad, en particular la *libertad frente al Estado*. Se trata de la que se ejerce en “la santidad del hogar”, donde se ubica a la vida familiar

y particular, una especie de “soberanía privada dentro de las propias paredes”. La privacidad mantiene todo su poderío en el hogar y su mayor riesgo es la intrusión de los actores gubernamentales (la policía y otros oficiales del Estado) en esa esfera (Withman 2004). Al contrario de la trayectoria europea, ni las normas sociales ni las regulaciones o el derecho parecen considerar a la prensa como el gran enemigo de la privacidad.

En 1962, el científico de los laboratorios Bell Telephone de New Jersey sostuvo, en el simposio *El hombre y la computadora*, que recoger y procesar información en los ordenadores estaba cambiando la naturaleza de la privacidad personal en los Estados Unidos. El desarrollo de la tecnología multimedia y de las bases de datos, en la década de los setenta, provocó un nuevo pliegue en la compleja tarea de definir qué es lo privado desde las prácticas y las regulaciones. Los servicios de inteligencia gubernamentales, las corporaciones privadas, las compañías de seguros, el sistema de rentas o del seguro social son algunos de los actores involucrados en este cambio social y tecnológico.

Así, se ampliaron las prácticas de monitoreo de la ciudadanía. Ello condujo a que la Corte Suprema aceptara casos que contribuyeran a sentar jurisprudencia sobre la existencia de un derecho a la protección de la vida privada basado en el criterio sociológico de la existencia de *legítimas expectativas de privacidad* que tiene como centro las expectativas sociales (Poulet y Rouvroy 2009). De acuerdo con este principio, la privacidad no solo se sostiene en las expectativas de cada sujeto, sino también en los intereses que la sociedad considera razonables; solamente se estabilizan las expectativas que esta reconoce.

Para algunos autores y juristas, se trata de un estándar volátil porque simplifica el derecho a la vida privada en los ámbitos de protección y control que tiene una persona en un tiempo y espacio específicos. Tal es el caso de los lugares en donde se han instalado cámaras de videovigilancia; al margen de que tal instalación sea legítima o no, estas disminuyen el grado de protección de la vida privada de las personas. Por ello, las expectativas de privacidad y su aplicación son “inversamente proporcionales a la intensidad del despliegue tecnológico”; a más tecnología menor privacidad, a menor tecnología mayor privacidad (Poulet y Rouvroy 2009, 164-65). Así, en las sociedades donde los sistemas de vigilancia

son más invasivos, los individuos tienen menos capacidad de hacer respetar su privacidad, pues su legítima expectativa de hecho disminuye o se anula una vez que el modelo de vigilancia se instala;¹³ las *expectativas de privacidad* no serían otra cosa que el derecho de los individuos a no ser “sorpresa” por los sistemas de vigilancia, ahí donde ignoren que existen (Poullet y Rouvroy 2009).

Uno de los casos que sentó mayores precedentes sobre este punto fue el de Katz vs. Estados Unidos. En los años sesenta del siglo XX, los sistemas de escuchas empezaron a volverse práctica común por parte del FBI (Federal Bureau of Investigation) y otras agencias gubernamentales en la investigación y seguimiento de casos delictivos. El dilema que el caso presentó en la corte fue si el FBI había violado la cuarta enmienda de la Constitución al colocar un sistema de grabación en una cabina de teléfono pública, sin permiso de la corte. Charles Katz, acusado de apuestas interestatales, objetó la introducción de artefactos de escucha para usarlos como evidencia en contra suya, y ganó el caso. El argumento detrás de la defensa fue el control que tiene el individuo sobre la información que le concierne, el poder de decidir qué información sobre sí mismo desea divulgar, su facultad incluso para rehusarse a volverla pública (Lane 2009).

Como hemos visto, las tradiciones legales europea y estadounidense responden a diferentes culturas de privacidad, con lo cual producen dos sistemas jurídicos únicos. El marco jurídico europeo tiene como centro del derecho a la privacidad el respeto a la dignidad personal, en particular el *derecho a la propia imagen, nombre y reputación* (el derecho a la autodeterminación informacional). Asimismo, está vinculado al control de la imagen pública y al derecho a que la gente nos vea del modo en que deseamos ser vistos. Dentro de este sistema de valores, el primer enemigo son los medios de comunicación (Withman 2004).

A pesar de que ambos sistemas llegan a conclusiones similares, lo hacen partiendo de perspectivas muy diferentes y de un entendimiento distinto de cómo la privacidad cuenta en la sociedad. El derecho americano gira sobre el concepto de libertad, especialmente en torno a las incursiones que pueda realizar el Estado en la vida privada a través de la policía y otros oficiales estatales. El derecho europeo lo hace, en cambio,

¹³ Una persona que es filmada por una cámara en un espacio público y que ha sido informada no tiene posibilidad de reclamar expectativas de privacidad en ese lugar y momento específico.

alrededor de problemas referentes a la dignidad pública, el honor y la posición de los individuos en la sociedad (Withman 2004).

La información, una forma de clausura de la privacidad

Hacia la segunda mitad del siglo XX evoluciona la conceptualización del derecho a la privacidad; así, el individuo aislado del resto de la sociedad y las libertades individuales dejan de ser los únicos referentes. A partir de la Segunda Guerra Mundial, la intimidad es vista también como la posibilidad de *control de la información personal* (Pérez Luño 1984).

El aspecto positivo de la intimidad sirve precisamente de fundamento al denominado “derecho a la autodeterminación informativa” o también “libertad informática”; tal derecho persigue la protección de la intimidad personal y la consolidación de una plena capacidad del individuo sobre cualquier ámbito de su personalidad, lo cual redundaría en una protección íntegra de la vida privada (Ballester 1998, 51).

Esta acepción de la privacidad en gran medida está fundamentada por una preocupación que surge en los años sesenta: las bases de datos que poseen el gobierno y otras instituciones importantes (Nissenbaum 2010), porque la privacidad se vincula a tecnologías digitales que tienen un gran poder sobre la información de las personas. Estas tecnologías tienen tres capacidades relevantes: monitorear y seguir a los sujetos; agregar y analizar información en tiempos muy cortos; y, diseminar y publicar información.

Los *sistemas de monitoreo y seguimiento* de las personas son cada vez más sofisticados; existen cámaras en gran parte de los lugares públicos y dentro de las áreas comunes de los edificios, somos controlados con tecnología biométrica cuando cruzamos la frontera, tenemos sensores de movimiento y calor en nuestras casas. La propia información se ha convertido en una forma de monitoreo, en una manera de *dataveillance* (Clarke 1988). La tecnología ha permitido la democratización¹⁴ de formas de *dataveillance*

¹⁴ Por democratización se entiende en este acápite a la expansión del acceso a un mayor y diverso espectro de la comunidad de usuarios (Nissenbaum 2010).

antes inimaginables o inaccesibles, por ejemplo, de padres preocupados por sus hijos; gracias a servicios como Chaperone, ofrecido por Verizon en Estados Unidos, los padres monitoreaban dónde van sus hijos cuando salen fuera de casa. La misma tecnología celular ofreció oportunidades de seguimiento más lúdicas, como la incorporación de cámaras o grabadoras en los aparatos móviles. Los propios automóviles poseen, en la actualidad, cajas negras (del estilo usado en los aviones) que hacen seguimiento de las acciones del conductor; los EDRs (*electronic data recorders*) fueron instalados en los autos a partir de la implementación de las bolsas de aire, sin embargo, gran parte de los conductores no conocía que sus vehículos estaban dotados con este sistema.¹⁵

El ciberespacio es otro lugar de monitoreo y seguimiento todavía más sofisticado. A pesar de que pueda generar una noción de anonimato, cada paso queda registrado automáticamente. Miremos, por ejemplo, los proveedores de ruta en los sitios web (que nos brindan las calles y el suelo por donde caminamos en línea): ellos graban cada ventana que se visitó, el tiempo que se permaneció en cada sitio, el orden del recorrido, etc. DoubleClick es una de las compañías que explota la funcionalidad de las cookies que se instalan en el computador de los sujetos durante sus visitas a distintos sitios web. Amazon.com al guardar las preferencias de sus usuarios y cruzarlas con la información de otros clientes con preferencias similares provoca una especie de relación personal con el sitio, una sensación de familiaridad que hace la visita más confortable.

Las *prácticas de agregación y análisis de la información*, en un principio concentradas en muy pocas instituciones, se democratizaron entre las décadas de los setenta y ochenta. En 1973, cuando eran todavía muy restringidas, el Departamento de Salud, Educación y Bienestar Social encargó un reporte sobre récords, computadoras y los derechos de las personas. Este informe tuvo como objetivo convertirse en referencia de una política pública para equilibrar los beneficios que ofrecían las bases de datos y dichos derechos. Uno de los puntos más importantes que ofreció el reporte es el Código de Prácticas Adecuadas sobre la Información, en el cual aparecen los cuatro principios más importantes sobre la

¹⁵ Desde el año 2006, el Departamento de Transporte de los Estados Unidos obligó a las compañías de autos a informar a sus clientes de la existencia de EDR en sus vehículos (Nissenbaum 2010).

recolección y uso de los datos personales que darían forma a las políticas de privacidad en el mundo entero: a) prohibición de bases de datos secretas, b) la reutilización de la información con propósitos diferentes a los del momento de recolección, c) demandar seguridad adecuada de su información, d) permitir que las personas accedan a su información y que inspeccionen y corrijan sus récords.¹⁶

Otro punto importante del Código fue el reconocimiento de actores significativos y las trayectorias de regulación que ellos han apoyado. Así, el gobierno y ciertos actores del sector privado (bancos, compañías de seguros, de telecomunicaciones, entre otras) aparecen como los grandes poseedores de información, de la tecnología para recolectar información de forma unilateral y gestores también de la protección de los datos de las personas. Por tanto, se trataba de poderosos artefactos al servicio de actores sociales y políticos dominantes que tenían acceso a información de casi cualquier persona.

Sin embargo, la trayectoria de las prácticas de recolección y uso de la información es cuestionada por las propias instituciones, que se sienten vulnerables y desprotegidas frente a lo que se pueda hacer con sus datos. Así, el deseo de privacidad entra en juego al poco tiempo de iniciarse los mecanismos de monitoreo y concentración de la información, justamente porque se vislumbra el poder que sobre ella tienen las grandes instituciones. Si bien con la democratización del uso de bases de datos, parte de este escenario desaparece, estos grandes actores todavía son los que mayor uso hacen de la información de las personas.

La movilidad de la información es otro elemento que entra en acción. Los datos en formato electrónico-digital se emiten desde puntos totalmente diversos, también pueden accederse desde múltiples lugares. Entonces, la agregación de la información da paso a los *dossiers* o carpetas digitales (Solove 2004). Con la creación de los perfiles, cada vez más sofisticados gracias a la triangulación de la información proveniente de distintas bases, se intenta no solo configurar a los sujetos, sino también predecir lo que harán. Esta práctica fortalece a toda una industria dedicada a la recolección y análisis de información, que ofrece servicios

¹⁶ Alan Westin fue uno de los miembros del Comité que elaboró el reporte. Coloco esta referencia por el valor de los aportes de Westin y la importancia de su producción para este libro.

a otros sectores de la sociedad. Un ejemplo es Acxiom Corporation, una empresa con cobertura de datos de multifuentes sobre millones de hogares y millones de personas en decenas de países, que incluye información demográfica, propiedades, comportamiento de compra y *estilo de vida*; también ofrece un servicio al gobierno estadounidense denominado “mitigación del riesgo” que, con objetivo proteger a América, entrega información personal, de trabajo, de la comunidad y de seguridad nacional, incluso aquella información sensible “permitida por la ley” (Nissenbaum 2010).

El efecto de agregación al que hace referencia Solove consiste en la configuración de la carpeta digital, algo más que la suma de la información que recoge y, por ende, ensaya recrear distintas biografías. “Nuestras biografías digitales son unas biografías no autorizadas, solo parcialmente ciertas y muy reductivas [...], nuestras biografías digitales están siendo creadas por las compañías que amasan información personal y récords públicos entre otros tipos de datos” (Solove 2004, 46-7); pero lo más grave, como ya lo indicaba el jurista Kenneth Karst en los sesenta, es que “se convertirán en los únicos hechos significativos al momento de investigar a las personas” (citado por Solove 2004, 48).

Datos personales

En el estudio realizado por Slobogin y Schumacher (1993) sobre la coincidencia entre las expectativas de privacidad de la ciudadanía y las que había sentenciado la Suprema Corte, evidencian que no hay coincidencia entre ambas.¹⁷ Los ciudadanos, en la práctica, presentan una dicotomía entre lo que piensan y lo que hacen, “aunque las personas en las encuestas expresan un fuerte deseo de privacidad, están listas a negociar la por

¹⁷ En 1990, el 79 % de los encuestados respondió que sí a la propuesta: “si la Declaración de Independencia se escribiera hoy ¿estaría de acuerdo en añadir ‘privacidad’ al lado de vida, libertad y deseo de felicidad?” (Westin y Harris 1990).

En 1998, las personas entrevistadas respondieron “de algún modo” o “mucho” a la pregunta: “¿cuán preocupado está usted sobre las amenazas a la privacidad en América hoy en día?” (Westin y Harris 1998).

El año 2000, el 85 % de las personas encuestadas respondieron “de algún modo” o “mucho” a la pregunta: “¿le preocupa que las empresas y las personas que usted no conoce obtengan información personal sobre usted y su familia?”. Y el 54 % se opuso al monitoreo y búsqueda de personas por

conveniencia, entregando información personal a cambio de pequeñas recompensas” (Acquisti y Grossklags 2007, 15-6).

Los defensores de la privacidad argumentan que aquello que los escépticos reconocen como una opción, no son acciones deliberadas ni libres. No es justo caracterizar una opción como deliberada cuando la alternativa no es viable o las personas simplemente no están bien informadas. En el año 2003, el 57 % de las personas que participó en una encuesta creía que si una compañía tenía términos de privacidad no compartía la información de sus clientes con otras empresas; el 59 % no sabía que los sitios web recolectaban su información, incluso si no se habían registrado en el sitio. En 2005, otra encuesta reveló que el 75 % creía que si un sitio web tenía una póliza de privacidad no podía vender la información de sus usuarios; el 73 % pensaba que los bancos estaban prohibidos por ley de vender información de sus clientes sin su autorización y un 64 % indicaba lo mismo para el caso de los supermercados y las bases de datos de sus clientes (Nissenbaum 2010, 105-6).

El derecho a la vida privada es uno de los más complicados de definir, justamente por el escaso consenso al momento de su reconocimiento. Uno de los primeros problemas con los que nos topamos es la relación que se establece entre la vida privada y la información personal. Por otra parte, la protección de la vida privada se ha considerado, con frecuencia, el modo de determinar hasta qué punto el Estado o los otros individuos pueden inmiscuirse en los asuntos de una persona.

Así, existen dos textos claves para estudiar la protección de los datos personales: las Líneas directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre protección de la privacidad y flujos transfronterizos de datos personales de septiembre de 1980; y el Convenio 108 del Consejo de Europa (CE) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de enero de 1981. En los preámbulos de ambos textos aparecen

internet. El año 2003, el 86 % de las personas entrevistadas apoyaba una ley que le diera a las personas el derecho a controlar cómo los sitios web usan su información (Turrow 2003).

Otros estudios en cambio muestran otros datos: solo un 20 % de las personas lee las pólizas de privacidad de los sitios donde interactúa y únicamente un 7 % se queja de ellas. Los escépticos están convencidos de que las personas actúan de forma distinta a como se expresan en las encuestas: en casi todas las situaciones donde la gente tiene que escoger entre privacidad y otro bien, ellos eligen el otro bien.

dos grandes objetivos: la protección de la vida privada y las libertades individuales (Convenio del CE), y la libre circulación de la información (Líneas directrices de la OCDE). Dos objetivos que aparentemente se contradicen, pero que en la legislación internacional deben armonizar entre sí.

Por una parte, las Líneas directrices de la OCDE establecen principios sobre la recolección, utilización y gestión de los datos personales y representan un consenso internacional sobre estos temas. En general, han generado códigos de conducta a escala mundial sobre recolección y uso de datos personales, pero su definición y campo de aplicación son tan generales que la noción de dato personal varía de un país a otro y, lo que es más grave, su campo de aplicación cambia notablemente dentro de épocas y contextos socioeconómicos diferentes. En primer lugar, definen como dato personal cualquier información relacionada con un individuo identificado o identificable (sujeto de los datos).¹⁸

En el artículo 2 de ese documento se especifica el campo de aplicación en los siguientes términos: “estas directrices aplican a datos personales del sector público o privado, que debido a la forma en que se procesan, a su naturaleza o al contexto en que se usan, suponen un peligro para la privacidad y las libertades individuales”. A primera vista, esta disposición parecería atenuar el efecto global que tenía el primer artículo; propone que solo los datos que representen un peligro sean tomados en consideración, pero no hay ninguna referencia sobre los criterios que definen, con precisión, los datos peligrosos para la vida privada y las libertades individuales. La vertiente de la normativa internacional que vincula la vida privada con la protección de datos personales, tomando como referencia las Líneas directrices de la OCDE, deja poco claro qué se entiende por vida privada y qué parte de ella merece una verdadera protección. La simplificación de la noción de vida privada a dato personal, además de ser ambigua y parcial, no define los conceptos de vida privada ni de libertades personales.

Por otra parte, en el Convenio 108 del CE se definen los datos de carácter personal como “cualquier información relativa a una persona física identificada o identificable”, definición casi idéntica a la de

¹⁸ Parte 1, “Definiciones generales”, Líneas directrices de la OCDE, <http://bit.ly/1HWG9Qk>.

la OCDE.¹⁹ La convención europea hace más énfasis en garantizar la seguridad de los datos acumulados, pero al igual que en el documento de la OCDE no contiene indicaciones de cómo aplicar las normas propuestas. De este modo, cada país se compromete a adoptar los principios dentro de su propia legislación y a crear las instituciones que velen por dichos derechos.

En cuanto al derecho positivo, el Parlamento y el Consejo europeos definen la vida privada como “el derecho del individuo a una vida retirada y anónima” o “el derecho de ser dejado solo a vivir su propia vida con un mínimo de interferencias de los otros”.²⁰ Así, el derecho positivo europeo no supera las dificultades que tienen los otros precedentes normativos internacionales. Lo que sí queda claro es que se trata de armonizar la protección de la vida privada de los individuos y la circulación de sus datos personales.

De esta manera, lo que entendamos por vida privada deberá permitirnos hacer frente a las amenazas que puedan surgir contra la dignidad y la autonomía de las personas, teniendo en cuenta plenamente el contexto dentro del cual nuestras libertades deban ser explicadas (Solove 2002). “La privacidad será aquí simplemente aquello que el individuo hace de la libertad que se le reconoce. No es definible *a priori*: su ámbito de aplicación solo aparece a través de los conflictos que suscita su ejercicio” (De Schutter 1999, 839).

La necesidad de conceptualizar qué es la privacidad tiene un tinte pragmático importante: diseñar soluciones legales para problemas particulares (Solove 2008). En tal sentido, en vez de ser considerada desde una aproximación abstracta, puede ser abordada de manera pluralista desde los problemas que se vinculan a ella. Estas dificultades donde la privacidad está en juego, según Solove, son una alternativa para zanjar la vaguedad que la aproximación abstracta ofrece y es, también, un mecanismo efectivo para legislar y crear política pública que proteja la privacidad.

Como hemos visto, parece casi imposible definir qué es la vida privada, pero esta dificultad no impide que el derecho renuncie a protegerla.

¹⁹ Capítulo primero, “Disposiciones generales”, art. 2, inciso a, <http://bit.ly/1HSfZo2>

²⁰ Directiva de 1995 (95/46 CE) del Consejo Europeo, 31-50, <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:31995L0046>

La doctrina se centra en definir los contenidos que son relevantes al derecho de la protección de la privacidad, especialmente dentro del contexto social donde son protegidas las relaciones individuales de autonomía. En este sentido, el respeto a la vida privada es también un derecho fundamentalmente *relativo*.

La *pretensión de privacidad* expresa, así, el deseo de controlar a los otros. Incluso sus mayores defensores la describen como el derecho a controlar el flujo de información sobre sí mismos.

La gente se vende a sí misma del mismo modo que vende productos [...]. No hay tal cosa como el deseo de las personas a ser dejados solos, muy pocas personas quieren estar solas. Ellos quieren manipular el mundo a su alrededor, seleccionando formas de presentarse a los otros (Solove, Rotenberg y Schwartz 2006, 51-2).

Capítulo 3

Ciberespacio y redes sociales

Según el Manifiesto del Ciberespacio del año 2002, no era posible que los gobiernos regularan internet, incluso si intentaban legislarlo, no tendría efectos reales. El ciberespacio aparecía como un lugar que se disputaba el utopismo libertario: “libertad sin anarquía, control sin gobierno, consenso sin poder [...]. Rechazamos: reyes, presidentes y votos. Creemos en el consenso bruto y en el código que funciona”.¹ Ya Lessig (2006) explicaba en su libro *Code 2.0* que sí era susceptible de regulación, y lo que había que replantear era la noción de regulación hacia el código informático, y, desde ahí, comprender que la ley del ciberespacio se basaba justamente en el código.

Lessig se preguntaba entonces si el ciberespacio iba a prometer privacidad o acceso, libertad de expresión o cultura permisiva, o cómo su arquitectura iba a regularnos especialmente frente a las constantes transformaciones. Reconocía una primera generación de codificadores que provenían del sector no comercial, herederos de la cultura *hacker* y constructores del ciberespacio; a quienes le siguen una generación regida por el comercio; y, finalmente, una tercera que está alineada con los gobiernos.

En un inicio, la propia naturaleza de internet hizo que la regulación fuera muy difícil, pero hoy, luego de años de estandarización de protocolos y de lenguajes digitales, el ciberespacio se ha convertido en un lugar cada vez más sofisticado de regulación. Y es justamente la arquitectura de los lugares del ciberespacio la que puede ejercer mayor control

¹ “The Cyberspace Manifiesto. A Manifiesto and Declaration of the Sovereignty of Cyberspace”, 31 de diciembre de 2002, acceso el 27 de mayo de 2015, (blog desaparecido de la web).

sobre los individuos. El problema es que “no estamos entrenados para pensar cómo las distintas tecnologías pueden alcanzar el mismo objetivo a través de modos diferentes”, y esto es lo que confunde nuestra intuición de modo peligroso (Lessig 2006, 31-2).

Los primeros cambios hacia una naturaleza de control en internet fueron orquestados por el comercio. En 1995, con la ley alemana que reguló la pornografía se escribió el futuro de internet. Hasta ese año, los proveedores de dicho servicio no tenían la capacidad de filtrar la información a la que podían acceder sus usuarios en sus servidores. CompuServe, presionado por la ley alemana, fue el primero en producir la tecnología que impedía a usuarios de Baviera acceder a la información depositada en sus servidores y con ello bloquear, tan solo a ciudadanos alemanes, el contenido pornográfico que sus servidores tenían en todo el mundo. CompuServe desarrolló una tecnología capaz de reconocer en dónde estaban físicamente sus usuarios y qué estaban haciendo, les impidieron acceder a contenidos en línea por medio de una tecnología de filtros aplicados país por país.

Con ello se marcó un antes y un después en el uso del ciberespacio. Desde ese momento fue imposible continuar siendo invisibles, el anonimato y la libertad de movimientos en el ciberespacio dejaron de ser una opción. Del mismo modo que dicha invisibilidad había sido una opción de los codificadores, estos debían producir códigos de control cada vez más estrictos para sostener los negocios en línea a los que servían, como el caso de CompuServe. El sujeto digital invisible que imaginó la cultura *hacker* había desaparecido. El anonimato ya no era una condición propia del ciberespacio, de hecho actualmente, requiere de grandes esfuerzos por parte de los sujetos y es casi imposible obtenerlo porque la arquitectura de la web vuelve rastreables las acciones que operamos en ella.

Tales cambios, si bien fueron condicionados por las leyes de los gobiernos, en realidad se diseñaron para alcanzar los objetivos comerciales de las empresas. Este conjunto de actores se constituyó, así, en un grupo social relevante en el desarrollo de la arquitectura de internet. Desde 1995 “quién hizo qué y dónde” (Lessig 2006, 39) fue el fundamento de las tecnologías de identificación en línea, en cuya base están tres nociones fundamentales: identidad, autenticación y credenciales. La identidad se asienta en una serie de atributos como edad, nombre, sexo,

dirección, educación, número de identificación, profesión, preferencias de compra en línea, etc. Una vez que estos atributos se transmiten a otros deben volverse creíbles, y para ello es necesario implantar procesos de autenticación de los datos transmitidos a través de artefactos estándares como las credenciales. Estas tres nociones tienen el propósito de elevar el grado de confianza sobre los datos que se transmiten y, con ello, permitir que los propios Estados puedan también obtener información sobre su ciudadanía, en caso de ser necesario, dentro de los circuitos comerciales creados en el ciberespacio. Los procesos de autenticación se han vuelto cada vez más importantes también en el mundo social, debido al incremento del uso del ciberespacio para fines lúdicos. Una vez que las dinámicas de sociabilidad se extienden a los mundos virtuales, habitarlos implica, asimismo, permitir procesos de autenticación cada vez más sofisticados. Queremos evitar que otros se hagan pasar por nosotros y gustosos aceptamos establecer ciertas garantías contra el fraude en línea.

Entender cómo funcionan los conceptos de identidad y de autenticación en la web, implica revisar los protocolos que los vuelven posibles. Transmission Control Protocol (TCP)/ Internet Protocol (IP) son los que permiten el intercambio de paquetes de información entre dos computadoras: identificada la información, el sistema la divide en partes más pequeñas (paquetes) y registra la dirección desde la que se origina la información y la dirección a la que se envía. La transmisión de la información se ejecuta a través de *routers* que identifican las direcciones y realizan el envío.

Los arquitectos de la web, Jerome Saltzer, David Clark y David Reed, quienes diseñaron el principio detrás de estos protocolos, lo denominaron *end-to-end principle*. Se trata, en pocas palabras, del principio más importante que rige internet. Su naturaleza minimalista ha permitido que otros protocolos y lenguajes puedan anidarse sobre él sin generar conflictos.

El IP no revela por sí mismo la identidad de las personas, pero permite que el ISP (Internet Service Provider) o el proveedor de internet que lo asignó puedan rastrear las actividades realizadas en línea. Esto es posible gracias a que antes de asignar ningún IP, los ISP “registran” al dueño del IP a través de contratos de servicios. Esta tecnología resulta

muy valiosa para una empresa, particularmente en relación con la publicidad y la focalización de productos. De este modo se inventó el mapeo de los IP que permite localizar desde dónde navegan los cibernautas; ello facilita no solo a las empresas, sino también a los gobiernos, información que rebasa las fronteras de lo virtual sobre las personas. Pero ¿se había consultado a los usuarios si querían ser rastreados? ¿Se había debatido los beneficios o problemas de dicho rastreo para las personas? Todas estas tecnologías, desarrolladas al margen de esas voluntades, fortalecieron los sistemas de control en internet hasta niveles poco pensados por quienes navegamos en línea.

Otra tecnología que permite rastrear a los sujetos en línea son las *cookies*. Surgieron en 1994, igualmente, para resolver una necesidad de las empresas: incrementar su negocio. En ese año, Netscape creó un protocolo que les permitió a los servidores depositar una pequeña cantidad de información en las computadoras (las *cookies*), que empezaba a reportar los sitios web por los que se navegaba. Con ello los servidores adquirirían información muy valiosa que podían vender a las empresas sobre los hábitos de navegación de sus usuarios. Aunque el cambio del diseño era muy pequeño en la arquitectura servidor-cliente, sus consecuencias eran inconmensurables por el potencial de control que había generado. Las *cookies* son registradas casi por todos los sitios web que navegamos, y si en una de esas visitas entregamos información personal, esta también es recogida por las *cookies*. Así, el sitio web “sabe” quiénes somos cada vez que ingresamos.

Para lograr procesos de identificación todavía más poderosos se inventó la tecnología del *single sign-on* (SSO); con ella las personas logran una serie de privilegios una vez que ingresan a un sitio web. En vez de ser considerado un visitante que tiene restricciones de acceso a ciertos lugares e informaciones del sitio web, el SSO entrega a los usuarios una credencial para recorrerlo sin reservas. Según Lessig (2006), el SSO ha sido muy importante para consolidar los procesos de identificación en internet.

No obstante, Microsoft fue la compañía que consolidó las prácticas de identificación en la web con su proyecto Identity Metasystem, con el cual creó todo un nivel destinado a la identificación, complementó los ya existentes y produjo un nuevo tipo de funcionalidad. Con su protocolo

permitió que las personas se identifiquen a través de una arquitectura que selecciona tan solo las credenciales necesarias para cada acceso. Para ciertos lugares, únicamente se requiere el número de identificación, el correo electrónico y el nombre de la persona. Para otros, en cambio, el sistema entregará el número de tarjeta de crédito, la dirección y el teléfono, por poner un ejemplo. Aunque fue Microsoft quien diseñó el protocolo, una vez en la web puede ser emulado por cualquiera, porque se ha convertido en parte de la infraestructura de internet. De este modo refleja fielmente la arquitectura más básica de la red: cualquiera puede construir niveles de complejidad mayores sobre los principios básicos, como el TCP/IP. Con tecnologías baratas de autenticación en línea, la frecuencia de acciones que no requieran procesos de identificación disminuye drásticamente.

La capa de internet dedicada a la identificación se basa en tecnologías de encriptación. Sobre la ambigüedad de esta tecnología, Baker y Hurst alertaron: “la criptografía es de lejos la mejor y la peor de las tecnologías. Puede detener crímenes y crear nuevos. Puede debilitar las dictaduras y también llevarlas a nuevos excesos. Puede volvernos anónimos y puede seguir cada una de nuestras transacciones” (citados por Lessig 2006, 53).

Ello debido a que la criptografía funciona en relación con la “confidencialidad” como una forma de mantener la comunicación secreta; con respecto a la “identificación”, tiene como fin prevenir la falsificación de las identidades. Esta dualidad también se refleja en función de la regulación, pues cuando se trata de confidencialidad queda afuera, pero cuando se hace cargo de la identificación permite una regulación muy estricta.

En los primeros años de internet, la encriptación servía básicamente para mantener secreta la información y estaba directamente relacionada con la privacidad. Pero tiempo más tarde, en su fase comercial, la encriptación se ha vuelto parte de las tecnologías que han contribuido a fortalecer la capa de identificación de la web como el protocolo IPv6; que contiene una función de identificación para rastrear cada paquete de información en internet, volviendo prácticamente imposible el anonimato en línea.

Dentro de una arquitectura TCP/IP existen cuatro capas funcionales, de abajo hacia arriba: enlace de datos, red, transporte y aplicaciones. La plomería de internet se basa principalmente en las tres primeras capas,

dentro del nivel de enlace de datos son muy pocos protocolos los que operan; en la red, el protocolo dominante que habilita la información para vehicularla de un punto a otro es la trayectoria determinada mediante el IP; y en la capa de transporte son dos los protocolos más sobresalientes: el TCP y el UDP (User Datagram Protocol), ambos operan del mismo modo, solo que el UDP es menos confiable pues ofrece pocas garantías. La cuarta capa de aplicaciones alberga más protocolos, entre los más importantes: el FTP (File Transfer Protocol), SMTP (Simple Mail Transport Protocol), http (Hyper Text Transfer Protocol); esta capa regula en gran medida cómo nos conectamos de computadora a computadora, incluye *browsers*, sistemas operativos, módulos de encriptación, sistemas de correo, Java, P2P, entre muchos otros.

Gran parte del desarrollo de estas tecnologías está vinculada a la necesidad de las empresas de adaptarse a las medidas que los gobiernos les han impuesto para su operación en internet. El caso de la ley alemana sobre pornografía es un claro ejemplo. Pero algo que todavía no se ha discutido en este texto es la capacidad no solo de las empresas, sino también de los gobiernos de normar el comportamiento de las personas fomentando el cambio de la arquitectura de la web. Puesto que muchas veces es muy difícil para el gobierno lograr modificaciones en la conducta de la ciudadanía tan solo a través de la ley, ha promovido la invención de nuevos códigos de programación para lograr este objetivo. Promover una arquitectura que facilite regular el comportamiento de las personas es posible gracias a la alteración del código en cualquiera de las capas de internet. En el caso norteamericano es interesante notar cómo el FBI ha trabajado más con los reguladores desde que las cortes sentenciaron en contra de ciertas prácticas que el buró federal mantuvo para conseguir acceso a la información de las personas.

Los gobiernos pueden intentar normar el comportamiento de forma indirecta, al regular directamente los códigos utilizando su arquitectura con el propósito de volver más regulable la conducta de las personas. Esto conlleva entender que la naturaleza de la regulación es dinámica, que los individuos pueden resistir de muchas maneras, unas veces enfrentando la fuerza del código personalmente, otras resistiendo a través de otro código. Los protocolos de compartición de datos P2P son códigos que han ayudado a debilitar la efectividad de las regulaciones de *copyright* o derechos de

autor. Así unas veces el código funciona como ley, otras como mecanismo antirregulatorio para minimizar el costo de la ley.

Cuando el código se pone al servicio de las empresas empieza a ser controlado, justamente porque las empresas son objeto de control por parte del Estado. Y es ahí cuando los diseñadores de código empiezan a jugar un papel fundamental en este tipo de regulación. El profesor Jonathan Zittrain escribió en 2006 el artículo “La Internet Generativa”, donde sostuvo que las computadoras y las redes *end-to-end* generaban una plataforma generativa de invención extraordinaria, en la que hasta ese momento habían sobresalido las buenas experiencias y habían sido menos visibles las posibilidades de ejercer el mal dentro de la plataforma.² Me llaman la atención inventos como Hotmail creado por un inmigrante indio, o Google diseñado por los desertores de la Universidad de Stanford. Sin embargo, en los últimos años se ha visto cómo gusanos y virus han infestado millones de computadores en el mundo, creando desconcierto, pérdida de información y riesgos nacionales de filtración de información. Pero Zittrain se preguntaba ¿qué es lo que ha impedido que los diseñadores de código produzcan un daño irreparable a internet, cuando todos sabemos que esto sí es posible? Del mismo modo que la Patriot Act solo pudo entrar en vigencia luego de un ataque como el de septiembre de 2001, aunque gran parte de su texto había sido escrito mucho tiempo antes, la total regulación de internet no será viable hasta que ocurra un *cyber-Armageddon*.

Ha sido más fácil acostumbrarse al crecimiento de la web sin que cuestionemos verdaderamente hacia dónde nos lleva. Ello ha significado naturalizar los controles que se han ido gestando en el ciberespacio como parte del paisaje virtual, sin que lleguemos a imaginar su increíble capacidad de vigilancia. ¿Nos hemos preguntado cómo es capaz de funcionar como ley, no solo condicionando, sino determinando lo que las personas pueden o no hacer dentro de la red de redes? ¿Nos hemos interesado por el modo en que el poder actúa dentro de esta arquitectura, quiénes ejercen ese poder, cómo funciona? La arquitectura del ciberespacio es, en sí misma, una forma de poder; por ende, quien controla el código tiene el poder.

² Este enfoque se denominó la “teoría Z”, en honor de Zittrain.

Para Lessig, los diseñadores de código son hacedores de ley. Entonces lo importante es conocer cómo el código regula, quién lo escribe y quién controla al diseñador del código. Pues son los escritores de código quienes

determinan cuáles son y serán las configuraciones de internet, si la privacidad será protegida, el nivel de anonimato que será permitido, el alcance del acceso que será garantizado. Son ellos quienes van a construir su naturaleza. Sus decisiones, que ahora tienen lugar en los intersticios en donde se codifica la Red, definen lo que es la Red (Lessig 2006, 79).

Un caso en el que se puede revisar esta afirmación es el de China y Google. El gobierno de esa potencia asiática ha encontrado un mecanismo para trabajar con el buscador de información en línea más importante del mundo. Google ha desarrollado un código que evita que la información que ese gobierno censura salga en los resultados de búsqueda que realiza la ciudadanía china. Este mecanismo de filtro de información no es explícito, de modo que para un cibernauta en China no es posible conocer qué información no ha podido ser publicada en Google. Así, cada vez que realiza una búsqueda solo aparece la información no censurada, haciéndole pensar que esa es “toda” la información que existe sobre el tema. Google ha diseñado la tecnología que ayuda a China a controlar lo que pueden ver sus ciudadanos y se ha beneficiado, por otra parte, de servir a ese amplísimo mercado. El principio que rige esta relación es el del mercado y no el de “neutralidad de internet”. La regulación sirve tanto al mercado como al gobierno a través del código, ya que este se ha convertido en un regulador, un definidor de los términos en los que se puede ocupar los lugares en el ciberespacio. Funciona al modo de las fronteras nacionales, norma quiénes y cómo pueden acceder al territorio. Los códigos pueden también condicionar cómo se accede a los objetos digitales y los modos de interacción de dichos objetos. Lo que no pueden hacer los sujetos que habitan los mundos virtuales es cambiar los códigos que rigen dichos espacios ni demandar un balance de todo aquello que el código les quita.

El inicio de internet fue posible gracias a que los códigos que se diseñaron eran abiertos, y aunque el código implica control, el abierto permitía a los usuarios ser conscientes de dicho control. La cultura de

los diseñadores de código juega entonces un rol fundamental en cómo se ha diseñado internet, ya que actúa como un mecanismo para crear independencia; “los valores que operan dentro de un espacio determinado no son solamente los valores de la libertad de expresión, de la autonomía, del acceso o de la privacidad. Son los valores que limitan el control” (Lessig 2006, 152).

Origen de las redes sociales

Licklider y Taylor³ se preguntaban, en 1968, en su artículo “La computadora como un artefacto de comunicación”, cómo serían las comunidades interactivas en línea. Los autores especulaban, en esa época, en que estarían conformadas por miembros separados geográficamente pero unidos por intereses comunes. Se adelantaron, así, al imaginar el concepto de red social cuando avizoraban: “ya no se enviarán cartas o telegramas, simplemente se identificará a las personas cuyos archivos estarán vinculados a los de uno” (Licklider y Taylor [1968] 2001, en línea).

Rheingold acuñó en 1987 el término *comunidades virtuales*, como producto de su participación en *The Well*, definiéndolas como “un grupo de personas que puede o no conocerse cara a cara y que intercambian palabras e ideas a través de la mediación de computadores y redes” (Rheingold 2008, 5). Muchas de las conexiones que se establecen tienen que ver con “lazos latentes” (Haythornthwaite 2005) o contactos fuera de la web, y con mantener los lazos de su nueva red social en línea.

Desde la introducción de los sitios web de redes sociales (Social Network Sites-SNSs) se volvió popular una gran variedad de sitios temáticos, así como de prácticas culturales y tecnológicas. Unas incorporaron blogs, fotos, video, conectividad en teléfonos celulares, pero todas han estructurado la red a partir de perfiles personales que consisten en páginas únicas donde las personas pueden “escribir para existir” (Sudén 2003, 3). Los perfiles se construyen entregando información personal en formatos que la red solicita con datos como edad, ubicación, intereses, fotos, entre otros.

³ Taylor fue uno de los fundadores de ARPAnet, que más tarde se convertiría en la internet.

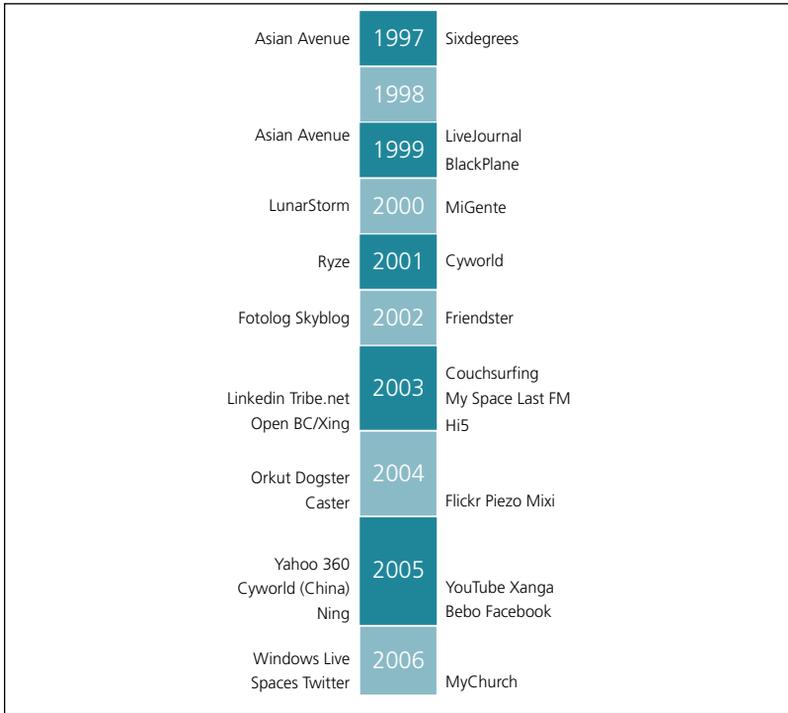
Usenet fue la primera red que permitió a las personas enviar mensajes a grupos con tópicos específicos. En 1982, Minitel empezó a funcionar en Francia como servicio nacional en línea del servicio postal francés; en 1985, AOL (America Online) inició su servicio en Estados Unidos y llegó a dominar el mercado al permitir a sus usuarios interactuar entre ellos. El servicio de mensajería instantánea empezó a conectar a las personas en línea, unas veces con sus verdaderos nombres, otros a través de pseudónimos. Las comunidades en línea se fortalecieron con la *www* (World Wide Web) y aparecieron Geocities, Tripod o The Globe, sitios web que permitían abrir páginas personales que se podían vincular con otras creadas por los usuarios. Match.com surge en 1994 para ayudar a encontrar pareja y Classmates.com en 1995 para encontrar a los antiguos compañeros de escuela.

Sin embargo, fue en 1997 cuando la era de las redes sociales verdaderamente se inició con Sixdegrees.com. que conectaba personas con sus nombres reales y proyectó las características que más tarde definirían una red social: “un servicio donde los usuarios pueden construir un perfil público o semipúblico, articular una lista de otros usuarios con quienes se comparte una conexión, navegar sobre la información de sus conexiones y con aquellos que son parte del sistema” (boyd y Ellison 2007, 212). Ello implicó establecer un perfil dentro de un contexto de relaciones que no necesariamente estaba orientado a conocer nuevas personas, sino a articular y volver visibles las redes sociales de cada usuario. Sixdegrees fue el primer servicio en línea que intentó identificar y mapear relaciones “verdaderas” entre gente “real”, lo cual fue visionario para su época (Kirkpatrick 2010). Tenía dos aplicaciones que organizaban la conexión entre usuarios: Connect Me, para ver el mapa de relaciones con las personas con quienes se quería conectar, y Network Me, que conectaba a personas con los mismos intereses y perfiles.

En poco tiempo, las redes sociales se multiplicaron y aparecieron AsianAvenue, BlackPlanet, MiGente, LiveJournal (gráfico 1); algunas funcionaban a escala local como la red coreana Cyworld o la sueca LunaStorm. Aparecieron también redes temáticas que, según Festa (2003), se apoyaban mutuamente porque no competían entre sí, como Ryze,⁴

⁴ Basada en comunidades tecnológicas, emprendedores e inversionistas.

Gráfico 1. Surgimiento de las redes sociales



Tribe.net,⁵ LinkedIn⁶ y Friendster.⁷ Muchas adoptan el modelo basado en los perfiles para replicar el éxito de Friendster y para llegar a diferenciarse demográficamente, varias se enfocan en personas que hacen negocios como Xing, VisiblePath o LinkedIn, otras se centran en conectar personas a través de sus intereses como Dogster, Couchsurfing,⁸ MyChurch,⁹ Flickr,¹⁰ Last.FM.¹¹

⁵ Ayuda a compartir información de los clasificados de Craigslist entre conocidos, para comprar lo que otros venden.

⁶ Organiza perfiles profesionales.

⁷ Red de amigos.

⁸ Conecta a los viajeros para que lleguen en casas particulares.

⁹ Vincula a las iglesias cristianas y sus miembros.

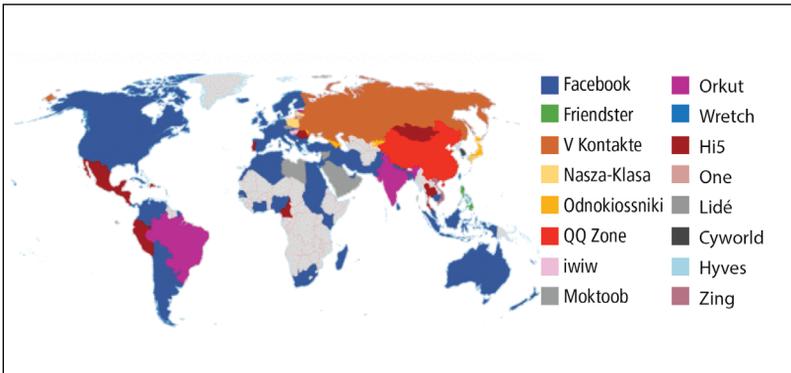
¹⁰ Para compartir fotos.

¹¹ Crea comunidades de amantes de la música a través de blogs y de organizar sus gustos musicales.

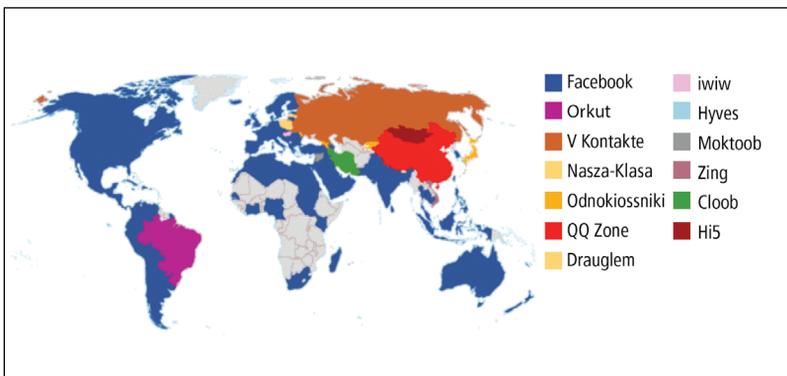
Algunas redes no lograron tener éxito en los países a los que sus diseñadores apuntan, pero tuvieron una inmensa acogida en otros lugares. Tal es el caso de Orkut, la red social de Google que fracasó en Estados Unidos, pero que se volvió un fenómeno social en Brasil y en India. MySpace logró incluir millones de miembros fuera de Estados Unidos y luego terminó centrándose en músicos y fanáticos de bandas musicales, aun cuando sí emplea perfiles de usuarios, es importante anotar que no resulta obligatorio que los perfiles sean “verdaderos”.

A diferencia de los primeros lugares virtuales de interacción que configuró la World Wide Web como los chats públicos o los MUD que privilegiaban el anonimato y la posibilidad de crear múltiples identidades y juegos de rol, en las redes sociales, desde 1997, se estabilizaron como centro los perfiles personales. Entre las grandes excepciones a este modelo está Second Life, que funcionaba a través de la creación de avatares y de identidades ficticias. Las redes sociales virtuales dejan de ser un fenómeno local y empiezan a convertirse en una manifestación global de masas. Así, Facebook se inserta en esta dinámica al crecer de forma llamativa a escala mundial desde el año 2009 (mapas 1, 2, 3 y 4).

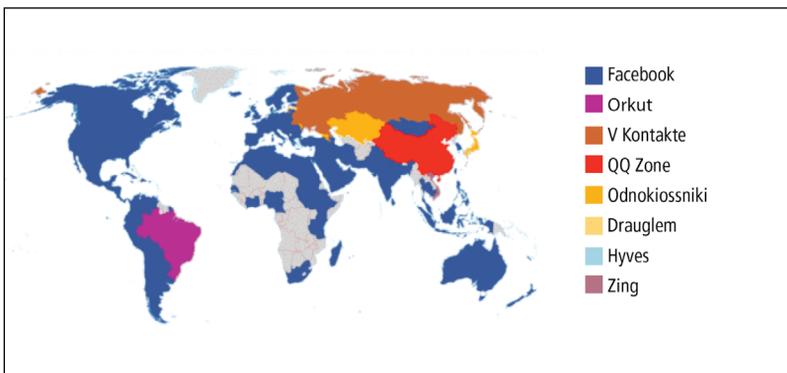
Mapa 1. Posición de las redes sociales en el mundo a junio de 2009



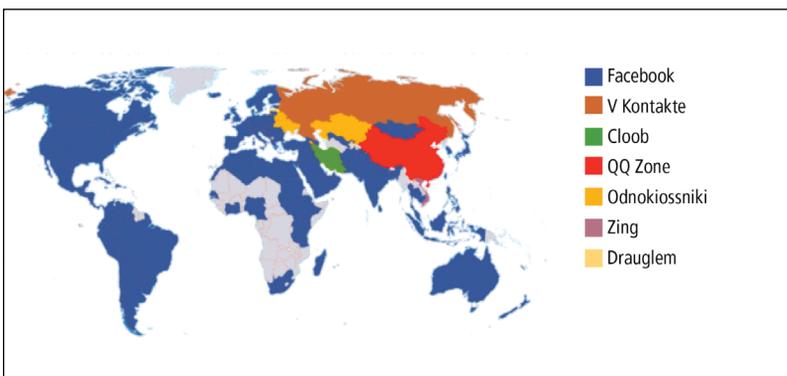
Mapa 2. Posición de las redes sociales en el mundo a junio de 2010



Mapa 3. Posición de las redes sociales en el mundo a junio de 2011



Mapa 4. Posición de las redes sociales en el mundo a junio de 2012



El nuevo fenómeno de las redes

El crecimiento global de las redes sociales puso en entredicho el control de la información personal al convocar a usuarios, activistas y gobiernos (Acquisti y Gross 2006). En ello encontramos por lo menos tres tipos de prácticas que plantean problemas de privacidad: subir contenidos sobre sí mismos, subir contenidos sobre otros y la capacidad de monitorear y seguir a terceros.

Los usuarios de las redes sociales imaginaron su espacio en la red como un lugar destinado para unos pocos, no abierto a cualquiera; con ello la capacidad de expresar sus gustos, sus sentimientos y sus opiniones se potenciaba. Sin embargo, tal libertad chocó con sorpresas importantes: expresar una opinión en una red social podía implicar perder el empleo, algunas personas fueron despedidas de sus trabajos debido a comentarios realizados en sus perfiles sobre sus lugares o compañeros de trabajo.

Subir información sobre terceros es otro aspecto de la privacidad a debate. La idea de control de la información con que Facebook, por ejemplo, promocionó su red, resulta particularmente interesante. Mark Zuckerberg, su fundador, sostuvo que la privacidad ha sido considerada de forma muy importante dentro del diseño del sitio intentando que los usuarios puedan controlar quién ve qué de su información. La estrategia de Facebook fue descrita por Zuckerberg como dar a las personas la capacidad de controlarlo todo.¹² Sin embargo, encontramos por lo menos dos prácticas donde dicha premisa no se cumplió: colocar un *tag* (o nombre de la persona) dentro de una foto sin el consentimiento del otro, o escribir sobre incidentes que conciernen a terceros.¹³ La práctica de *tagging* crea un hipertexto entre el *tag* y el perfil de la persona cuyo nombre aparece en la foto, es decir, cualquiera puede entrar al perfil de un tercero (aunque sea en su versión limitada), sin que este haya dado su consentimiento.

Otra aplicación creada por Facebook que contradice el principio de control por parte del usuario es el News Feed; con ella aparece

¹² “Yo creo que donde sobresalimos es cuando le dimos a las personas el control sobre todo” (Cassidy 2006, 59).

¹³ Warren y Brandeis ya señalaban que la tecnología permite la exposición de aspectos de la vida privada que antes se consideraban de dominio íntimo.

automáticamente un despliegue de todo lo que los “amigos” de mi red han realizado diariamente. La aparición de News Feed creó una ola de reacciones en contra, de parte de los propios usuarios, para sorpresa de los fundadores de la red, quienes no entendían el porqué de la molestia sobre esta nueva forma de presentación de la información que ellos mismos habían ofrecido a sus amigos de la red (Schmidt 2006). Lo que los usuarios reclamaron fue el nivel de “publicidad” que estaba detrás de News Feed, es decir, el incremento del grado de exposición de todo lo que se hace en línea.

Fuera del entorno virtual de la propia red, lo que ha cambiado en estos últimos años es la agregación de la información de las redes sociales a los *dossiers* digitales. Dentro de las búsquedas de Google ahora es posible encontrar el perfil de todo aquel que tenga una cuenta en una red social global. Con ello se ha dado paso a la cosecha de información que brindan las propias personas en sus redes sociales, y de triangularla con la que ofrecen otras bases de datos. Así, las prácticas de generación de perfiles quedan configuradas como mercadería altamente solicitada.

Vivir en un panóptico informativo implica cuatro tipos de riesgos: intrínsecos y extrínsecos de perder la libertad, simbólicos y de metamorfosis psicopolítica (Reiman 1984). Los riesgos intrínsecos resultan de la censura interior que se ejerce una vez que la persona se siente observada y grabada. Los riesgos extrínsecos ocurren cuando las personas dejan de exhibir comportamientos que puedan resultar de algún modo impopulares o poco convencionales, por miedo a perder su trabajo, hacer el ridículo o a que se le nieguen ciertos beneficios; la privacidad opera contra estos dos riesgos como un modo de proteger la libertad y como salvaguarda de una vida interior crítica. El riesgo simbólico de las estructuras institucionales es negar al individuo la capacidad de soberanía sobre sí mismo, es decir, que la privacidad, una capacidad de retiro del escrutinio público, permita una expresión individual de soberanía. Y, finalmente, la metamorfosis psicopolítica ocurre cuando las personas están bajo constante vigilancia: pierden no solo la libertad de actuar como quieran, sino de pensar fuera de la norma, optando por lo convencional, “un centro feliz” en sus opciones y en su pensamiento.

Los efectos disciplinarios del panóptico hacen que el sujeto se mire a través de los ojos de quien lo observa e interiorice los principios del

otro; llevan, además, a la disminución de la capacidad de desear y planificar de una manera propia. La privacidad es un aspecto importante del entorno en donde puede formularse la autonomía personal, su ausencia puede disminuir peligrosamente dicha posibilidad (Reiman 1984, 175-78). El filósofo Ferdinand Schoeman acota “que la privacidad se ve como un reclamo o derecho a determinar cuál información sobre uno mismo está disponible para otros [...] erróneamente se presume que la privacidad es algo que debe ser protegido a discreción del individuo a quien le pertenece la información” (citado por Solove 2008, 25).

Por otra parte, la información como producto tangible tropieza con dificultades: la información personal, con mucha frecuencia, se construye en relación con otros, y las leyes de propiedad intelectual protegen expresiones tangibles y no ideas en sí mismas. La propia concepción de “control sobre la información” concentrada en la facultad de decisión del individuo ha sido refutada por Schwartz (1999); asimismo, se ha discutido erróneamente que la persona tiene autonomía para ejercer control sobre su información personal en todas las situaciones, pero el problema es que “esa misma autonomía es en sí misma moldeada por el procesamiento de los datos personales”. En otras palabras, los individuos no pueden tomar decisiones importantes sobre su propia información porque existen disparidades en el conocimiento y poder para negociar la transferencia de dicha información: la regulación social de la información (Schwartz 1999). “La privacidad es un aspecto de la estructura social, una arquitectura de la regulación de la información, no solo un asunto de ejercicio individual del control” (Solove 2008, 29).

Sin embargo, existen amenazas a la privacidad que poco se relacionan con la noción de lo íntimo, por ejemplo, la transmisión de información entre bases de datos. El intercambio de información es una amenaza a la privacidad del sujeto, pero no afecta de forma primordial sus relaciones de amistad, confianza y amor. Estas amenazas vienen más bien de organizaciones privadas y gubernamentales como los bancos, la policía, los empleadores (Regan 1995). El paradigma del control de la privacidad se convierte en la “trampa de la autonomía”, porque la organización de la información privada, a través del control individual de los datos personales, se basa en la premisa de autonomía del sujeto, su cualidad preexistente. Ello no se cumple en la Era de la información,

donde el control de la información privada se construye de la mano de los procesos a los que está sujeta la información (Solove, Rotenberg y Schwartz 2006). El problema de la libertad de opción es algo que no se toma en cuenta en la versión liberal ideal¹⁴ de autonomía individual, porque es negligente con las verdaderas condiciones de opción que tienen los individuos en el manejo de sus datos personales.

El desarrollo de las tecnologías de la información y la comunicación puso en escena una nueva faceta de la privacidad: la vida privada informacional. Esta noción de vida privada está ligada a una suerte de derecho a la propiedad intangible que se ejerce sobre los datos personales de los individuos y que ha dado paso al *derecho a la protección de los datos personales* en el ámbito constitucional. Estos datos son, entonces, considerados una condición indispensable para la libre construcción de la personalidad, y se debe garantizar que la información personal no sea obtenida o utilizada de una manera que escape a su control.

Según las tradiciones americanas y europeas de la privacidad, son dos las nociones que compiten por definir la privacidad en línea: una centrada en el control sobre la información personal y otra basada en la dignidad. La primera ha prevalecido hasta ahora como la noción dominante de la privacidad utilizando regulaciones, tecnologías, legislación y políticas corporativas. Las redes sociales han enfatizado el concepto de privacidad derivado del control del usuario sobre su información. Aunque muchos usuarios entregan voluntariamente información personal y parecen no preocuparse por la privacidad mientras lo hacen, reaccionan indignados cuando esta información se vuelve pública y es utilizada fuera de la red social a la que pertenecen. Levin y Sánchez (2009) proponen el concepto de *privacidad de red (network privacy)* para resolver esta dicotomía entre la privacidad basada en el control o en la dignidad. De acuerdo con este concepto, en la privacidad de red la información es considerada privada por los usuarios de la red mientras no se vuelve pública fuera de ella, esto en el caso de que la información haya sido generada por el usuario. No es así cuando la información es producida por otros, mientras no afecte su *personae* digital.

¹⁴ Los individuos son capaces de interactuar libre y en igualdad de condiciones mientras el gobierno o el público no interfieran.

Aunque los miembros de las redes sociales tienden a publicar mucha información personal (fotos, relaciones personales, posiciones políticas), mantienen expectativas de privacidad y la sienten violentada cuando audiencias inesperadas descubren su información en línea. Dentro de esta contradicción entre publicación voluntaria de información íntima y deseo de privacidad, ¿podemos hablar de expectativas razonables de privacidad? En la teoría jurídica hasta ahora se ha privilegiado la privacidad como el control de las personas sobre quién tiene acceso a su información personal. Mientras más controles sobre la información se les otorgan a los usuarios, mayor es el nivel de privacidad que alcanzan. Las redes sociales como Facebook también fundamentan la privacidad en la noción de control. Su credo, por ejemplo, reza: “deberías tener el control sobre tu información y deberías poder acceder a la información que los otros quieren compartir” (Levin y Sánchez 2009, 1005-6).

No obstante, socializar en línea presenta un reto fundamental a la teoría del control. La información personal es aquella que identifica un individuo o la relacionada con una persona que no desea que esta sea difundida abiertamente en un momento determinado. La jurisprudencia norteamericana ha basado la noción de privacidad sobre el control de la información personal y la autonomía para decidir con quién compartirla, mientras la jurisprudencia europea ha adoptado el concepto de dignidad o el derecho fundamental a la vida privada como valores legales sustantivos (Levin y Sánchez 2009, 1008). La versión de la privacidad como control está vinculada a las *prácticas justas de la información* (Fair Information Practices-FIP). El objetivo de esta institución es asegurar que las personas mantengan el control sobre su información personal cuando esta se encuentra en manos de una organización. La FIP provee información a las personas sobre cómo las organizaciones manejan (recolectan, usan, difunden y retienen) la información que se les ha encargado, para que puedan tomar decisiones sobre entregarles o no su información personal. En general, las cortes norteamericanas presumen que la información deja de ser privada cuando su dueño, voluntariamente, la volvió pública o cuando se utiliza información a la que se tiene acceso público. La ley no protege la privacidad en espacios públicos, incluso cuando la información es de carácter sensible.

La doctrina que sustenta la privacidad sobre la dignidad sostiene el principio de la personalidad inviolable. Para Bloustein (1964), la privacidad se sostiene en el respeto a la dignidad individual, la integridad y la independencia; la moral personal define la esencia de los seres humanos. Cuando la privacidad de una persona es violada queda expuesta al escrutinio público en una desnudez no autorizada, lo que vulnera su sentido del ser de modo tal que se convierte en una afrenta fundamental a su dignidad (Bloustein 1964). El enfoque de la privacidad como dignidad también enfatiza el desarrollo de la personalidad y del ser interior (Goffman 1981), pues cuando un individuo puede mantener ciertos aspectos de su vida fuera del alcance de los otros es capaz de construir “personalidades situadas”, que funcionan como personas públicas distintas, compuestas de elementos particulares capaces de actuar en diferentes contextos. En su teoría de la presentación del ser, Goffman sostiene que cada personalidad muestra los aspectos que los sujetos consideran apropiados para cada contexto en el que se encuentran.¹⁵ En Europa, la privacidad está protegida por la Convención de los Derechos del Hombre y por varias constituciones nacionales, como un derecho a la dignidad humana, autodeterminación informacional, el desarrollo libre de la personalidad y de la vida privada. La base teórica del derecho a la privacidad en Europa es la dignidad,¹⁶ por ello incluso protege la privacidad de las figuras públicas; difiere del sistema norteamericano que favorece el modelo de control y autonomía.

Las novedades de cambiar las previas prácticas sociales por las virtuales tienen que ver con la exposición de las personas en espacios públicos, la indistinción entre amigos y conocidos, así como con los réditos económicos que la socialización representa para las empresas. El riesgo que tienen los más jóvenes de lastimar su reputación con la información que voluntariamente publican en línea es sumamente alto y solo cobra valor

¹⁵ La representación del ser utiliza la metáfora del teatro para explicar cómo las personas utilizan máscaras concretas para públicos específicos. Las relaciones con los otros usualmente están marcadas por patrones de conducta vinculados con diferentes tipos de asociaciones que ayudan a mantener sistemas diferenciados de relaciones.

¹⁶ Las cortes europeas reconocen el derecho a la privacidad de las personas públicas y han sentenciado consistentemente en contra de la prensa cuando los reporteros han violado la privacidad de políticos, o estrellas del cine o la música (Levin y Sánchez 2009).

cuando buscan trabajo o entran en el mercado laboral.¹⁷ Una segunda cualidad de la vida en línea es la naturaleza de las relaciones interpersonales y el extenso sistema de conexiones que contiene, donde la noción de la amistad ha perdido su nomenclatura tradicional y se ha fortalecido el modelo de lazos débiles y de interconexión de la información. El tercer elemento de la socialización en línea es que tiene lugar en redes sociales que son empresas que hacen negocio con la actividad social de sus usuarios; así, son estas compañías las que ponen las reglas del juego, empezando por los términos del servicio que deben ser aceptados por los nuevos usuarios para ingresar a la red, las políticas que deben ser respetadas por todos los miembros y el diseño del código que regula el estilo de socialización de la red y el comportamiento de los individuos.

En la investigación que realizaron Levin y Sánchez (2009) sobre redes sociales y las expectativas de privacidad de sus miembros, se preguntaban si son razonables las expectativas de privacidad cuando los usuarios suben voluntariamente información sobre sí mismos en plataformas públicas. A continuación, muestro los puntos más relevantes del estudio para introducir la voz de los usuarios en el análisis de la privacidad en las redes sociales en ese momento.

Información que se publicaba en los perfiles personales

El 50 % publicaba nombre completo, ciudad, colegio, estado de relación, intereses, pasatiempos, música favorita, películas, libros y foto del perfil. Lo que más se publicaba: foto, 77 %; ciudad, 76 %; colegio, 72 %; nombre completo, 68 %. Solo un 3 % usa un nombre falso o de broma y un 14 % sube fotos falsas o de broma. Lo que menos se publicaba: dirección completa, 6 %; horario de clases, 8 %; número de teléfono, 16 %. Esta información muestra que la juventud distinguía entre datos personales, útiles para socializar con otros, y datos que pueden ser peligrosos en las manos equivocadas.

¹⁷ De los usuarios de redes sociales, solo el 10 % era mayor de 55 años y cerca de un 50 % registraba menos de 35 años.

Percepción sobre la información publicada

Los usuarios compartían información que esperaban quede en el contexto de la red de amigos. Un 90 % no se preocupaba de que sus amigos ingresen a sus perfiles, pero un 24 % no deseaba que sus padres lo hagan y un 35 % se preocupaba mucho de que sus empleadores accedan a sus perfiles. Lo que más les intranquilizaba es que un extraño ingresara a sus perfiles (43 %). Ello significaba que la información subida por los estudiantes estaba dirigida a sus amigos en el contexto de la red social. Un 67 % declaró preocuparle más que la familia viera sus fotos que sus conocidos, y un 64 % consideraba incorrecto que las personas tengan acceso a información que no estaba dirigida hacia ellas.

La juventud no responsabilizaba a las redes sociales por las fugas de información personal

Un promedio de 69 % exoneraba a las redes sociales de cualquier daño causado por las fugas de información y un 18 % culpaba a los desarrolladores del sitio. Consideraban que las redes tienen el rol de entregarles mecanismos para proteger la información que, sobre los sujetos, se publica (*posts*) y que son los sujetos los que deben utilizarlos para protegerse de ser etiquetados con información que pueda ser embarazosa.

La privacidad, una práctica para ejercer control sobre la información

Un 72 % había configurado su cuenta a través de las herramientas de control de la privacidad, un 54 % había bloqueado a personas para que no accedieran a su perfil, y un 61% creía haber tomado acciones para proteger el acceso a su perfil. El usuario de una red social, que interactúa basado en la confianza de que la tecnología bloqueará el acceso a su información de audiencias no deseadas, se siente traicionado cuando no funciona como esperaba. Un 42 % informó haber leído las políticas de privacidad de su red social y un 45 % indicó haberlas entendido. La diferencia de un 3 % que entendió las políticas sin haberlas leído puede entenderse porque alguien se las explicó previamente o se informaron sobre ellas en otro espacio como un blog, una clase o un artículo. A

pesar de que casi la mitad de la juventud no había leído ni entendido las políticas de privacidad casi un 70 % había utilizado los controles de privacidad para configurar sus cuentas. Esto tiene que ver con la cultura tecnológica de los jóvenes: consideran que necesitan leer los manuales para entender cómo funciona la tecnología.

Los jóvenes entendían que no tienen el control sobre lo que los otros publican sobre ellos

Un 34 % no estaba seguro de saber controlar la información que otros publicaban sobre ellos y un 30 % no sabía si debería preocuparse por la información que sobre ellos se originaba en otros. Más de un 46 % se preocupó por este tipo de información y un 45% dijo sentirse indefenso al momento de defender su personaje en línea en un escenario específico. Aunque un 38 % señaló que sabía cómo protegerse de la información que publicaban otros, un 29 % dijo no saber cómo controlar dicha información. Un 43 % consideró que su información podía ser conocida por extraños y a un 41 % le preocupó su seguridad emocional cuando extraños podrían acceder a su perfil. El alto número de jóvenes que no se sentían seguros con los riesgos de información publicada por otros y su incapacidad de controlarla muestra la dificultad de sostener un sistema de protección de la privacidad basado en el control, que desecha el valor de la dignidad como un componente fundamental de la privacidad. Un sistema como ese difícilmente es eficaz.

Preocupación por el daño a su reputación

El 67 % de personas encuestadas mostró preocupación por la existencia de un acceso no autorizado a su información, lo que responde a la doctrina del control; un 32 % se inquietó ante los efectos del acceso a su información personal y de sus relaciones, lo que responde a la doctrina de la dignidad.

Todas estas categorías muestran algún aspecto de la dignidad, donde la información es usada de modo inesperado, incluso en los casos en que se haya utilizado solo hasta cierto punto. Las fugas de información crean daños reales: los jóvenes percibían que su privacidad era *algo más*

que lo que ellos publicaban y no se limitaba solo a la habilidad de controlar la información subida. La privacidad también tiene que ver con los efectos de la información publicada por otros, una información que no puede ser controlada con las herramientas que las redes sociales les ofrecen. Ello evidencia que la privacidad en línea puede ser afectada incluso cuando los usuarios son capaces de controlar perfectamente la información personal que publican.

Otra percepción entre los jóvenes en aquel entonces era que los empleadores no deberían solicitar a sus empleados ser amigos dentro de una red social; a pesar de que es una práctica muy común, un 66 % de los jóvenes no estaban de acuerdo con ella. Así surge una nueva versión de la privacidad, la privacidad en red. Esta es

[...] una noción de la privacidad basada en el acceso esperado a la información personal de grupos sociales. Estas expectativas se basan en la necesidad de mantener identidades sociales discretas, o personalidades situacionales. Cuando un usuario en línea percibe una amenaza a la privacidad, en realidad es su reputación, su dignidad, su persona o su identidad en línea lo que está en riesgo (Levin y Sánchez 2009, 1045).

Entonces, la privacidad se relaciona con la representación del ser (Goffman 1981), pues a los usuarios les preocupa el daño a su reputación y dignidad dentro de las redes sociales. Así, la falta de control sobre la información personal no ha disminuido la participación en las redes, los jóvenes siguen deseosos de socializar en ellas, no les inquieta el hecho de saber cómo controlar su información y están dispuestos a que su privacidad sea invadida. Son muy pocos los que confían poder controlar la información que sobre ellos se produce dentro de la red y muchos se declaran impotentes para proteger su perfil en línea. No solo les interesa cuántas personas conocen su información sino quién la conoce. Esta forma de ver la privacidad complementa las explicaciones de la privacidad fuera de la pantalla, las cuales enfatizan las expectativas individuales del alcance de la difusión de la información privada y no en las expectativas individuales de que su información personal no sea diseminada en ningún caso. La privacidad en red

puede ser un producto de los nuevos medios sociales y de las normas sociales tradicionales. Los usuarios parecen estar trasladando sus

expectativas de privacidad fuera de la pantalla a sus experiencias sociales en línea. Los individuos que no están en línea pertenecen a muchas redes sociales y presentan distintas *personae* en diferentes contextos [...] en un sentido, la información que comparten en una red social no es privada, pues es conocida por los miembros de la red. Pero se mantiene un sentido importante, que está confinado a la red por medio de un entendimiento implícito de confidencialidad y confianza. Las normas fuera de la pantalla dictan que la información personal no debe revelarse por fuera de la red en la que fue originalmente compartida (Levin y Sánchez 2009, 1046).

La privacidad en red combina la noción de control y la de dignidad, haciendo hincapié en la última, porque apela a las normas que las redes sociales promueven. Desplazar el énfasis de la estructura de interacción social en la recolección de datos personales que hacen las organizaciones dentro de la red es anular cualquier posibilidad de proteger la privacidad como un elemento fundamental para la dignidad.

SECCIÓN 2
FACEBOOK

Capítulo 4

El artefacto sociotécnico

En este capítulo caracterizo la agencia del artefacto Facebook en la construcción de un espacio público estandarizado, a partir de la influencia de las capas informáticas sobre las capas culturales. Para estudiar el fenómeno de la privacidad dentro de Facebook he tomado, como punto de partida, el enfoque de la Construcción Social de la Tecnología (SCOT, por sus siglas en inglés) de los estudios de ciencia, tecnología y sociedad, pues permite explicar cómo se configuran los artefactos tecnológicos en su interacción con los sujetos. Dicho enfoque es particularmente útil ya que al alejarse de la versión determinista propone el desarrollo autónomo de los objetos, nos centra en el estudio de las relaciones de ida y vuelta entre sujetos y objetos; ello muestra cómo se producen las normas sociales con respecto a la privacidad y el valor del código dentro de los espacios virtuales tecnológicamente configurados. Así, las “trayectorias sociotécnicas” (Thomas 2008) de Facebook son el producto de la co-construcción de objetos, prácticas y actores heterogéneos.

La construcción social de la tecnología también invita a trabajar el objeto de esta obra de forma situada. Con el estudio de caso de las nociones de privacidad en la red social Facebook, descubro cómo el espacio público virtual logra estandarizarse a través del código y se vuelve controversial en las relaciones que produce con los usuarios de la red. Es esta historia de co-construcción la que pretendo explicar en las siguientes páginas.

La SCOT, desarrollada por Pinch y Bijker (2008) entre otros, ofrece un marco teórico metodológico que enfatiza lo local y los grupos sociales relevantes que intervienen en el proceso de construcción del artefacto. Dentro de un análisis diacrónico he comparado los cambios

que fue adquiriendo el artefacto sociotécnico Facebook en sus inicios, la fuerza de sus regulaciones y el ensamblaje, no siempre armonioso, entre empresas, publicidad, gobierno, usuarios y artefacto.

Uno de los principales presupuestos de la SCOT es considerar a la sociedad como un tejido sin costuras (Bijker 1995) donde lo tecnológico no puede ser distinguido de lo social de forma apriorística. La metáfora del tejido sin costuras es la base del planteamiento constructivista social de la tecnología que he utilizado para (de)construir la relación entre lo social y lo tecnológico. Puesto que la sociedad moderna no está compuesta por piezas solo sociales, tecnológicas o económicas, no es posible distinguir *a priori* entre lo económico, lo social o lo científico.

Un segundo aporte es reconocer que los artefactos sociotécnicos pueden ser significados de forma distinta por los grupos sociales. La SCOT toma prestado el concepto de grupo social relevante de la sociología del conocimiento científico y lo utiliza como una categoría de los actores (Thomas 2008). Primero Collins lo usa en su análisis relativista, y luego Bijker (1995, 48) como una categoría de análisis.

el mundo tal como existe para esos grupos relevantes es un buen lugar para que el analista inicie su investigación [...] la racionalidad básica de esta estrategia es que solo cuando un grupo social es explicitado en algún lugar del mapa se genera un sentido que lleva al analista a tomar el hecho en consideración.

Puesto que cada grupo social relevante tiene su propio contexto, puede interpretar el mundo de manera diferenciada y otorgarle, así, significados diversos a un mismo artefacto. Una actividad clave del análisis constructivista es precisamente de-construir esos significados y rastrear las distintas perspectivas ubicadas detrás de la construcción social de los artefactos, identificar los sentidos que se les ha otorgado y descubrir de qué están hechos. Los grupos sociales relevantes “constituyen a los artefactos”, pues permiten centrar nuestra atención en ellos. “A partir de esta multiplicidad de visiones, socialmente situadas, aparecen tantos artefactos como visiones de los artefactos mismos” (Thomas 2008, 233-34).

La flexibilidad interpretativa hace referencia, entonces, a los significados que le son adscritos al artefacto, o al hecho de que distintos artefactos puedan servir al mismo problema. Mientras los grupos sociales

construyen significados del artefacto que no logran consensuar, la flexibilidad interpretativa es alta; pero cuando los significados se acercan entre sí y es posible definir el artefacto de un modo común, entonces se produce lo que Bijker denomina clausura. La estabilización del sentido del artefacto se debe a dos cosas: o los grupos sociales relevantes se convencen de que el artefacto es una solución a un problema, o el problema ha sido redefinido por los grupos sociales relevantes. Con el fin de estudiar la trayectoria de la privacidad dentro de Facebook debo explicar cómo funciona la red social; es decir, describir los procesos gracias a los cuales ha logrado una baja flexibilidad interpretativa que clausura un sentido del artefacto, y ha alcanzado un creciente grado de estabilización como producto de la disminución de dicha flexibilidad (Bijker 1995).

Mientras la noción de artefacto nos concede un primer nivel de investigación, el concepto de marco tecnológico nos introduce en un segundo nivel de análisis, enseñándonos la serie de relaciones que se forman entre los grupos sociales relevantes y los artefactos, a través de los procesos de clausura y estabilización. Con los marcos tecnológicos podemos describir los paradigmas dentro de los que funcionan los grupos sociales y explicar desde qué estrategias, teorías, prácticas, regulaciones, conocimiento tácito o doctrinas construyen el artefacto, o ver la forma en que los grupos permanecen unidos frente a ciertos artefactos abriendo la caja negra de sus interrelaciones. Los marcos tecnológicos nos sacan de la dicotomía sociedad-tecnología a la que remiten los artefactos, descifran los procesos dinámicos en las interacciones individuales dentro de los grupos sociales relevantes, pues no son entidades fijas, y visibilizan las estrategias puestas en marcha para resolver los problemas (Thomas 2008).

Finalmente, los ensambles sociotécnicos son el tercer nivel de agregación del análisis constructivista que empleo en esta obra. Con ellos puedo revisar las relaciones de poder a gran escala e incluir los otros actores tecnológicos y sociales, al igual que sus respectivos grupos sociales relevantes. En este nivel enfatizo lo sociotécnico, las dos caras de la misma moneda de los procesos de construcción de grupos sociales relevantes: artefactos y hechos (Bijker 1993, 128-29). Son tres las posibles configuraciones de los ensambles sociotécnicos que plantea Bijker: a) *no hay un marco dominante*, lo que significa que la flexibilidad interpretativa es alta y las innovaciones pueden ser radicales; b) existe *un grupo*

social dominante que impone su marco sobre los otros, configurando el problema y las soluciones que constituyen al artefacto, en cuyo caso las innovaciones son más bien convencionales y los cambios radicales solo los pueden traer actores con baja inclusión en el marco; y c) *dos o más grupos sociales dominantes* con sus marcos en conflicto confrontarán interpretaciones, lo que clausurará el proceso y la innovación tenderá a fusionar los intereses de ambos grupos (Thomas 2008, 239).

De esta manera, el análisis sociotécnico produce un doble razonamiento: reconstruir el momento en que los artefactos tecnológicos se vuelven parte constitutiva de las relaciones sociales, políticas, económicas y culturales, y el momento en que estas distintas relaciones se materializan en artefactos tecnológicos. No se trata de la relación entre la tecnología y la sociedad

porque las sociedades están tecnológicamente configuradas, exactamente en el mismo momento y nivel en que las tecnologías son socialmente construidas y puestas en uso. Todas las tecnologías son sociales. *Todas las tecnologías son humanas* (por más inhumanas que a veces parezcan).

Por eso no se trata de considerar las tecnologías como *productos* o *procesos productivos*. Solo recientemente hemos percibido que las formas de *organización* también son tecnologías. Desde aquellas que asignan un orden a un conjunto de operaciones, de acciones bélicas, o de sistemas de evacuación de un estadio, hasta aquellas que adquieren formatos normativos, como los sistemas legales o las regulaciones de comercio [...] *La dimensión tecnológica atraviesa la existencia humana* [...] Lo curioso es que, normalmente reflexionamos poco sobre la tecnología. Pasa desapercibida, naturalizada como la lluvia o las olas. Solo se hace visible en dos momentos particulares: cuando deja de funcionar o cuando cambia rápidamente (Thomas 2008, 10).

La sociedad en red: Silicon Valley y los visionarios

La trayectoria sociotécnica de Facebook no inició en el año 2004 en los dormitorios de Harvard; empezó a finales de los años noventa con los emprendimientos en internet que surgieron a fines de esa década en

distintas partes de los Estados Unidos y que terminan configurando la web tal cual la conocemos hoy en día. Utilizo la construcción social de la tecnología para explicar cómo este contexto histórico se volvió parte del propio desarrollo de Facebook y la red de relaciones y apoyos que su fundador establece con otros innovadores. Los conceptos de *grupos sociales relevantes*, *flexibilidad interpretativa* y *marco tecnológico* (Bijker 1995) me permiten mapear los problemas y soluciones en los que este grupo de innovadores trabajó en los inicios de la red y, con ello, introducir la gramática de sentido en la que Mark Zuckerberg se sumerge cuando imaginó Facebook.

¿Qué es lo que estos pioneros tenían en mente? ¿Qué necesidades satisfacían los servicios que inventan? Todos querían “conectar” a las personas en línea; bajo la estructura de red, estas iniciativas ofrecían a los cibernautas la posibilidad de habitar el ciberespacio de forma más regulada. Los fundadores de redes y servicios en línea necesitaban construir un ciberespacio normado para que pudiera ser habitado por sus usuarios. Si la gente iba a participar en espacios virtuales comunes era necesario condicionar su comportamiento para que lo hicieran en función de su diseño.

El código determina quiénes pueden acceder a qué objetos digitales [...]. Cómo este tipo de programación va a regular las interacciones humanas [...] depende de las opciones que tomemos. O en otras palabras, el código del ciberespacio define las libertades y controla el ciberespacio [...] Pero ¿quién va a crear el código y con qué valores? (Lessig 2006, 6).

La arquitectura de internet es muy sencilla. Lo interesante de su diseño es que permite que aniden otras estructuras y se tornen más complejos los espacios virtuales. Estas capas de códigos que se yuxtaponen van configurando las características de los lugares del ciberespacio y construyendo las arquitecturas de control. Hoy en día estos diseños resultan cada vez más comunes y se convierten, a simple vista, en estructuras complejas de regulación de comportamientos. Resulta novedoso, pero fundamental, relacionar el diseño con la regulación. Es el único modo de descubrir cómo funciona el código a través del diseño, y cómo la arquitectura de un sitio web es capaz de normar los comportamientos

de quienes lo habitan. Para Lessig (2006, 34-8), “la regulación es una función del diseño” y, por tanto, la naturaleza de un lugar en el ciberespacio es el producto de su diseño. Por ello, el ciberespacio es el lugar más regulado que la humanidad haya conocido jamás.

El primer grupo social relevante recibirá el nombre de “visionarios”. Este se encarga de organizar la internet social conectando a las personas a través de objetivos específicos: encontrar amigos en línea, conseguir una cita amorosa, pagar en línea, compartir información. Algunos de ellos son fundadores, cofundadores o inversionistas y se encuentran geográficamente distribuidos en California, Nueva York, Boston y Florida. A pesar de que no todos comparten el mismo perfil, un número importante de las personas aquí agrupadas tiene muchos rasgos en común.

En 1997 Sixdegrees.com apareció en Nueva York. Fundada por el abogado Andrew Weinreich, fue la primera red social que utilizó el modelo de “contactos” en línea. Poco tiempo antes de desaparecer, en 2001, patentó el concepto de “red social”, licencia que fue comprada por Reid Hoffman y Mark Pincus.

Luego de trabajar un tiempo en Apple Computer, Hoffman inició su propia compañía: SocialNet.com, un servicio especializado de citas. Asimismo, trabajó en Paypal, servicio de pago en línea; cofundó e invirtió en LinkedIn, la red de contactos para profesionales, y fue su gerente general. Invirtió en Friendster, fue uno de los primeros inversionistas de Facebook, además, dueño de acciones y miembro del directorio de Zynga.

Mark Pincus fue fundador de Tribe.Net y de Freeloder.Inc., al igual que inversionista de Friendster y Facebook. Fundó Zynga en 2007 y es uno de los desarrolladores de aplicaciones más importantes dentro del ecosistema de Facebook, con productos estrella como Farmville o Mafia Wars. Friendster, la primera red social con éxito en los Estados Unidos, logró conectar a usuarios de todas partes del país y tuvo como miembros a otros fundadores, cofundadores e inversionistas de otras redes (Zuckerberg de Facebook y Tom Anderson de MySpace). Su fundador Jonathan Abrams era muy amigo de Sean Parker, uno de los fundadores de Plaxo.

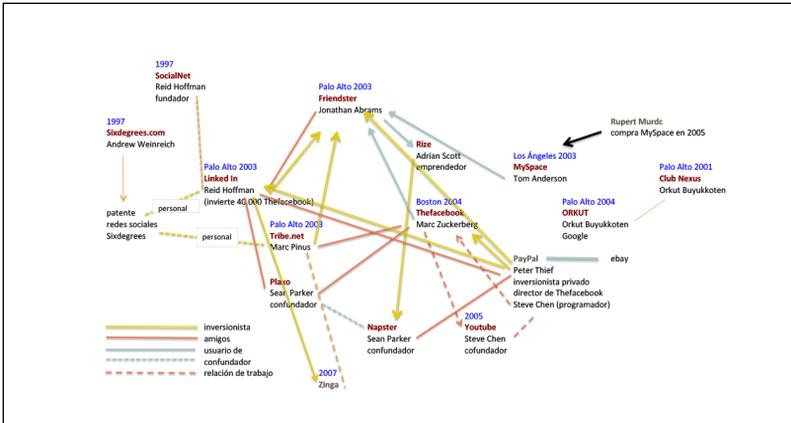
A propósito Sean Parker, cofundador de Napster y Plaxo, ayudó a Zuckerberg en su primera ronda de inversiones con Thefacebook: trajo al primer accionista externo de la compañía, Peter Thiel. Parker fue el primero en entender el potencial de Facebook y asesoró a Zuckerberg

desde su inicio en Palo Alto. Se unió a la compañía como presidente fundador y a su salida siguió relacionado con Facebook como accionista y amigo personal de Zuckerberg. Inversionista y miembro del directorio de Spotify, un servicio de música en línea sueco, logró firmar una alianza con Facebook para que los usuarios de la red social compartieran sus listas de música con sus amigos mediante esta aplicación. Peter Thief, también fue cofundador de Paypal y accionista de Facebook, ha invertido en emprendimientos como LinkedIn, Friendster, Booktrack, Slide, Yammer. Ha sido parte del directorio de Facebook desde su inicio como compañía en California.

En los años iniciales de Thefacebook, varias compañías ya estaban funcionando en línea: Paypal, LinkedIn, Friendster, TribeNet, Napster, Plaxo, MySpace y Orkut, entre las más importantes. Poco más tarde aparecieron YouTube, Zynga y otras. De estas diez compañías, he rastreado relaciones entre ocho de ellas que resultaron fundamentales para Facebook, bien en cuanto a inversión, bien respecto al asesoramiento y las alianzas estratégicas. Así, la interacción entre los visionarios se da en dos niveles: las relaciones personales de sus cofundadores e inversionistas y los problemas comunes a resolver.

Las relaciones establecidas entre ellos (gráfico 2) también estaban mediadas por los lugares donde se formaron y donde el emprendimiento de los negocios en línea era más consistente. Palo Alto es el lugar donde surgió SocialNet, Friendster, TribeNet, Club Nexus, LinkedIn, Orkut, Paypal, Facebook (en Palo Alto pasa de Thefacebook que se origina en Boston al nombre y ubicación de origen de la compañía). Varios se conocen desde su etapa universitaria en Stanford, Harvard y Berkeley. Otros se mantienen activos entre compañías, como es el caso de Thief, quien además de ser inversionista en cuatro de ellas, también es parte del directorio de Facebook. La capacidad de los visionarios de involucrarse en varios emprendimientos también es muy alta. Parker ha sido parte fundamental de tres muy importantes: Plaxo, Napster y Facebook. Pinchus ha hecho lo propio con Tribe.Net, Zynga y Facebook. Estos visionarios han comprendido que dominar dentro del ciberespacio depende del código informático y de organizar las preferencias de los usuarios, que la web es temática y requiere de mecanismos que potencien la socialización entre personas según sus intereses.

Gráfico 2. Mapa de relaciones personales entre redes vinculadas a Facebook



Imaginando Facebook. El valor del código

Los espacios virtuales del ciberespacio se regulan principalmente a través del código. Entonces, las reglas de comportamiento se imponen en gran medida gracias a estas regulaciones y, otro tanto, por medio de la sanción social, mas no por el Estado. “Una regla se define no por su estatuto, sino por el código que gobierna dicho espacio”; como lo indica Kapor, “su arquitectura es su política” (citado por Lessig 2006, 24). Del mismo modo la conducta individual en el ciberespacio se regula por medio del código; en unos casos, los espacios virtuales son más libres (navegación, redes sociales, por ejemplo), en otros casos son más controlados (acceso a banca en línea, bases de datos pagadas, entre otros). La naturaleza del código se refleja en su arquitectura.

El primer Facebook, llamado Thefacebook, tomó ideas de otras redes sociales que ya estaban en el mercado. De Sixdegrees.com copió el envío de invitaciones vía correo electrónico para ingresar a la red. De Plaxo, el concepto viral de identificar información de las personas a través de sus contactos. De Friendster, los perfiles con fotos. De Club Nexus (2001), la idea de una red cerrada de estudiantes universitarios que incluía chat, invitaciones a eventos, columnas tipo blog y un motor de búsqueda que permitía encontrar a personas con intereses similares (ilustración 1).

Ilustración 1. Thefacebook, 2005



Fuente: <https://bit.ly/2Rxhaq7>

El código diseña lo que contiene el sitio, organiza el espacio virtual de modo que pueda ser habitado por sus usuarios. Thefacebook no tenía contenido propio, pero perfiló un “modo” de representar que fue vital para la forma en que se construyó la red: los lugares, en principio, fueron alimentados por los miembros de la red social y funcionaron como cadena de referencias mutuas a través de las cuales se armó el tejido. La falta de información fue una invitación para que sus miembros la llenaran con datos, mas, ello no debía implicar demasiado trabajo para no abrumarlos. Thefacebook pedía, como condición para ingresar, crear un perfil con una foto y con información personal (gráfico 3).

A diferencia de otras iniciativas, Thefacebook no añadía aplicaciones sino las quitaba, para que los usuarios se concentraran y crecieran dentro de las ya existentes. El diseño del sitio era extremadamente minimalista y fue evolucionando según el tipo de aplicaciones que más utilizaban los usuarios, rastreando a los que más amigos tenían. En su despegue, Thefacebook permitía actualizar el perfil de usuario, añadir amigos, *poke* y ver los perfiles de los otros. El desarrollo del código de Thefacebook fue un claro ejercicio de co-construcción entre la función del diseño del espacio virtual y los usos sociales de la arquitectura. Este proceso sociotécnico se estableció dentro de la tensión entre la capa social y la tecnológica, una suerte de condicionamiento recíproco a través

Gráfico 3. Características de Thefacebook



de negociaciones entre actores y artefactos (Thomas 2008; Oudshoorn y Pinch 2005; Vercelli y Thomas 2007). El código se vuelve así más social y las acciones de sus miembros se tornan tecnológicamente más estructuradas.

Desde un inicio, los controles de privacidad fueron clave para el funcionamiento de Thefacebook, pues una vez que se ingresaban a la red todos los miembros podían acceder al perfil del nuevo miembro. Por tanto, se establecieron dos condiciones que ayudaban a mantener la privacidad: usar el nombre verdadero y tener una dirección de correo electrónico de Harvard.edu. El código filtraba automáticamente, funcionaba como barrera para gente que estaba fuera de la universidad. En principio, mantener un círculo exclusivo de miembros permitió autenticar los perfiles, ya que no era posible suplantarlos.

El equipo de escritores de código se volvió cada vez más eficiente y aprendió mientras el proyecto se expandía. El crecimiento explosivo de Thefacebook tuvo que ver con una combinación poco usual del desarrollo de código para ordenar lo que las personas podían hacer en la red social y los usos que sus miembros hacían del espacio virtual. Chirs Ma, un inversionista de *Washington Post Company*, describió a Zuckerberg

como un psicólogo, conocedor del profundo deseo de la juventud de tener ciertos tipos de interacciones sociales en la universidad y que su interés más importante son sus amigos: lo que hacen, lo que piensan y dónde lo hacen (Kirkpatrick 2010).

Los programadores eran jóvenes de apenas veinte años que estaban en sintonía con los códigos culturales de sus usuarios y que lograban responder, velozmente, a las tendencias de comportamiento que los miembros de la red producían. Todos eran también estudiantes de universidades de élite norteamericanas y no separaban lo que eran de lo que hacían. Estructuraron, así, una red de relaciones virtuales y, a su vez, construyeron socialmente el artefacto tecnológico.

Los diseñadores de código y Zuckerberg lograron que Thefacebook creciera metódicamente; cuando podían pagar más servidores abrían la red en una nueva universidad, cuando no podían se quedaban por un tiempo con las ya incluidas hasta poder invertir en servidores nuevos. Podían también mantener los costos bajos porque utilizaban *software* libre MySQL y lenguaje de programación PHP. Si el proyecto hubiese empezado unos años antes, no habría tenido éxito porque el *software* libre no se había consolidado todavía y no se hubiese podido utilizar en una red social como esta.¹ Al año de haber empezado abrían Thefacebook en una nueva universidad solo si el 20 % de los estudiantes había solicitado ser miembro. Así los jóvenes estaban en lista de espera hasta que en la universidad se abría la red social. Ello garantizaba que una vez que Thefacebook se iniciaba, el ingreso del resto de estudiantes era muy rápido y masivo. La técnica no solo se utilizaba en la escritura de código, también era fundamental en el modelo de negocios que se estaba construyendo.

La primera aplicación de Thefacebook fue *poke*,² Zuckerberg la definió como “algo divertido que no tenía un propósito específico”. Las aplicaciones que se añadieron a los pocos meses fueron el muro, los

¹ Tal fue el caso de Sixdegrees.com, que fracasó por “haber llegado demasiado pronto”, pues el servicio era muy caro de mantener y operar. Contratava más de 90 empleados, pagaba mucho dinero por el desarrollo de aplicaciones, servidores y por licencias a Oracle. Sin contar con una conexión muy lenta que volvía el servicio muy pesado. A pesar de sus 3 500 000 de usuarios, su fundador Andrew Weinreich (abogado) vio que el servicio no duraría mucho más y patentó las innovaciones de Sixdegrees.com.

² “Dar un toque”, traducido de este modo por los propios usuarios de Facebook.

grupos y los comentarios vinculados al grupo. Con el muro las personas empezaron a escribir en sus propios perfiles, comentar sobre lo que habían visto, enviar mensajes (equivalentes a correos públicos); cualquier amigo podía ver lo que se escribía en el muro, una especie de cartelera personal que desde el inicio tuvo mucho éxito. Zuckerberg, Parker y Moskovitz acuñaron el término “el trance” para caracterizar la forma en que los estudiantes usaban el sitio, pues era algo hipnótico: una vez que se empezaba a hacer clic en un perfil no se podía parar, se iba de un perfil a otro mirando la información. Un efecto de socializar en línea fue volver obsoletas las agendas de teléfonos y de correos electrónicos: si alguien quería contactar a otro simplemente lo buscaba en Thefacebook y le enviaba mensajes. Los grupos eran páginas creadas por los miembros que se ligaban a sus perfiles.

La competencia también estaba diseñando otras aplicaciones. Yahoo había comprado Flickr, un servicio que permitía subir fotos gratuitamente y etiquetarlas; así una foto que tenía las etiquetas “Venecia”, “góndola” o “paisaje” podía ser buscada por cualquiera. Con el paso de Thefacebook a Facebook se volvió a intentar un proyecto de fotos que funcionara sobre la nueva estructura, pero ya no como programa independiente, sino como una aplicación libre. Se añadió algo “típicamente Facebook”, según Dough Hirsch, vicepresidente de la compañía: saber quién está en la foto. Así, surgió la idea de etiquetar las fotos de Flickr con una condición: las etiquetas solo estarían relacionadas con quien aparecía en la fotografía. Se comprimieron los archivos para facilitar la velocidad de despliegue lo cual afectaba la resolución de las imágenes; el problema era si los usuarios aceptarían fotos de baja resolución, y lo hicieron. La popularidad en Facebook se medía por cuántos amigos se tenía y por cuántos *tags* o etiquetas se poseía, se había convertido en la aplicación más popular de internet, pues al mes de ser lanzada, 85 % de los usuarios activos había etiquetado por lo menos una foto; a finales de 2010 albergaba 40 000 millones de fotos, convirtiéndose en el repositorio gráfico de internet más grande del mundo (Kirkpatrick 2010).

La aplicación de fotos de Facebook tenía dos antecedentes que la volvían posible: la fotografía digital y la popularidad de aplicaciones como la de Flickr. También el nuevo código había creado un tipo de circularidad

dentro de la red, cada *tag* era una nueva conexión que se activaba entre un gran grupo de personas, pero también estaba introduciendo serios problemas al consumir servidores y saturar el almacenamiento de datos contratado para los siguientes seis meses. Zuckerberg denominó este nuevo tipo de sociabilidad como Social Graph, el *tag* funcionaba solo porque tenía un sistema que alertaba a alguien si había sido etiquetado, y los *tags* determinaban cómo las fotos eran distribuidas a través del servicio. Al ver el crecimiento del *tagging*, los diseñadores entendieron que el Social Graph podía usarse como un sistema de distribución, pues este mecanismo eran las propias relaciones entre los miembros. “Una internet más social era el sueño de Zuckerberg y esto le permitió empezar a formular una teoría más amplia de lo que Facebook realmente era” (Kirkpatrick 2010, 157).

Desde sus inicios, Facebook sabe quién es cada individuo, puede ubicarlo físicamente, tiene registrados sus “amigos” por categorías, puede armar la red de relaciones familiares, sus intereses, su lugar de trabajo. Puede censurar los contenidos no deseados y borrarlos sin autorización del usuario. El código funciona para regular cada acción que los usuarios realizan dentro de la red, desde el momento en que las personas se registran en este espacio virtual hasta el sitio que ocupan en relación con otros dentro de la red (amigos, conocidos, perfiles limitados). Cada vez que no ha gustado un comportamiento empiezan a cambiarlo rediseñando la arquitectura del sitio. En este sentido, el potencial de control que Facebook tiene sobre sus miembros es extraordinario. Zuckerberg pensaba que las personas podrían “compartir” mucho más si no se les dejaba hacer lo que quisieran y se les imponía cierto “orden” (Kirkpatrick 2010, 100).

Luego de la inclusión de universitarios y estudiantes de colegio, faltaba incorporar a los adultos. Para ello se idearon redes de trabajo a partir del supuesto de que las personas adultas socializan en sus trabajos y que ello aumentaría la ubicuidad de las grandes compañías. En mayo de 2006, estas redes se abrieron pero pasaron desapercibidas, la única que funcionó fue la de la Armada (Marina y Fuerza Aérea) norteamericana. Por lo visto, los militares tendían a desarrollar relaciones similares a las de los estudiantes universitarios. Facebook incorporó nuevas aplicaciones, entre ellas *timesorting*, un código que ordenaba la lista de amigos de cada usuario en relación con quiénes habían cambiado su foto de perfil recientemente.

El resultado fue un promedio de 25 entradas más a los perfiles actualizados. No olvidemos que Zuckerberg sostenía que el éxito de Facebook se podía medir por cuántas personas “regresaban” al sitio. El código tiene la capacidad de transformar las conductas de las personas; así, los programadores descubrieron con cada cambio en el código cómo ello acontecía frente a sus ojos. Para idear códigos nuevos era necesario, primero, entender cómo socializaban los usuarios y, en segundo lugar, desde las conductas ya estabilizadas en el sitio, diseñar nuevas aplicaciones que permitieran lograr que los miembros de Facebook hicieran lo que Zuckerberg quería: que regresaran muchas veces a su red y que construyeran una nueva forma de socialización en línea. De esta manera, Facebook se fue transformando gracias a los mecanismos de co-construcción que se establecieron entre las prácticas de los usuarios y las formas de relacionarse que se aprendían en el sitio, para luego ordenarlas de acuerdo con los intereses de Facebook.

Hasta ese momento, cada usuario debía navegar por los perfiles de sus amigos para saber qué había cambiado. El *timesorting* era un atajo muy efectivo para enterarse de esos cambios sin tener que hacer manualmente la búsqueda de las novedades. El valor del nuevo código fue rápidamente capitalizado para cambiar parte de la propia estructura de Facebook y volver accesible, a otros, todo aquello que los usuarios habían vuelto público en su perfil. Se creó una página para mostrar todas las cosas que los amigos habían cambiado en sus perfiles, según Moskovitz, “queríamos construir una pantalla que lo mostrara todo. Así que concebimos la idea de *News Feed*. El orden en que se mostraría la información dependía del comportamiento de cada usuario, de lo que le gustaba mirar” (Kirkpatrick 2010, 180). Ello implicaba que cada página de perfil tenía que ser distinta; era el reto tecnológico más importante que la compañía había asumido, si tomamos en cuenta que cada usuario tenía un promedio de 100 amigos, el *software* debía revisar la acción que cada uno de ellos producía para decidir a quién enviársela y a quién no, dependiendo de los gustos de cada usuario receptor de información.

Con ello, se lograba que los usuarios se suscribieran a un sistema de información que Facebook referenciaba, algo parecido a lo que hacía el

sistema de información Really Simple Sydication (RSS).³ La novedad era que, a partir de entonces, se aplicaba información sobre los comportamientos de las personas, un verdadero salto del nuevo sistema. El proyecto duró ocho meses en construirse, y participaron programadores con perfiles como el de Chris Cox, psicólogo, lingüista, graduado en Ciencias de la Computación (citado por Kirkpatrick 2010, 181). Su lanzamiento fue a inicios de clase, en el otoño, para aprovechar el ingreso de miles de usuarios nuevos. Los escritores de código denominaron a cada tema que provocaría una alerta, una “historia”; y al *software* que procesaba cuáles historias debían ir a los perfiles de qué usuarios, “el publicador” (Kirkpatrick 2010, 188). News Feed se lanzó el 5 de septiembre de 2006; Ruchi Sanghvim, jefa del proyecto, escribió:

Facebook se ha hecho cirugía plástica. Hemos añadido dos chéveres características, News Feed que aparece en la página principal y Mini Feed que aparece en el perfil de cada persona. News Feed resalta lo que pasa en sus círculos sociales en Facebook, actualiza una lista personalizada de nuevas historias día a día, de modo que puedan saber cuándo Mark añade a Britney Spears a sus favoritos o cuándo están solteros de nuevo... Mini Feed es similar, excepto que se centra alrededor de una persona. Cada persona en Mini Feed muestra qué ha cambiado recientemente en su perfil y qué contenido (notas, fotos, etc.) ha añadido.⁴

Así, los cambios de arquitectura en las aplicaciones no siempre pasan desapercibidos y pueden generar una reacción de los usuarios del sitio. Eso fue lo que sucedió con News Feed. Los usuarios lo odiaron, escribieron cosas como “Ruchi es el Diablo”. Las quejas salieron de la pantalla y alcanzaron los medios de comunicación, la más importante tenía que ver con el acoso. Tanto quienes leían algo sobre otros o quienes sabían que estaban siendo leídos sentían distintas formas de asedio. La objeción a News Feed fue que enviaba a otros demasiada información personal (ilustración 2).

³ Este sistema era muy utilizado por los medios de comunicación y los blogs. Las personas se suscribían a esos sitios web y recibían los productos que allí se producían.

⁴ Información fuera de línea, <http://blog.facebook.com/blog.php=2207967130>

Ilustración 2. Mini Feed, 2006

The image is a screenshot of Mark Zuckerberg's Facebook profile from 2006. The page is titled "Mark Zuckerberg's Profile (This is you)" and "Harvard". The profile picture shows a young Mark Zuckerberg. The "Status" section indicates he is at work, updated on Friday. The "Harvard Friends" section lists 174 friends, with three shown: Carolyn Abram, Melanie Deitch, and Kasey Galang. The "Friends in Other Networks" section lists Harvard (147), Facebook (96), and San Francisco, CA (82). The "Mini-Feed" section displays 10 stories, including Mark commenting on Ezra Callahan's note, Mark editing his profile picture, Mark writing on the wall for the group LOCKDOWN, Will tagging Mark in two photos, and Mark and Julia becoming friends. The "Information" section shows contact info, email, and ATM screenname.

Fuente: <http://bit.ly/1HLP2Eu>.

El código lo que hacía era tratar todos los comportamientos en Facebook de forma idéntica, dentro del mismo flujo de información, quitándoles el contexto dentro del cual habían sido practicados. Zuckerberg contestó, dentro de Facebook, dos días después del lanzamiento:

Tranquilícense. Respiren. Los escuchamos. No somos ajenos a los grupos de Facebook que se han creado (a propósito, Ruchi no es el diablo). Y estamos de acuerdo, que acosar no es atractivo, pero saber lo que pasa con tus amigos sí lo es. Esta es información que las personas tenían que buscar todos los días, y ahora está bien reorganizada para que ustedes puedan aprender de las personas a las que quieren. Nada de su información es visible para nadie que no la pudiera ver antes de los cambios (2006b, en línea).

Ben Parr, estudiante de la Universidad de Illinois, creó el grupo “Estudiantes en contra del News Feed de Facebook” en el que escribió: “Fueron demasiado lejos esta vez Facebook, muy pocos de nosotros queremos saber automáticamente lo que actualizamos [...] News Feed es demasiado espeluznante, demasiado acosador y esta característica debe terminar”. El grupo alcanzó 100 000 fans en un día y en tres días aumentó a 700 000. Otros 500 grupos se organizaron en contra y al menos un 10 % de los usuarios no estaba de acuerdo con el nuevo Facebook.

Pero ¿cómo lograron los diseñadores de código mantener las características atractivas del sitio y evitar que las personas abandonen la red social? Cox, Sanghvi y Bosworth se dedicaron a escribir, en 48 horas, nuevas características de privacidad que les dieran a los usuarios cierto control sobre la información que se desplegaba sobre ellos en News Feed. Los cambios de estatus o los comentarios en las fotos fueron de los primeros asuntos en tomarse en cuenta en este nuevo diseño. Zuckerberg volvió a escribir a los miembros de Facebook.

Esta vez sí que la fastidiamos. Hicimos un mal trabajo explicando lo que eran las nuevas características y lo hicimos todavía peor al no darles control sobre ellas [...] No hemos construido los propios controles de privacidad inmediatamente. Esto fue un error de nuestra parte y me disculpo por ello. También les informo que estaré participando en una discusión en vivo y en directo sobre *News Feed* en un grupo llamado “El libre flujo de la información en internet” (2006c, en línea).

Además de los anti-News Feed se armaron grupos como “si alcanzo 100 000 usuarios mi novia acepta hacer un trío”, que logró la meta en tres días. El alcance viral que tenía el nuevo Facebook era la verdadera revelación para sus codificadores. Todo ello con la radical premisa de Zuckerberg: total transparencia.⁵

Las lecciones para los escritores de código eran varias: a la gente le gustaba saber de los otros y los usuarios pasaban más tiempo dentro de Facebook que antes.⁶ Las personas sentían que se habían removido obstáculos que los

⁵ Para Zuckerberg, alcanzar la transparencia radical era un proyecto con una duración de entre 10 y 15 años (Kirkpatrick 2010, 275).

⁶ Antes del servicio, los usuarios veían 12 000 millones de páginas dentro de Facebook; para octubre con News Feed, la cifra subió a 22 000 millones.

protegían de la intrusión. Se requería de tiempo para que los usuarios se adaptaran a los cambios, en especial si estos ponen de cabeza los mecanismos “normales de comunicación” reemplazándolos por una comunicación simultánea. Y, finalmente, el comportamiento de las personas estaba más expuesto y, por tanto, se les podía pedir explicaciones por sus acciones.

Sobrellevada la controversia de News Feed, nuevos cambios se hicieron en la red; los álbumes de fotos ahora se podían modificar, cambiar el orden de las imágenes y escoger quién podía o no verlas. No obstante, Beacon, otra característica que Facebook lanzó en agosto de 2007, originó graves problemas en la imagen de la compañía; consistía en un mecanismo para que los usuarios pudieran compartir información de sus actividades fuera de Facebook, en otros sitios web. Ello incluía las compras que los usuarios realizaban en línea y cuya información se repartía en el News Feed de sus amigos.

El producto tuvo que ser rediseñado inmediatamente, de un sistema *opt-out*,⁷ se tuvo que pasar a un sistema *opt-in*. Se incluyeron opciones en los controles de privacidad sobre Beacon, de modo que se pudieran desactivar algunas de sus aplicaciones o se pudiera apagar del todo. Beacon puso en entredicho lo que la compañía hacía con los datos de las personas lo cual generó una mala imagen de Facebook. La vulnerabilidad que los usuarios sintieron sobre su información creó una campaña mediática muy fuerte sobre el derecho a la privacidad. Tomó mucho tiempo para que esto se calmara; sin embargo, Zuckerberg estaba convencido de que Beacon llegó en un momento en que los usuarios todavía no estaban listos para compartir la información de lo que hacían en otros sitios web dentro de Facebook. En cierto sentido, pensaba que Facebook tenía las características de un gobierno más que de una compañía tradicional, pues establecía políticas dentro de una gran comunidad, mucho más que otras compañías de tecnología (Kirkpatrick 2010, 254).

⁷ El término fue acuñado por Richard Thaler y Cass Sustein en su texto *Nudge: Improving Decisions about Health, Wealth, and Happiness* (2008). Sugiere que una organización que presenta una opción puede inducir un resultado específico. A diferencia de un sistema *opt-in* (la persona voluntariamente firma una autorización), el sistema *opt-out* asume que la persona implícitamente ha aceptado la opción que el sistema le propone. En el caso de la donación de órganos, un sistema *opt-in* obliga a firmar la aceptación de que sus órganos sean donados, uno *opt-out* procede a la donación sin el consentimiento formal de la persona o la familia, porque automáticamente es un donante y para dejar de serlo se debe firmar una solicitud de “no donar” sus órganos previamente.

Al año siguiente apareció una característica de Facebook todavía más agresiva, para mostrar lo que los usuarios hacen fuera de Facebook y reflejarlo dentro de sus perfiles y sus News Feed: Facebook Connect, que se apoya en la noción de Social Graph, que fue la ruptura conceptual que Zuckerberg había logrado en Facebook, la interrelación de la sociabilidad en la red. Esta serie de nodos y conexiones en sentido matemático se traducían a individuos y conexiones de amistad conformando el más poderoso mecanismo de distribución creado en una generación, mecanismo que podía ser aplicado no solo a grupos, fotos o eventos, sino a cualquier otra cosa (Kirkpatrick 2010, 216). Una vez que las personas se conectan con sus amigos ensamblan una red, la cual se denomina Social Graph, que puede ser usada para distribución de cualquier tipo de información. Establecido esto, Zuckerberg quería hacer de Facebook una plataforma, del mismo modo que Bill Gates había producido una infraestructura de *software* estándar que facilitaba construir aplicaciones sobre ella. Zuckerberg pensaba que Facebook podía funcionar del mismo modo para aplicaciones con componentes sociales: “Queremos hacer de Facebook un sistema operativo sobre el que se puedan correr aplicaciones completas” (Kirkpatrick 2010, 217). Una vez que una compañía se convierte en el ecosistema de las otras, se vuelve muy difícil sacarla del camino. Gates lo había logrado con Microsoft; Apple, con su sistema operativo Macintosh, iPod y iPhone.

Antes de lanzar News Feed se abrió API, una interface de programación de aplicaciones. Esta permitía ingresar a otros sitios web con la cuenta de Facebook; así el sitio web asociado podía extraer los datos de los usuarios, incluida la lista de amigos. API pasó desapercibida por el escándalo alrededor de News Feed, pero también porque hasta ese momento Social Graph no estaba funcionando y no permitía que la distribución se realizara. Si bien los datos podían sacarse de Facebook, el flujo no era circular y no se podía regresar dentro de Facebook. Con News Feed esto cambió y ahora los amigos podían enterarse de las aplicaciones que sus contactos estaban utilizando y registrarlas en sus propios perfiles. Inmediatamente del éxito de las aplicaciones, Facebook tuvo que desarrollar controles para que los usuarios pudieran denunciar aquellas que podían considerarse *spam*, y así poder bajar la intensidad de la distribución de las aplicaciones dentro del Social Graph.

Como expresó Ethan Beard, veterano de Google y también jefe de mercado de Facebook, algo fundamental que añadía la noción de Social Graph es que mientras más evoluciona no solo relaciona a personas, “nos hemos dado cuenta de que en el *graph* también están los objetos, las organizaciones, las ideas con las que se conecta la gente. Al mapear todas estas cosas podemos lograr delinear una identidad más robusta de las personas” (citado por Kirkpatrick 2010, 213). Zuckerberg señaló que los mapas que Facebook produce con esta información son el “flujo de la conciencia y la comunicación humana, y los productos que nosotros construimos consisten en algunas miradas de este flujo [...]. El concepto de Social Graph ha sido un constructo muy útil, pero el concepto de *flujo social* será igualmente importante” (citado por Kirkpatrick 2010, 213).

Facebook Connect fue creada para permitir una interacción entre usuarios y el resto de la web. Así, los usuarios podían salir de la plataforma hacia otros sitios, a través de opciones como *share* o *like* y traer al News Feed de sus perfiles la información producida en esos sitios. Entonces Facebook dejaba de ser un ecosistema autocontenido y creaba una capacidad de diálogo con otros sitios web, que a su vez podían también utilizar la información de los usuarios. Muchas compañías lo vieron como un caballo de Troya, porque una vez que entrara en acción se convertía en un mediador entre el sitio y el usuario, lo cual le daba la capacidad de empezar, con el tiempo, a realizar demandas como la de cobrar por su uso. También se convirtió en otro mecanismo para rastrear las actividades de los miembros fuera de la red, y obtener así más información de sus usuarios.

En abril de 2009 surgió Facebook Open Stream API, una especie de Facebook Connect. Mientras Connect permitía a Facebook extenderse en otras plataformas de la web, API admitía distribuir la experiencia de Facebook fuera del propio servicio. Así, dejaba que cualquier sitio use y publique el flujo en otra parte, el cual siempre está controlado por los servidores de Facebook, que siguen a la información donde vaya. Para Parker esta fue la apuesta más importante que hizo Facebook, una estrategia que permitió a la compañía resolver el problema de ser una red cerrada y lograr ubicuidad. Zuckerberg sostuvo que en vez de construir murallas alrededor, “Facebook se va moviendo con las prácticas

de interacción de sus usuarios. Sabemos que gran parte de la interacción de ellos está fuera de Facebook, Facebook en realidad acaba de empezar” (citado por Kirkpatrick 2010, 315).

Con este diseño, la red dejaba de ser un sitio web y se convertía, más bien, en una infraestructura, en un gran almacén de información, un punto de tránsito, un registro de identidad y un enlace entre personas. Esto dentro del sistema de negocios le otorgó un lugar excepcional a Facebook, en el futuro podría incluso funcionar como una memoria auxiliar, que proporcione información y también realice pequeñas decisiones por uno en interacción con otros sistemas inteligentes (GPS, por ejemplo). En 2010 se creó Open Graph API, una característica que extiende la plataforma de Facebook a toda la web; una nueva caja de herramientas de programación que dejaba entrar y salir información de Facebook. Las aplicaciones más importantes del Open Graph en ese año fueron:

- *Like*: permite a los usuarios compartir páginas desde un sitio hacia su perfil de Facebook.
- *Activity Feed*: muestra a los usuarios lo que sus amigos están haciendo en su sitio a través de *like* y *comments*.
- *Recommendations*: ofrece al usuario sugerencias personalizadas de páginas que le podrían gustar en su sitio.
- *Like Box*: permite al usuario hacer *like* de su propia página y ver en la web directamente su flujo de información.
- *Login Button*: enseña las fotos del perfil de los amigos que ya están usando esta aplicación.
- *Facepile*: muestra las fotos de perfil de los amigos.
- *Comments*: permite al usuario comentar en cualquier pieza de contenido en su sitio.
- *Live Stream*: es una ventana que permite compartir las actividades en tiempo real con los amigos.

El éxito de Facebook tuvo que ver, desde el principio, con mantener el sitio limpio y minimalista, del mismo modo que lo hizo Google. Un producto “simple” que les permita a las personas compartir información de la manera más sencilla. Esta simplicidad en ambos sitios

sirve para enmascarar la complejidad del sistema que está detrás de la interfaz. De ahí que para entender cómo funcionaba en los inicios la relación usuario-red social es necesario revisar los principios del diseño de Facebook. Son estos principios los que guían la experiencia de uso de la pantalla, la experiencia de representación del yo y la comunicación con los otros.

En Facebook nuestro diseño es...

Universal

Nuestra misión es hacer al mundo más abierto, y esto significa alcanzar a cada persona, a cada esquina. Nuestro diseño debe funcionar para todos, para cada cultura, cada lengua, cada aparato, cada etapa de la vida. Por ello construimos productos que funcionan para el 90 % de nuestros usuarios y sacamos las características que solo funcionan para una minoría, incluso si esto significa retroceder a corto plazo.

Humano

Los usuarios regresan a nuestro sitio para estar rodeados de amigos y de otra gente cercana a ellos. Esta es una promesa central de nuestro producto, que las personas que nos interesan estén todas en un solo lugar. Así, nuestra voz y nuestro estilo visual permanecen en el fondo, detrás de las voces, las caras y las expresiones de la gente.

Limpio

Nuestro estilo visual es limpio y amigable, produce un lienzo en blanco para que sea llenado por nuestros usuarios. Un espacio minimalista que invita a la participación y a una comunicación honesta y transparente. Un estilo limpio no es la opción más fácil. Al contrario, los márgenes los tipos de escala y el color se vuelven más importantes mientras reducimos el número de estilos en los que nos fundamentamos.

Consistente

Invertimos nuestro tiempo sabiamente, al abrazar patrones y reconociendo que nuestra usabilidad mejora notablemente, cuando vemos que partes similares se expresan en formas similares. Nuestras interacciones hablan a los usuarios con una sola voz, construir la confianza. Reducir, reusar y no rediseñar.

Útil

Nuestro producto es más un instrumento que un entretenimiento, está diseñado para uso diario repetido, proveyendo un valor eficientemente. Así, nuestro centro de interacciones, las que los usuarios realizan

diariamente, son racionalizadas y purgan los clics innecesarios y el desperdicio del espacio.

Rápido

Valoramos el tiempo de nuestros usuarios. Reconocemos que las experiencias rápidas son más eficientes y fáciles.

Transparente

Los usuarios nos confían su identidad, sus fotos, sus pensamientos y su conversación. Nosotros somos recíprocos con la máxima honestidad y transparencia. Afrontamos claramente lo que sucede y su por qué [traducción de la autora].⁸

Desde el principio Facebook propuso un mundo más pequeño, un espacio común a todas las personas sin importar su edad, cultura o lengua. Ello implicó diseñar un lugar en el ciberespacio que lograra unificar esta diversidad. Dicha homologación de la socialización es posible si los usuarios cuentan con guiones de conducta estructurados desde la propia arquitectura del sitio. Entonces, la función del diseño se revela con toda su potencia en el momento de crear unos modos de relacionamiento “universales” que van a marcar la vida social virtual de los sujetos.⁹ Acompañados de un principio de transparencia que se combina con un estilo visual limpio, se privilegia el “mostrar” al individuo. Para mostrarlo desde una premisa de transparencia radical, Facebook fue limitando el poder de las personas de controlar aquello que consideran privado quitándoles herramientas que facilitan esta acción y entregándoles un nuevo conjunto de instrumentos, cada uno más complejo que el anterior. El estilo “limpio y amigable” que promociona la red se fue convirtiendo en opaco y difícil de manejar cuando los usuarios trataban de escoger el nivel de privacidad que esperan dentro de la red.

⁸ “Facebook Design Principles”, *Blog de Facebook*, 1 de julio de 2009, acceso el 15 de abril de 2011. <https://bit.ly/3balanT>

⁹ En Facebook se encuentra amigos, lo cual permite mantener la familiaridad de lo conocido, invisibilizando las estructuras virtuales que se han levantado para inventar formas de socialización homologadas. El hecho de que búlgaros solo traten con búlgaros en su propia lengua dentro de Facebook les hace sentir en un lugar hecho exclusivamente para ellos, se establecen unas fronteras de lo conocido que funcionan como guiones cognitivos certeros, mezclas de códigos lingüísticos, culturales, sociales y tecnológicos. La capa cultural parece más evidente y opaca a la capa tecnológica que organiza la vida social igual en Bulgaria que en Japón o Estados Unidos.

A mediados de 2010 se crearon los grupos cerrados, en los cuales las historias que se creaban dentro no podían ser vistas por los amigos externos al grupo. Un nuevo cambio se introdujo en el sitio: una caja de publicador Publisher sobre la página de entrada en Facebook, una caja igual a la que tenían los usuarios dentro de su perfil. Debajo de ella, News Feed se había transformado en un flujo de actualización de información de amigos, pero también de sitios comerciales dentro de Facebook de los que los miembros se habían vuelto *fans*. El mensaje era cada vez más fuerte: “compartir”.

El flujo de información de News Feed emuló la forma en que circulaba la información en Twitter, una red social a la que Facebook estaba muy atenta desde hacía tiempo. Con los cambios, ahora era posible personalizar el News Feed, se podía agrupar amigos y páginas para que solo apareciera la información por ellos producida, también era posible diferenciar entre fotos, videos y actualizaciones de perfiles y estatus. Solo quedaba una pequeña parte reservada a información, llamada “destacados”, que Facebook escogía para sus usuarios.

Al seguir las huellas de Twitter se pudo abrir, días después, un nuevo *set* de configuraciones de privacidad que permitía la elección de volver público partes (o todo) el perfil de usuarios de Facebook. Para Parker, la “amistad” en Facebook debía ser, cada vez más, un canal bidireccional de interacción, pues Facebook tiende, con más fuerza, a difuminar los tres componentes que son parte de “hacer amigos”: declarar que uno conoce a alguien, aceptar que accedan a su información y suscribirse a ver la información que el otro produce. Así cambia la dicotomía “amigo” o “no amigo”, ya que otras categorías se van incluyendo en el camino para lograr mayor interacción entre los miembros de la red.

En principio, la recreación del espacio apeló a nuevas formas de relacionamiento, a la organización de la información producida, a la incorporación de las aplicaciones como parte de los modos de representación (Timeline).¹⁰ Pero hay algo que se debe tomar en cuenta en la negociación entre diseñadores de códigos y usuarios: el esfuerzo que los miembros de Facebook han invertido en la construcción de sus redes,

¹⁰ Aplicación que Facebook incorporó para rediseñar los perfiles individuales de los usuarios a finales de 2011. Este nuevo perfil permitía resaltar las fotos, los comentarios y los eventos que cada persona tiene, como un mecanismo para contar mejor su “historia” (McDonald 2011).

en la importancia que tiene la extensión de la socialización fuera de la web. Facebook ha invertido agresivamente en código y ha moldeado fuertemente su arquitectura para ejercer control. Esta práctica también es muy común en otras redes sociales, Second Life es uno de esos casos. Y es ahí donde se puede ver con más claridad el valor del código. Philip Rosedale (CEO de Second Life) explicó, en una entrevista con Lessig (2006, 114),

pensamos que debemos lograr codificar todo lo que podamos, por la escalabilidad que ello nos permite. Solo debemos mantener una política fuera del código cuando es exclusivamente necesario o todavía poco viable. Hay cosas que miramos y pensamos, bueno, algún día seremos capaces de traducir eso en código, pero por ahora, hagámoslo manual.

Lo que hace falta es entender mejor cómo funciona la regulación. Las normas han regulado la sociedad por medio del estigma que construían dentro de la comunidad, el Estado lo ha hecho con el rigor de la ley, el mercado por medio del precio y la arquitectura gracias a los límites físicos que ha impuesto. En un constante balance, la arquitectura, la ley y la costumbre han estructurado las relaciones en los lugares físicos y en el ciberespacio, donde se mantienen límites similares a través de las estructuras del *software* y los controles de acceso electrónicos (Mitchell 1996, 159). Algo muy importante a tener en cuenta en esta relación código-usuario es que mientras más débil sea la noción de comunidad dentro de un lugar del ciberespacio, más fuerza adquiere la regulación a través del código.¹¹

¹¹ Tal es el caso de los bancos en línea, donde el cliente ingresa de forma individual siguiendo las normas y controles establecidos para acceder a su información y realizar transacciones.

Capítulo 5

Transformando la red en una empresa

Lessig distingue entre dos tipos de cultura: aquella creada profesionalmente y la amateur. La diferencia entre ambas es que, en la cultura amateur, las personas crean por amor a lo que hacen y no por el dinero. Por siglos, los bienes culturales se han resignificado al pasar de sujeto a sujeto o han servido como fuentes de inspiración para nuevas producciones culturales. La creatividad ha funcionado democráticamente, desde el niño o la niña que dibujan en la escuela hasta el o la joven que hace un *cover* de su banda favorita; en tal ámbito, las tecnologías digitales han contribuido a compartir la creatividad en el mundo, extendiendo notablemente el alcance de la cultura amateur. Sin embargo, hoy en día se ha construido un sistema de regulación que tiene por objeto normar la economía de la producción de la cultura amateur, que nunca había sido regulada. La tecnología digital ha contribuido a que la regulación sea más efectiva y a que la cultura creada, profesionalmente, se enriquezca de la cultura amateur.

Cuando Mark Zuckerberg creó Thefacebook, en Boston, se alió con Eduardo Saverin, un amigo suyo de Harvard, para que se hiciera cargo de la parte financiera del sitio web y generar ingresos. Repartió las acciones de la compañía: 70 % para él y 30 % para Saverin. Cada uno puso un capital inicial de mil dólares. A los pocos meses, cuando alcanzaron los 30 000 usuarios debieron invertir diez mil dólares más por socio. Saverin empezó a conseguir pequeños contratos de publicidad con compañías que vendían servicios y productos para estudiantes. La publicidad empezó a entrar en Thefacebook en abril, dos meses después de su creación. En junio ya ofrecían comprar la compañía en veinte millones de dólares.

Thefacebook dio el salto a la publicidad cuando otros sitios como Wikipedia o Craigslist mantenían un modelo no comercial.

Y2M y Mastercard¹ fueron las dos primeras compañías grandes en publicitar en Thefacebook y no se dio trato prioritario a ningún cliente; de hecho, no podían “ver” sus propios comerciales, porque el espacio estuvo restringido solo para quienes tuvieran un correo electrónico de las universidades aceptadas en el sitio web. En esos meses, Zuckerberg declaró que pensó vender información de sus usuarios a las compañías para que organizaran mejor su oferta de trabajo a los graduados de Harvard, pero decidió no hacerlo porque ello le quitaría la diversión al sitio.² Apenas se abrió a otras universidades señaló que “en el futuro tal vez venda publicidad para recuperar dinero, pero que por el momento el servicio es tan barato que no lo amerita”.³ Luego de cinco meses de iniciada la aventura, Google se interesó en comprar la compañía; varios inversionistas ofrecieron comprar acciones, pero todos fueron rechazados.

Cuando los diseñadores de código pasaron a vivir a Palo Alto y Sean Parker se incorporó al grupo, se inscribió la compañía en Delaware, porque su legislación era favorable para compañías que se iniciaban, como Thefacebook. Al revisarse los términos legales de la propiedad intelectual de la compañía resultó que Zuckerberg y Moskovitz tenían los derechos sobre el *software* y el diseño del proyecto. La nueva compañía tenía los siguientes porcentajes accionarios: 51 % para Zuckerberg, Saverin 34,4 %, Moskovitz 6,81 %, Parker 6,47 % y el bufete de abogados 1,29 %. Los empleados podían comprar acciones cuando el capital de la empresa aumentara con los fondos de los inversionistas.

La compañía creció al recibir préstamos e inversiones (gráfico 4), en un primer momento de Peter Thiel (cofundador de Paypal), de Western Technology Investments y de Accel Partners unos meses más tarde. El negocio con Accel constituyó un hito en las inversiones de Silicon Valley; Accel invirtió 12,7 millones en Thefacebook y el valor posinversión de la compañía se calculó en 98 millones de dólares. Si a esto se añade que

¹ Mastercard pagaba solo por aplicación llenada por estudiantes. Recibió en su primer día el doble de aplicaciones de las que esperaba obtener en los cuatro meses programados en la campaña.

² Entrevista en *The Harvard Crimson*, “The nature of the site”, <http://bit.ly/1n7DwFT>.

³ El costo del sitio era de 85 dólares al mes.

Jim Breyer invirtió un millón de su propio dinero y que, además, los fundadores recibieron un bono de un millón cada uno, la negociación no tiene precedentes.⁴

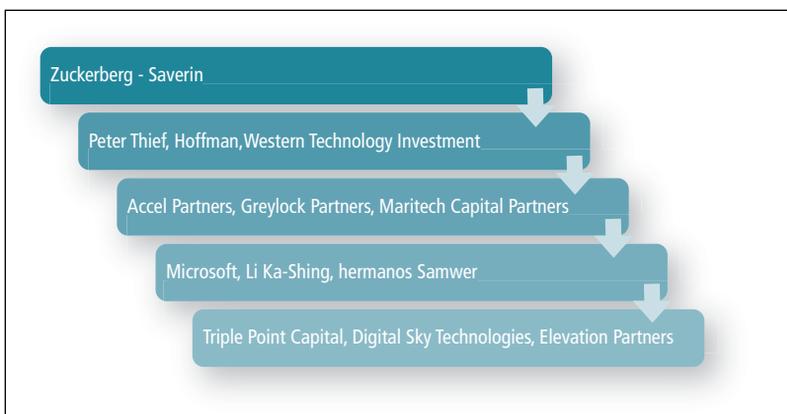
El año 2006 varias compañías querían comprar Facebook, luego de que MySpace fuera adquirida por Murdoch; MTV y Viacom estaban luchando por hacer una buena oferta, finalmente Viacom ofreció 1,5 mil millones de dólares por una compañía que apenas tenía dos años de haber empezado y que había obtenido solo 20 millones de ingresos hasta finales de 2005 (Kirkpatrick 2010). Ese año recibió su tercera inversión por un total de 27,5 millones de dólares en la que Thief y Accel Partners realizaron un aumento de capital. A pesar de las reticencias de Zuckerberg, Yahoo intentó comprar Facebook por 1000 millones de dólares en efectivo, pero las negociaciones no se concretaron.

Entre 2007 y 2008, Facebook negoció nuevas inversiones en la red. La primera negociación de la Serie D fue lograr tener una avalúo de 15 millones de dólares y sobre esa base vender a Microsoft el 1,6 % de sus acciones en 240 millones de dólares. A esto se añaden dos inversiones de Li Ka-Shing, un multimillonario de Hong Kong, por 120 millones, y de los hermanos Samwer de Múnich por 15 millones. En esa ronda se consiguió un total de 375 millones, la valoración más alta de la historia de cualquier compañía de tecnología. En 2008 la compañía tuvo unos ingresos por 300 millones y en 2009 por más de 550 millones, lo que implicaba un crecimiento impresionante del 100 %. En 2010 los ingresos superaron 1,3 millones de dólares.

En 2009, Digital Sky Technologies (DST) invirtió 200 millones de dólares en Facebook. DST es la compañía dueña de VKintakte (*in contact*), la red social clon de Facebook en Rusia. Con la internacionalización de Facebook se debió empezar a construir bases de datos fuera de los Estados Unidos.

⁴ En su primera gran inversión, Google fue valorada en 75 millones de dólares y no escuchó nada parecido a entregar bonos a los fundadores de una empresa que recién se iniciaba en el negocio.

Gráfico 4. Inversionistas de Facebook



En agosto de 2009 Facebook adquirió FriendFeed por 50 millones de dólares y con ello incorporó a varios fundadores de Google y de sus codificadores estrella. La idea era competir con Twitter, por lo que en agosto lanzó Facebook Light, concebido para teléfonos celulares y gente que no tenía acceso a banda ancha. Hasta ese año la compañía tenía menos de 500 accionistas para evitar que la Comisión de Intercambio y Seguridad norteamericana la obligara a publicar su información financiera; no obstante, su ingreso a la bolsa de valores era casi inevitable, ocurrió en febrero de 2012.

Nuevas alianzas para reinventar la publicidad en Facebook

A pesar de la inicial reticencia de Zuckerberg a incluir publicidad dentro de la red social, desde sus inicios contrató anuncios. Los primeros avisos comerciales de Thefacebook eran rectángulos verticales en la parte baja izquierda de la página; su salto a una nueva estructura comercial se dio en muy pocos meses al aprovechar la arquitectura del sitio en términos publicitarios. Con Paramount Pictures se produjo la primera innovación para producir publicidad, pues se armaron grupos de *fans* para promover sus películas. El anuncio invitaba a los usuarios a unirse a los *fans* y a discutir en el muro que película mantenía en Thefacebook.

Y2M trajo a publicitar los productos de Apple en la red, lo cual les dio una plataforma muy poderosa para estar en contacto con sus usuarios (estudiantes universitarios) y ofrecerles promociones como canciones gratuitas en iTunes. Apple pagaba un dólar al mes por cada uno de sus miembros en el grupo Apple. Otra innovación fueron los *flyers*, o anuncios que los estudiantes podían comprar y dirigirlos a públicos específicos como los compañeros de universidad.⁵

Se concibió AdSeed, un mecanismo equivalente al AdSense⁶ de Google adaptado a las redes sociales. Con él, cualquier producto, marca y objeto podía ser publicitado de forma personalizada en el “hogar” del espacio social. Lo importante de empezar con un público estudiantil universitario era que a esas edades se forman los hábitos de consumo: el primer carro, la primera tarjeta de crédito. Esto ya lo había comprobado Mastercard con su estrategia en Thefacebook.

Thefacebook no quería distraer a sus miembros con publicidad invasiva, de modo que estaban prohibidas las iniciativas *pop-up*. Esto obligada a los codificadores y las compañías contratantes a ser mucho más inventivos en el modo de exhibir la publicidad. Otro problema que la red tenía era que los usuarios no hacían clic con frecuencia en los anuncios publicitarios y eso los volvía poco receptivos a los mensajes comerciales. Por ello, el modelo publicitario que funcionaba ese momento en red, el modelo Google, no tenía futuro en Thefacebook. Se introdujo con cierto éxito otra estrategia de publicidad en línea, la CPA (Cost per Aquisition), con una compañía de juegos que pagaba 300 dólares por cada nuevo suscriptor de las partidas de póquer. Con un promedio de 200 usuarios registrados, ello reportaba un ingreso nada despreciable: 60 000 dólares mensuales.⁷ Otras compañías que financiaban grupos debían pagar mensualmente un mínimo de 25 000 dólares como Victoria’s Secret.

⁵ Cada anuncio costaba alrededor de 100 dólares diarios, incluso en las universidades más grandes. Este era un mecanismo muy bueno para promover actividades o anunciar fiestas. Para cuando Thefacebook cumplió un año, había enrolado a 400 universidades y había vendido 3,65 millones de dólares en *flyers* (Kirkpatrick 2010).

⁶ Programa que da ingresos a los sitios web a cambio de permitirle a la compañía de búsqueda colocar publicidad textual en sus páginas basadas en contenido.

⁷ Esto duró hasta que el juego en línea fue prohibido en Estados Unidos.

Dustin Moskovitz estaba atento a los gustos de los usuarios y empezó a sistematizar información que podía ser útil para dirigir publicidad a grupos específicos. Thefacebook fue la primera empresa que utilizó información proporcionada explícitamente por los usuarios, a diferencia de otras compañías que realizaban análisis inferenciales de los comportamientos y gustos de los internautas, a través de las *cookies* que se instalaban en sus computadoras.⁸

Ya en Facebook, Zuckerberg no estaba en contra de incluir publicidad, de hecho quería incorporar una que realmente sirviera a sus miembros. Por ello, en 2006, Facebook se asoció con J. P. Morgan Chase para promover las tarjetas de crédito Chase diseñadas, exclusivamente, para usuarios de esta red social. Las tarjetas ofrecían puntos Karma, que no expiraban y que se podían canjear por premios pequeños como entradas a conciertos. El sistema era muy sencillo, cada compra que se hacía con la tarjeta, por pequeña que fuera, otorgaba 20 puntos que podían ser acumulables, también se ganaba puntos por unirse al grupo de Chase en Facebook, por tomar un curso en línea sobre cómo manejar el propio crédito y, finalmente, la tarjeta era “social” pues se podía regalar puntos Karma a los amigos de Facebook.

Al estilo de Apple, Procter armó un grupo en Facebook con el fin de promocionar bandas para blanquear los dientes en las universidades, cerca de las tiendas Walmart donde se vendía el producto. El resultado fue 20 000 estudiantes uniéndose al grupo a cambio de entradas para cine y conciertos. Este experimento mostró que se podía lograr una publicidad diferenciada y llegar exclusivamente a los grupos objetivo, volviendo más potente la fuerza publicitaria de los productos.

Zuckerberg continuó negándose a utilizar publicidad tradicional, por lo que rechazó una oferta de Sprite, de un millón de dólares por una campaña, que volvería verdes las páginas de Facebook por un solo día.⁹ El reconocimiento del valor publicitario de Facebook era cada vez más evidente. Se asoció con Microsoft para que operara los *banners* en

⁸ Esta metodología tiene un alto índice de error, porque muchas computadoras son compartidas y los anuncios son vistos por personas ajenas al grupo objetivo.

⁹ MySpace firmó en agosto de 2006 un contrato con Google para que operara dentro del espacio de MySpace a través de la colocación de publicidad por 900 millones (solo este trato volvió rentable a MySpace para Murdoch).

Facebook desde su AdCenter; con ello logró 100 millones de ingresos en el año 2007.

Otra innovación de la publicidad en línea fue el ingreso de las aplicaciones a la estrategia de publicidad de Facebook. Ello implicaba concebir a la red social como un ecosistema al que podían ingresar otras compañías sin costo. El modelo de negocios detrás de esta propuesta fue generar más páginas vistas y guardar un espacio en las páginas de aplicación de los otros para colocar la publicidad vendida por Facebook. De modo que la economía del don, propuesta por Zuckerberg, funcionaba a favor de Facebook desde el inicio, al ampliar los espacios virtuales donde colocar su publicidad.

La euforia de la compañía en las vísperas del lanzamiento del “f8”, el evento que abriría las puertas de Facebook a los desarrolladores de aplicaciones, se tradujo en frases como “Vamos a cambiar la internet”, “Vamos finalmente a poner a la gente en internet”, “Estamos creando la economía real de la web”. Morin, expleado de Apple, pensaba: “Así se debió sentir la construcción de la primera Macintosh” (Kirkpatrick 2010, 223). El “f8” fue el primer gran anuncio que realizaba la compañía y generó mucha expectativa en Silicon Valley. Zuckerberg dijo a los 750 invitados: “Juntos estamos empezando un movimiento”. Más de 40 compañías presentaron sus aplicaciones. El *Washington Post* mostró el “compás político”, que permitía comparar tus puntos de vista con los de tus amigos; Joe Green, antiguo amigo de Zuckerberg en Harvard, exhibió *Causes*, una aplicación que ayudaba a las Organizaciones no Gubernamentales (ONG) a conseguir fondos; iLike¹⁰ fue otra de las estrellas de la noche.

En seis meses, 250 000 desarrolladores se registraron operando 25 000 aplicaciones y, por lo menos, la mitad de los usuarios había bajado una a su perfil. Zynga surgió así como una compañía de aplicaciones a raíz de la apertura de la plataforma de Facebook, y llegó a ser la compañía de aplicaciones más grande en Facebook. Las compañías de aplicaciones crecieron hasta el punto de que en 2010 los ingresos sumados entre todas ellas eran apenas menor al de Facebook, 835 millones de dólares.

¹⁰ Un día luego de lanzada, 40 000 usuarios la utilizaban; dos días después, 400 000.

Facebook obtuvo sus ingresos a través de la venta de publicidad, pero el verdadero negocio estaba en las aplicaciones. Estas usualmente incluían promociones de otras aplicaciones de Facebook, de modo que cada vez que un usuario hacía clic para registrarse en una de ellas, la compañía recibía cincuenta centavos. La compra de bienes virtuales era otra forma de ingreso que estaba adquiriendo fuerza; en 2010 se realizaron alrededor de 675 millones de transacciones dentro de Facebook para comprar *upgrades* en juegos, imágenes de rosas en San Valentín para regalar a los amigos, tarjetas de cumpleaños, la casa de la nueva mascota virtual, etc.

El problema de que los usuarios de Facebook se registraran en las aplicaciones era que autorizaban a extraer de sus perfiles la información que estas querían; una vez que la información estaba en manos del desarrollador, el usuario perdía el control sobre sus datos. No quedaba claro el uso que se puede dar a esa información, se sabe que ciertos desarrolladores vendían esta información a compañías fuera de la plataforma de Facebook. Marc Rotenberg, de Electronic Privacy Information Center (EPIC), sostiene que “Facebook y sus socios de negocios aprenden mucho sobre nosotros, en cambio nosotros sabemos muy poco sobre ellos o sobre lo que hacen con nuestra información y cómo la usan” (Kirkpatrick 2010, 233).

Facebook creó Facebook Connect para permitir a sus usuarios salir de los confines de la plataforma y navegar en otros sitios web con su identidad de usuario, compartiendo comentarios que se realizaban en otros lugares virtuales y referenciándolos al muro de sus perfiles. En la práctica se hizo a través del botón *like*. Al cabo de un año de empezada la alianza con Microsoft para la venta de publicidad, renegoció su contrato, le vendió un porcentaje accionario y cambió el modelo de publicidad dentro de Facebook.

Ahora cualquier entidad comercial podía crear una página en Facebook gratuitamente, con las mismas características de un perfil personal, incluida la característica de albergar aplicaciones. Lo denominaron el modelo de *sponsored page* que intentaba atraer la mayor cantidad de compañías posible en el supuesto de que, una vez dentro del sitio, estarían interesadas en publicitar incluso si tenían un sitio gratuito. Una vez que las compañías lograron abrir sus perfiles como usuarios, las alertas de amistad también empezaron a funcionar en News Feed. Así, si alguien se hacía

“amigo” del *Washington Post*, esta información llegaba a gran parte de su red de amigos, indicando incluso el artículo que la persona había leído. Significaba que la actividad que se realizaba en los sitios web externos se reflejaba dentro del Social Graph de Facebook.

Otra estrategia que se implementó de forma paralela fue el *self-service advertising*, una contratación de publicidad directa a Facebook a través de su sitio web. Les permitía a las compañías, incluso a las más pequeñas, entrar a internet, diseñar y comprar publicidad en Facebook apuntando a una audiencia muy específica. Con ello se lograba, igualmente, que los dueños de las páginas se convirtieran en usuarios asiduos de Facebook, porque tendrían que cuidar la imagen de la compañía dentro de la red social. Otro componente de este nuevo tipo de anuncio era la publicidad social, los *social ads* consistían en vincular mensajes comerciales al apoyo de un usuario de Facebook.

Con la llegada de Sheryl Sandberg¹¹ como número dos de Facebook se empezó a pensar en cómo monetizar la compañía, es decir, cómo convertir en dinero a los usuarios de Facebook.¹² Mientras Google ayudaba a las personas a encontrar las cosas que ya habían decidido comprar, Facebook les asistiría para decidir qué querían. Mientras la publicidad de Google “llenaba la demanda”,¹³ Facebook iba a “producir demanda”.¹⁴ Esta producción de demanda no había funcionado en Google, lo había intentado con su servicio de Gmail, pero no en el sitio de Google. Por otra parte, los datos mostraban que solo el 20 % de los ingresos de la industria de la publicidad venían de personas que sabían de antemano lo que estaban buscando. El otro 80 % era el que se podía cubrir con la introducción de la publicidad en Facebook, persuadiendo a las personas a comprar los productos publicitados.

¹¹ Graduada en Harvard, era una ejecutiva estrella de Google, que ingresó a Facebook en mayo de 2008.

¹² En ese momento, Microsoft estaba vendiendo publicidad *banner* (menos del 25 % de los ingresos totales de Facebook). Self-service estaba creciendo rápidamente. Social Ads o Sponsored Stories (publicidad que se insertaban en el News Feed de los usuarios), así como los regalos virtuales tenían un crecimiento rápido, pero con una producción de ingresos muy baja; además, Facebook Marketplace, como sistema de anuncios clasificados, había tenido una respuesta fría de los usuarios.

¹³ Cuando se busca en Google, la respuesta es una publicidad que usualmente es la que se está buscando; este proceso produce millones de dólares a Google.

¹⁴ Este tipo de estrategia publicitaria es la que ha funcionado en televisión por décadas.

A esas alturas, los usuarios de Facebook habían canjeado gran parte de sus horas frente al televisor o frente a otros sitios en la web por estar en Facebook. “Existía un desbalance entre los lugares donde los dólares eran gastados y donde las audiencias pasaban más tiempo” (Kirkpatrick 2010, 260). Por eso, la publicidad que Zuckerberg pensaba debía funcionar en Facebook era aquella que abriera un camino de ida y vuelta entre el usuario y los anunciantes.

Debe ser esencialmente información orgánica que la gente produzca en el sitio. Mucha de la información que la gente produce es inherentemente comercial. Y si se pone atención al perfil de alguien, casi todos los campos que lo definen son, de algún modo, comerciales –música, películas, libros, productos, juegos–. Es parte de nuestra identidad como personas que nos gusten ciertas cosas, pero esto también tiene un valor comercial (citado por Kirkpatrick 2010, 260).

Así surgieron los *Engagement Ads*, un formato de anuncios con un mensaje sencillo en el perfil del usuario, que invitaba a hacer algo en la parte derecha de la página (comentar un video, ganar algo; –Starbucks ofrecía cupones para café, por ejemplo). A diferencia de otro tipo de publicidad de Facebook, el *engagement* no envía al usuario a ningún sitio externo, su meta está dentro de la propia red, como las aplicaciones o los eventos. Estas publicidades, con el botón *like* dentro del propio anuncio, no obligaban a los usuarios a suspender su actividad en Facebook en ese momento, luego de hacer clic en *like*. Pero una vez hecho el clic, empiezan a recibir actualizaciones del anuncio (ilustración 3).

Estos anuncios pronto reemplazaron a la publicidad social, porque esta no generaba información orgánica¹⁵ que la gente producía al usar el sitio; además, una vez que el anunciante logra un tipo de conexión con el usuario se adquiere algo que Facebook denomina “valor derivado”. Esto es, cada conexión que una marca hace con un usuario produce un promedio de 200 impresiones adicionales.¹⁶ Así, Facebook se constituyó en un ambiente ideal para publicitar, pues sus miembros pasaban mucho

¹⁵ Concepto tomado de la biología para manejar la información dentro del diseño computacional de las aplicaciones y del proceso de toma de decisiones que dirige las opciones de inversión (Fry 2000).

¹⁶ Una impresión es una ocasión en la que un usuario ve información sobre esa marca.

Ilustración 3. Engagement Ads

\$5MM on hand ×

 Chase is donating \$5 million to charities in your community, and you help decide where it goes. Give us a hand and vote now!

 What's the coolest way to give out \$5MM?

14% One penny at a time

44% **Drop it from an airplane**

42% Let people vote

[See how your friends voted.](#)

 [Become a fan of Chase](#)

tiempo dentro de la red, lo que generaba un sinfín de oportunidades para presentar anuncios. En tan solo un año produjeron ingresos superiores a los 100 millones de dólares y Facebook cobró cinco dólares por cada mil *engagement ads*. Este tipo de publicidad también acabó, en pocos años, con el trato con Microsoft de vender *banners*. Ahora Facebook solo vendía *banners* a través del sistema *self-service advertisement*, que servía para compañías locales que los compraban a través de tarjetas de crédito.

Otra categoría que surgió con Sandberg es la que Rose, vicepresidente de desarrollo de negocios de Facebook, denominó Consumer Monetization. Los usuarios pagaban a Facebook directamente por algo. Los bienes virtuales ya estaban funcionando y se podía innovar en otras formas de consumo como “créditos Facebook”, pues los usuarios se sentían mucho más cómodos pagándole a Facebook en vez de hacerlo a un tercero. Las ganancias de Facebook representaron el 30 % del crédito consumido. Algunos juegos en línea en ese momento habían decidido utilizar únicamente este método de cobro a sus usuarios de Facebook.¹⁷

¹⁷ La red sacó su propio sistema de dinero para las aplicaciones al convertir el balance de sus miembros en cuentas de su propia moneda. Los desarrolladores que cobraban a los usuarios por sus bienes virtuales en Facebook tenían que usar el servicio. Facebook sostuvo que deseaban

De esta manera, los consumidores estaban dispuestos a interactuar, por ejemplo, los helados Ben y Jerry dejaron que la gente escogiera el próximo sabor; sus *fans* aumentaron de 300 000 a más de un millón en seis semanas (Kirkpatrick 2010). Antes de Facebook las compañías debían contratar servicios de inferencia conductual para examinar la navegación de los usuarios en internet, con el fin de apuntar a los posibles clientes por rango de edad, género, localidad e intereses. En Facebook, los propios usuarios producen perfiles de vida, que pueden ser utilizados por los publicistas para diferenciar los grupos objetivo. Facebook se había convertido así en el medio con públicos meta más importante de la historia. El problema nuevamente era que todas las personas, menos los usuarios, sabían cómo se utilizaban sus datos. Facebook indicaba que no se utilizaba información individual de sus usuarios, que se usaba solo la información agregada que producen, y que a los anunciantes se les dejaba escoger, de un gran menú, las opciones a contratar. Para los Engagement Ads se hacen búsquedas específicas de los productos, por ejemplo, sistematizar la música más escuchada por el grupo objetivo para que la compañía pueda tener una idea de qué tipo de música usar en su próximo comercial.

Otro ejemplo es el trabajo que Facebook desarrolló con Nielsen Homescan, un servicio que correlaciona información sobre los productos que se compran en los hogares norteamericanos y el comportamiento de estos usuarios en Facebook. De tal modo, los anunciantes conocían cuáles son los anuncios que los usuarios han visto y cuáles los productos que han comprado. Para Mike Lazerow, CEO de Buddy Media, “cuando combinas cuatrocientos millones de personas con datos de no solo dónde viven, sino de quiénes son sus amigos, qué les interesa y qué hacen en línea, Facebook tiene potencialmente el proyecto genoma de internet” (citado por Kirkpatrick 2010, 267).

Antes de la llegada de Sandberg a Facebook, la compañía solo tenía oficinas de ventas en Palo Alto, Nueva York y Londres. Luego sus locales principales se extendieron a Dublín y sus oficinas a Dallas, Atlanta,

“simplificar la experiencia de compra” y de paso se llevaban un 30 % del valor de cada transacción. Esta estrategia daba la oportunidad a las empresas de suscribirse en el sistema, pues Facebook ofrecía descuentos por créditos más grandes, por ejemplo, 50 créditos costaban 5 dólares pero 2360 créditos, 200 dólares.

Hamburgo, Detroit, Milán, París, Austin, Tokio, Hyderabad, Seattle, Madrid, Estocolmo, Los Ángeles, Sydney, Washington y Toronto. Según Sandberg, se había propagado el mito de que todos están esperando por el modelo de ingresos, pero Facebook tiene el modelo de ingresos y ese modelo es la publicidad, “ese es el negocio en el que estamos y está funcionando” (Kirkpatrick 2010, 273). Paralelamente a esta experiencia comercial, en los últimos años se ha notado una reducción de los ingresos por publicidad en la televisión, las revistas, la radio y los periódicos. Facebook se había convertido en un lugar ideal para invertir en publicidad, cuando la atención hacia nuevos medios estaba cambiando; ello significó invertir menos dinero en los medios tradicionales. Facebook mostró 297 000 millones de anuncios en el tercer cuatrimestre de 2010, lo que significó el 23,1 % de todos los anuncios en línea de ese año (Kirkpatrick 2010, 272).

La economía política de Facebook

Para entender la construcción de Facebook como artefacto sociotécnico abordo las teorías que guían a sus diseñadores. He anotado cómo Zuckerberg fundamentó el desarrollo de la socialización en Facebook, a partir de la teoría de la transparencia radical y del valor del código en la construcción de los espacios virtuales. No obstante, para comprender el modo en que monetiza la actividad de los usuarios es necesario analizar la economía política del artefacto sociotécnico. Por ello, empezaré introduciendo las nociones de economía digital, Free Labor o mano de obra gratuita hasta llegar a la economía del don, en el ámbito de la alta tecnología, para descubrir cómo Facebook instaura un régimen de propiedad en los datos de los usuarios.

Es necesario superar la noción de que el ciberespacio sirve para escapar de la realidad, pues nos impide entender cómo la “realidad” de internet está profundamente conectada con el desarrollo tardío posindustrial de la sociedad. Una de las características de la economía posindustrial son sus trabajadores del conocimiento, característica que profundiza en el cuestionamiento de la legitimidad de la distinción entre producción y consumo o trabajo y cultura (Terranova 2000). A través del Free Labor,

o mano de obra gratuita, podemos entender el proceso por medio del cual la producción y el consumo se reconfiguran, y revisar una lógica de valor distinta (Terranova 2000).

Seguendo a Barbrook ([1999] 2005), la economía digital se caracteriza por las nuevas tecnologías, los nuevos trabajadores (artesanos digitales) y por ser una economía mixta compuesta por tres elementos: un ámbito público (Estado), el mercado y la economía del don. Esta economía mixta permite que convivan, en simbiosis, la mercantilización de la información que propone el capitalismo y la economía del don *high-tech*. Barbrook propone que el capitalismo intenta reimponer el régimen de propiedad y la mercantilización como estrategia para resolver el anarcocomunismo de la web.

Dentro de la economía digital, la del don debe ser entendida como una importante fuerza de trabajo en el capitalismo tardío, y como un momento fundamental de la creación de valor en las economías digitales. Ello porque la fuerza de trabajo se debate entre un deseo histórico cultural de producción creativa y un capitalismo que enfatiza el conocimiento como la principal fuente de valor (Terranova 2000). Los desarrolladores de aplicaciones de Facebook no trabajan porque el capitalismo los obliga, lo hacen por un deseo afectivo y por una producción cultural que ha sido socialmente configurada.

El trabajo cultural, técnico y creativo que fundamenta la economía digital ha sido posible por el desarrollo del capital más allá de la industrialización temprana y los modos de producción fordistas, y, por tanto, es particularmente abundante en las áreas donde el posfordismo ha funcionado en las últimas décadas. En los países en vías de desarrollo, el fin de la fábrica ha explicado la obsolescencia de la vieja clase trabajadora, pero también ha producido generaciones de trabajadores que se han convertido en consumidores activos. Free Labor es el momento en que esta cultura de conocimiento de consumo se traduce en actividades productivas que se adoptan placenteramente y que la mayoría de las veces son explotadas sin vergüenza (Terranova 2000, 37).

Zuckerberg ha entendido cómo funciona la economía del conocimiento y ha construido algo fundamental para que se aplique, “un ambiente creativo y de comunicaciones abiertas donde los trabajadores pueden

funcionar efectivamente y mejorar su conocimiento” (Barbrook [1999] 2005). Tanto los usuarios de Facebook como los desarrolladores de aplicaciones encuentran este tipo de entorno de economía digital en la plataforma de la red, y le añaden un valor que la empresa mercantiliza a través de su régimen de propiedad. Hemos visto cómo Facebook aplica la licencia PI (propiedad intelectual) para apropiarse de los contenidos que sus miembros producen y monetizarlos.

Terranova (2010, 38) problematiza la noción de economía digital, abandona una de sus equivalencias (las formas de trabajo avanzadas) y escoge analizar la economía digital como un mecanismo específico interno de captura de conocimiento cultural y social, y un área de experimentación del valor y del trabajo gratuito cultural/afectivo. No se trata de ver cómo el capitalismo se apropia de los productos de la imaginación colectiva de una subcultura, sino de revisar un proceso de flujos que se originan dentro de un campo que ya es capitalista, que canaliza un trabajo colectivo en flujos monetarios y la estructura dentro de prácticas de negocio capitalistas. Entonces se observa que el capitalismo globalizado en la sociedad del conocimiento no es estructuralmente diferente al capital de los tiempos fordistas, sino que funciona de un modo diferente en los modos de acumulación.

El capital económico sigue siendo el capital económico, la función del saber se limita a operar a su servicio. El conocimiento no es el nuevo capital económico, sino que colabora a generarlo; pero ello puede hacerse solo si cierto capital económico previamente acumulado permite “contratar” a ese conocimiento poniéndolo a su servicio y subordinándolo consecuentemente; no cualquier conocimiento es valorizado por el capital. No estamos ante la valoración capitalista del conocimiento en general, sino solo de un muy específico tipo de conocimiento: aquel con consecuencias tecnológicas determinables (Follari 2005, 273-74).

En las últimas décadas, los movimientos culturales han generado millones de dólares a las multinacionales capitalistas, tanto por el consumo como por la producción de bienes culturales. Han entregado elementos que han sido capitalizados por la industria para crear tendencias en los ámbitos de la moda, música, videojuegos, televisión y cine.

El producto del trabajo cultural colectivo no ha sido simplemente apropiado, ha sido canalizado voluntariamente y estructurado controversialmente dentro de las prácticas de negocios capitalistas. La relación entre cultura, industria cultural y trabajo en estos movimientos es mucho más compleja que la noción que sugiere la incorporación. En este sentido, la economía digital no es un nuevo fenómeno, pero es una nueva fase de una larga historia de experimentación (Terranova 2000, 39).

Para entender cómo los usuarios de Facebook generan valor es necesario recurrir a la noción de “trabajo inmaterial” que utilizan los autonomistas italianos. El trabajo inmaterial está compuesto por dos aspectos: el *contenido informacional* de la mercancía (los cambios en el lugar de trabajo, las destrezas adquiridas) y la actividad que produce el *contenido cultural* de la mercancía. El trabajo inmaterial tiene que ver con una serie de actividades que normalmente no se reconocen como trabajo y que son fundamentales para crear tendencias culturales, estándares artísticos, gustos, normas de consumo y opinión pública.¹⁸ “El trabajo inmaterial es una virtualidad (una capacidad indeterminada) que le pertenece a la subjetividad de la producción posindustrial como un todo” (Lazzarato citado por Terranova 2000, 41).

En tal sentido, Facebook canaliza un conocimiento que es inherentemente colectivo y lo compensa económicamente de forma selectiva. Utiliza un trabajo cultural colectivo que vuelve posible que Facebook exista como negocio rentable y que genere ganancias a expensas de la socialización virtual de sus miembros. La originalidad de Facebook, como modelo de negocios, ha sido consolidar una entidad colectiva que reúne a redes de trabajo inmaterial, estructurándolas de forma jerárquica y permitiéndoles actualizar su virtualidad en producciones afectivas, culturales y técnicas.¹⁹ Así, la empresa retiene el control de estas virtualidades y de sus procesos de valorización.

¹⁸ El conocimiento se resiste a la cuantificación y el trabajador del conocimiento es una categoría social impugnada. Por ello, el trabajo no es equivalente al empleo, por lo que con esta distinción es posible visibilizar la importancia que tiene el trabajo afectivo y cultural en las industrias mediáticas, las viejas y las nuevas (Terranova 2000).

¹⁹ Un trabajador del conocimiento no necesariamente debe ser un sujeto con una formación específica calificada, puede ser cualquiera que tenga la capacidad de realizar una actividad dentro de las sociedades posindustriales.

En una entrevista, Zuckerberg explicó su concepción de la economía de Facebook a partir de la teoría del don.

Es una alternativa a la economía de mercados en culturas menos desarrolladas. Se contribuye con algo a alguien y esa persona en respuesta, bien por obligación o generosidad, corresponde también con algo. Toda la economía funciona en una economía de contribución mutua. El marco que permite que esta economía funcione es que las comunidades son lo suficientemente pequeñas como para que sus contribuciones sean visibles. Una vez que las comunidades crecen, el sistema colapsa [...]. Internet crea ahora las condiciones de transparencia necesarias para que las economías del don funcionen a gran escala y coloca la carga en las compañías y las obligaciones para ser más buenas y más confiables. Cambia la forma en que los gobiernos funcionan, un mundo más transparente crea un mundo mejor gobernado y más justo (Kirkpatrick 2010, 287).

Para el creador de Facebook, cada expresión pública individual era un “don” para con los otros. En la forma más banal era una ofrenda a la amistad, a la sinceridad; en una forma más política, era un don a una economía de libre intercambio de ideas. Internet se estaba convirtiendo, en esta perspectiva, en el locus de la sociedad civil 2.0. Los políticos también se han beneficiado de esta economía del don. Así lo demuestra la campaña de Obama para la presidencia, quien lo hizo de forma excepcional con la ayuda de Chris Hughes; ellos consiguieron millones de seguidores en Facebook para armar grupos de apoyo a la candidatura; movilizaron, en masa, a los seguidores de Obama.²⁰

Facebook redefine las noticias en millones de páginas que son producidas por individuos y consumidas por sus amigos; “crea noticias para ti, tú creas noticias para mí” actualiza un entramado de la economía del don que Zuckerberg promueve. Así, no intenta ser un repositorio de noticias producidas fuera de la red social; todo lo contrario, funciona porque las noticias se generan dentro de la red, y ese es el valor que Zuckerberg le dio siempre a News Feed, como una fuente relevante de noticias o “historias” como él las llamaba (Kirkpatrick 2010, 295).

²⁰ Al reconocer las herramientas digitales lograron involucrar a una generación que se mantenía alejada de las campañas políticas.

“Las redes de personas actúan como un filtro relevante y descentralizado de las noticias fuera de Facebook y las introducen en la red [...]. Le queremos dar a las personas el mismo poder que tienen los medios de comunicación para lanzar un mensaje” (Parker citado por Kirkpatrick 2010, 296).

Free Labor no equivale necesariamente a explotación del trabajo. En las experiencias de las primeras comunidades virtuales era difícil encontrar una compensación financiera al trabajo de sus miembros. Por tanto, era un trabajo gratuito y placentero, no impuesto por nadie. El movimiento de *software libre* es un ejemplo de este tipo de Free Labor en internet.²¹ Zuckerberg aprovechó los códigos y los lenguajes generados dentro de este movimiento y capitalizó las características que convertían un sitio en el mejor sitio web dentro de internet: ser visible en la web, ser un espacio de fácil acceso, pero, sobre todo, ser construido por sus usuarios. La ética *hacker*, que había permeado la socialización virtual, fue utilizada por Facebook en su diseño minimalista de una página en blanco a ser escrita por sus usuarios. Justamente esta arquitectura permitió que el sitio crezca gracias al trabajo de sus miembros, a través de las innumerables horas que le dedicaban a generar contenidos, relatar su vida y subirlos traducidos a información. La mano de obra gratuita que opera en Facebook, a través de la interacción de sus miembros, es parte de la combinación entre economía del don y la economía capitalista que opera en internet, lo que no significa que estas prácticas sean benignas o poco problemáticas.

Los propios medios comunicación ingresan al ecosistema de Facebook y se benefician de su economía del don, para lo cual tienen que actuar como individuos. Facebook se ha convertido en uno de los vehículos de tráfico de mensajes más importantes de internet para los medios de comunicación, solo le sigue de cerca Google. Compite con los medios en la publicidad, ya ha captado el financiamiento en anuncios que antes iban a la televisión, los periódicos y las revistas. Por ello varios medios han decidido trabajar con Facebook, beneficiándose en el camino de conocer mejor a sus audiencias y su demografía. Muchos piden a sus

²¹ No debemos olvidar que la base ideológica que fundamenta el *software libre*: la cultura libre, no niega dos categorías fundamentales del capitalismo, la propiedad y el mercado (Lessig 2006).

usuarios utilizar su identidad de Facebook para hacer comentarios a sus amigos.

No obstante, ha surgido un recelo recurrente respecto de internet, pues se afirma que contribuye a la desaparición de la realidad basada en una preocupación humanística por la “vida real”. Esta hiperrealidad confirma una sociedad sin humanidad y es la culminación de la conquista del campo de la representación. Las mercancías en la web no son materiales, son excesivas y no mantienen relación con los límites de las necesidades sociales de la vida real. Para Terranova, el problema de plantear el ciberespacio en estos términos radica en que la desaparición de las mercancías no es una desaparición material, sino una subordinación visible a la calidad del trabajo detrás de ellas. Esto es,

la mercancía no desaparece como tal, sino que se torna progresivamente efímera, su duración se comprime y se convierte más en un proceso que en un producto terminado. El rol del trabajo continuo, creativo e innovador como la base de un mercado de valor es crucial para la economía digital. El proceso de valorización (de la producción de valor monetario) pasa a ser el primer plano del trabajo que literalmente da vida a la mercancía (Terranova 2000, 48).

La hipótesis de Terranova de que Free Labor es estructural a la economía cultural del capitalismo tardío va más allá de oponer dos versiones de internet en el eje capital-anticapital. No se trata de descubrir si internet personifica el capitalismo o rompe con él, sino de entender cómo expande una lógica económica y cultural híbrida. En este marco, Zuckerberg ha utilizado la economía del don como una apariencia para introducir el régimen del capital en la producción gratuita de los contenidos culturales de sus usuarios.

Capítulo 6

Construyendo historias personales y *dossiers* digitales

Desde que las personas empezaron a habitar el ciberespacio han desarrollado un sentido social de los espacios virtuales, se han acostumbrado a pensar en los mundos en línea como lugares para socializar (boyd 2006; Donath y boyd 2004; Dwyer 2011). Los foros han funcionado para conectar a desconocidos, los servicios de citas son cada vez más populares y la gente se ha habituado a relacionarse con un gran número de personas a través de los medios digitales. Las redes sociales en línea son un producto de esta cultura digital; funcionan tanto como entornos para formar lazos nuevos, como representaciones de estas redes en el despliegue de conexiones individuales.

Gran parte de las personas que ha ingresado a una red social, incluida Facebook, lo hicieron por recomendación de amigos; otro porcentaje se volvió miembro para mantenerse en contacto con amistades y familiares de un modo más conveniente. Ello indica cómo la presión de los pares tiene un rol clave en el proceso de adopción de la tecnología (Quan-Haase y Young 2010). Facebook desde su inicio estuvo destinado a incorporar en el espacio virtual a los conocidos en persona, se trataba de una red social cuyo propósito no era encontrar a desconocidos –Social Searching–, sino de saber más sobre quienes ya conocemos –Social Browsing– (Lampe, Ellison y Steinfield 2006; Steinfield, Ellison y Lampe 2007). A su vez, la dimensión de mantenerse en contacto con los conocidos tiene dos funciones: vigilar –el deseo de observar lo que hacen sus contactos, cómo se ven, cómo se comportan–, y buscar –el deseo de reconectarse con los conocidos fuera de la pantalla–.

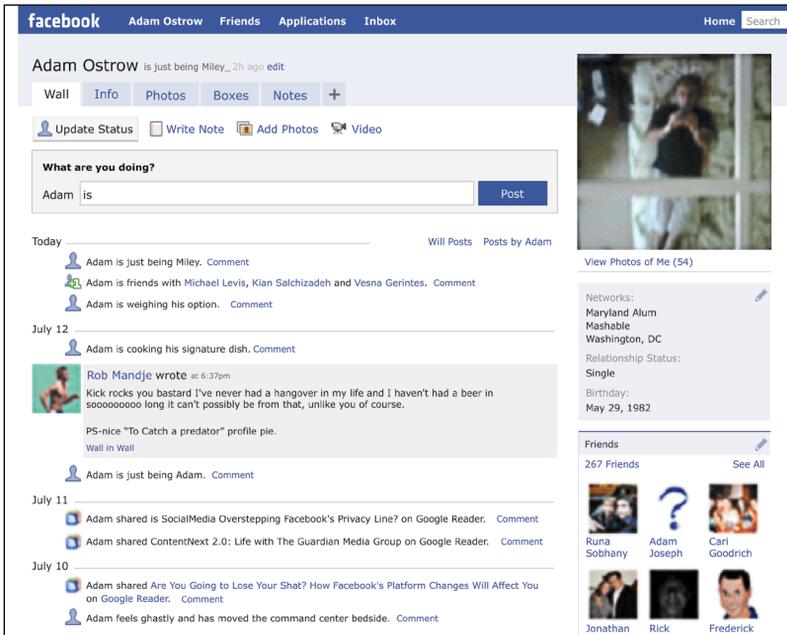
El perfil

La necesidad de crear un perfil digital, un yo virtual que se materializa a través de la información utilizada, condiciona la negociación de la representación del ser en línea. El perfil digital se va construyendo a través de las herramientas de Facebook. No hay mil modos de representarse, Facebook ofrece uno solo, el que su código condiciona. Entre otras cosas, no se puede subir un abanico de fotos al perfil porque el código permite subir una sola, o no se puede habitar Facebook como un avatar porque los mecanismos de confianza no dejan espacio para el anonimato. El perfil se elabora entonces a partir de las características que la propia red ha diseñado para que sean completadas por los miembros: nombre completo, foto de perfil, dirección de correo, ciudad, formación y empleo, información de contacto (teléfono y dirección), información básica (idioma, sexo, situación sentimental, fecha de nacimiento, creencias religiosas, creencias políticas), un mensaje de los usuarios para describirse, citas favoritas y familia.

Los nuevos miembros pueden optar por llenar todos los ítems de este menú o tan solo utilizar los que más les gusten, en función del tipo de representación de sí mismos que desean mostrar. Una vez que el perfil es visible se puede completar con una serie de nuevos elementos: fotos, acontecimientos importantes, “lo que estás pensando” dentro de su muro personal (Mini Feed), amigos, aplicaciones y actividades recientes.

En los mundos virtuales, incluso en Facebook, los usuarios se someten al diseño del sitio y se configuran a sí mismos siguiendo las pautas que el sistema les ofrece, en definitiva, también participan de un rol determinado, solo que más imperceptible. Mantienen así la adhesión al rol a través de la “regla de la conservación de la ilusión” (Giffin 1984), la cual consiste en que los jugadores se mantengan dentro de sus personajes y olviden que el contexto —en este caso, el espacio virtual— es una simple ficción. El éxito de internet es que ofrece espacios de simulación que apelan a las habilidades previas del usuario para adaptarse a escenarios de ficción, como las adquiridas durante la niñez. Y es justamente en la aventura del desdoblamiento que se pierden, entre otras, las nociones de privacidad que tanto valoramos fuera de la web. Por tal razón, firmamos los contratos que nos permiten ingresar al juego sin prestar mayor

Ilustración 4. Perfil en Facebook, 2008



Fuente: <http://bit.ly/1HLP2Eu>.

atención, sin leerlos siquiera –según Levin y Sánchez (2009) cerca de la mitad de los usuarios de Facebook no ha leído ni comprendido los términos del servicio– porque la atracción de obtener gratificaciones inmediatas es mucho más poderosa que el celo por nuestra privacidad.

Crear un perfil se enmarca en la relación entre cómo los sujetos se perciben y son percibidos, para lo cual es necesario intentar varias puestas en escena, jugar con los elementos de representación que el artefacto ofrece y aprender nuevos modos de relacionamiento utilizando los componentes del sitio (muro, News Feed, aplicaciones, álbumes de fotos). Estas prácticas son críticas para la socialización pues están atravesadas por normas sociales desconocidas fuera de la pantalla y por la interrelación de elementos tecnológicos y sociales. Las dinámicas de producción de identidad requieren la creación de cuerpos digitales y del despliegue público de la misma; las personas deben representarse textualmente hasta lograr “ser”, deben moldear su yo virtual a través del lenguaje y los elementos

icónicos que están a su alcance hasta lograr su re-presentación.¹ Los artefactos digitales reemplazan el mundo físico para crear el cuerpo digital y, es a través de la interacción con otros cuerpos digitales, que los artefactos de *performance* crean el contexto del entorno digital (ilustración 4.). Por ello es fundamental que la personas logren interpretar el contexto social para que actúen de acuerdo con lo que les es permitido (boyd 2007).

Los usuarios, entonces, siguen guiones para poder habitar Facebook. Su representación se construye en relación con lo que la red social le permite; es esta relación entre usuarios y tecnología la que descubre la inflexibilidad y cómo los objetos tecnológicos ciñen las relaciones sociales y los vínculos entre las personas y las cosas (Akrich 1992; Latour 2002). Al comparar la tecnología con el cine, Akrich (1992, 208) sugiere que,

[c]omo un guion de cine, los objetos técnicos definen el marco de acción juntamente con los actores y el espacio en el cual se supone deben actuar [...]. Los diseñadores construyen –explícita o implícitamente– imágenes de usuarios con distintos gustos, competencias, motivos, aspiraciones, prejuicios políticos, etc.

Así, inscriben estas representaciones en el contenido tecnológico de los nuevos artefactos. Como resultado, estos contienen unos guiones y prescriben, de forma más o menos coercitiva, lo que los usuarios deben o no hacer para producir el funcionamiento deseado del artefacto tecnológico. Tanto Latour (2005) como Akrich cuestionan la SCOT, desde la teoría actor-red, por sostener que solo las personas pueden tener el estatus de actores. Mientras que el guion intenta describir cómo los objetos técnicos “participan en la construcción de redes heterogéneas que reúnen a actores de todo tipo y tamaño, humanos o no humanos” (Akrich 1992, 206), las tecnologías son representadas como proyectos de identidad.

Akrich y Latour introducen los conceptos de *suscripción*, *de-inscripción* y antiprograma en el estudio del rol activo de los usuarios en la construcción de sus relaciones con los objetos tecnológicos. Usan la

¹ Quéau (1995, 105) propone que “toda representación es una presencia debilitada, que *carece* de presencia, pero que subsiste porque se repite, se sustituye a sí misma. A pesar de su nombre, la representación no es una *re*-presentación sino una *re*-introducción del sentido, un retorno del sentido”.

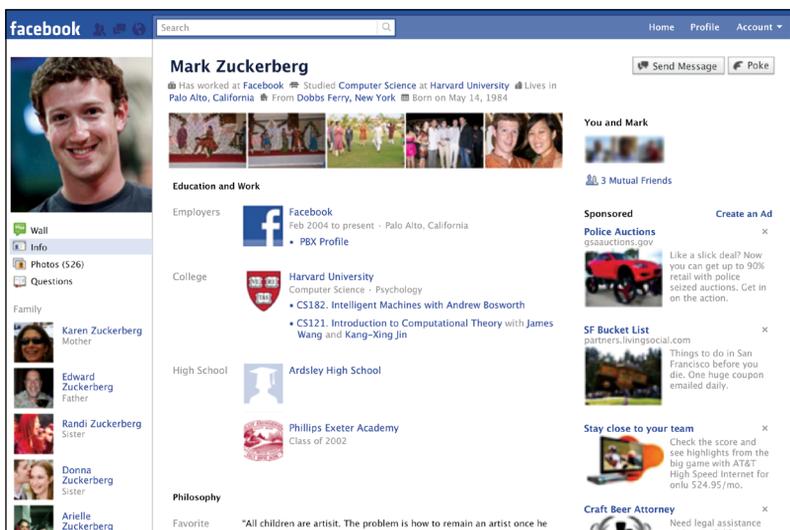
suscripción y de-inscripción para analizar las reacciones de los actores humanos (y no humanos) a lo que les es prescrito y proscrito, cómo suscriben, rechazan o negocian estas prescripciones. De modo que, el análisis del guion concibe a diseñadores y usuarios como agentes activos del desarrollo tecnológico. Algunos teóricos han incluido el estudio de redes de sujetos para comprender el apego entre las personas y las cosas y explorar, de qué manera, las tecnologías trabajan en la articulación de subjetividades (Callon y Rabeharisoa 1999; Law 1998; Law y Mol 2001; Moser 2000).

Seguir el guion de Facebook puede ser solo una parte de cómo el sujeto se alinea con una tecnología específica. Las normas sociales fuera de la pantalla están ejerciendo gran presión para que las personas ingresen a la red social: “He tratado de aguantar y de ir contracorriente pero no puedo” (estudiante citado por Cassidy 2006, en línea). Los amigos influyen en los otros para ser parte de Facebook, muchos diseñan sus perfiles para ganarse la aprobación de sus pares.

En Facebook logras representarte de un modo nuevo en un espacio nuevo [...], no se trata de cambiar quién eres, sino de enfatizar diferentes aspectos de tu personalidad [...]. Si no tienes un perfil en Facebook, no tienes una identidad en línea [...]. No significa que seas antisocial, o que seas una mala persona, pero ¿dónde están las huellas de tu paso por una comunidad universitaria? No existes –en línea por lo menos–. Por eso es que tenemos a tanta gente ingresando. Necesitas estar en Facebook (Chris Hughes, citado por Cassidy 2006, en línea).

El perfil de Facebook (ilustración 5) constituye el cuerpo digital de los sujetos, pero a la vez es una creación social, un texto que provoca conversaciones. Los perfiles construyen contextos sociales como procesos de comunicación y son una expresión de las normas sociales que rigen la red. Los perfiles negocian los límites de lo público y lo privado y enfrentan la capa tecnológica del artefacto en un constante aprendizaje de cómo interactuar para producir sentido en contextos digitales.

Ilustración 5. Perfil en Facebook, 2010



La construcción del Social Graph

La búsqueda de amigos y la conformación de la red personal de conexiones establecen vínculos con otros conjuntos de representaciones que pueden ser de distintos tipos: públicos, mutuos, sin matices y descontextualizados (Donath y boyd 2004). Los vínculos mutuos se establecen cuando se aceptan las relaciones de amistad, relacionando ambos perfiles en los Social Graphs de cada persona; los vínculos públicos permiten que cualquier miembro de la red acceda a la información del perfil, expuesta a la red social, sin que medien vínculos mutuos de por medio; los vínculos sin matices no diferencian entre amigos y conocidos, compañeros de trabajo y familiares.²

La red de relaciones en sí misma se convierte en parte del capital social que los usuarios adquieren dentro de Facebook y se incorpora a su perfil como un elemento más de representación del ser. Cada sujeto tiene una serie de posibilidades de representación que el código le ofrece (foto, intereses, creencias políticas y religiosas, lugar de trabajo, ciudad, música favorita, cine, lista de amigos, entre otras) y la lista de conexiones se convierte en parte del contexto dentro del cual su identidad virtual se

² Facebook incorporó la posibilidad de agrupar a los contactos en grupos personalizados.

construye. Pero también funciona como un mecanismo para establecer la confianza en la persona y en la red, pues la circularidad de la información termina validando los perfiles reales. No olvidemos que TheFacebook estableció dos condiciones fundamentales para ser parte de la red: usar el nombre verdadero y tener una dirección de correo electrónico de Harvard.edu. Esto con el objeto de autenticar los perfiles y asegurarse de que las personas fueran quienes decían ser, con lo que se esperaba generar mecanismos de confianza para que los miembros actúen en línea y utilicen el sitio llenándolo de información sobre sí mismos.

La lista de conexiones de un perfil contribuye a crear la identidad virtual ya que permite triangular la información que la persona reclama como cierta dentro de su perfil. Los amigos son quienes van a ratificar las descripciones que arman el mosaico de la identidad en Facebook, la red condiciona, con su arquitectura, la producción de normas sociales que premian la fidelidad de las descripciones o que sancionan a quienes las falsifican.³ La representación del ser fusiona el mundo virtual y el mundo fuera de la pantalla a través de estas prácticas de verificación. Y es justamente ello lo que provoca uno de los primeros problemas de habitar un espacio que aplanan los contextos presenciales donde funcionan las personalidades situadas (Goffman 1981).

Este nuevo *locus* virtual reúne a las distintas “personas públicas” que se interrelacionan en contextos diferenciados en la vida de los sujetos. Exhiben, así, facetas de su identidad que antes eran visibles para unos y opacas para otros. El borrar los contextos de las relaciones y de las máscaras utilizadas para cada uno de ellos crea, entonces, una potenciación de la exhibición del sujeto en su representación virtual. Ahora el usuario ya no puede ser “varios”, pues está obligado a ser “uno solo” y deberá mostrar su identidad “única” como lo propone Zuckerberg; ya no una identidad fraccionada. Ello en la premisa de que la transparencia radical contribuye a dar consistencia a las personas de forma relacional, entre lo que ellas proyectan y lo que los otros responden a dichas proyecciones.

El Social Graph también reúne, por medio de los vínculos, a diversas relaciones sociales en un mismo espacio; junta por ejemplo a la familia

³ “Los grupos sociales tienen el considerable poder de crear normas sociales. El poder de la reputación fuerza conductas de cooperación que funcionan a través de las conversaciones alrededor de él y no en prácticas de confrontación con el sujeto” (Donath y boyd 2004, 75-6).

con antiguos compañeros de escuela o con conocidos de negocios, yuxtaponiendo redes de relaciones que antes no se cruzaban entre ellas. El costo del sistema de confianza que Zuckerberg ha puesto en escena, a través del acceso a la información de los perfiles entre amigos, es la reducción de la privacidad, pues los ha expuesto a un sistema de conexiones que los ubica en un lugar virtual pero completamente público.

La gente quiere acceso a toda la información alrededor de ella pero también quiere el control sobre su propia información. Estas dos cosas se oponen mutuamente. Tecnológicamente podríamos colgar toda la información para que todos la vean, pero a la gente no le gustaría porque quieren control sobre su información [...] La información está dirigida a las personas correctas. Así que darle el control a la gente sobre quién ve qué, ayuda a incrementar el flujo de información en la red (Cassidy 2006, en línea).

El propósito de la vitrina de Facebook es conectar a la gente, abrir una cuenta en Facebook es contactar con amigos y conocidos. A partir de terrenos comunes, los usuarios empiezan a vincularse (amigos de amigos, conocidos del barrio, primos lejanos). Pero las conexiones no son un simple producto de intereses comunes, los usuarios deliberadamente intentan configurar una red que vuelva más fácil y eficiente sus vidas en línea, al reunir a todos aquellos a los que aprecia y a los que puede necesitar contactar en cualquier momento. Mientras en el mundo, cara a cara, las personas dedican mucho tiempo a mantener diferenciados los contextos de sus vidas, “las redes sociales vuelven visibles las conexiones para todos, eliminando las barreras de privacidad que las personas mantienen entre distintos aspectos de sus vidas [...] revelando asimismo facetas que pueden causar incomodidad tanto para el usuario como para el observador” (Donath y boyd 2004, 77). Podríamos decir que existen los Facebooks que cada uno crea: “Facebook es una especie de espejo de nuestra existencia social y no siempre disfrutamos de todos los aspectos de las comunidades de las cuales somos parte” (Wittkower 2010, XXII).

De esta manera, las redes sociales ofrecen un espacio para construir identidad y estatus, resolver los sentidos culturales y negociar la vida pública. Tienen cuatro características que no están presentes en la vida fuera de la red: persistencia, posibilidad de búsqueda, copia exacta y audiencias invisibles (boyd 2007). Así, Facebook promueve el crecimiento

de las redes personales; en muchos casos el número de amigos se vuelve un signo de popularidad. Los amigos operan como contexto de una audiencia imaginada que guía el comportamiento de los otros a través de normas sociales de conducta (Fono y Raynes-Goldie 2005). La competencia contribuye a configurar la amistad en línea y a fortalecer los lazos débiles de la red (Granoveter 1998, citado por Strahilevitz 2005).⁴

Interactuando en Facebook

A partir de un diseño minimalista, Facebook ha otorgado a los miembros aplicaciones y características del sitio para facilitar estar al día con lo que generan sus conexiones. Y una de las razones por las cuales la red es tan popular es porque permite a los usuarios tener relaciones activas con sus amistades. Un estudiante de Harvard comentó: “Es un modo de mantener a los amigos sin tener que hacer ningún esfuerzo [...]. La interfaz te da la información que necesitas para hacerlo: cumpleaños, fotos, mensajes, información de contacto, etc.” (Cassidy 2006, en línea).

Según Zuckerberg, las personas pueden compartir mucho más si no se les deja hacer lo que quieran y se les impone cierto orden (citado en Kirkpatrick 2010, 100). El código de Facebook lo hace visible, al mismo tiempo, los lazos alrededor de los usuarios. El código del *software* se constituye en una forma de arquitectura social (Lessig 2006).

Facebook ha resultado una red atractiva justamente porque los usuarios pueden extender su sociabilidad en los espacios virtuales, esos lazos fuertes son los que sostienen su interacción en línea (los amigos cercanos, la familia) y funcionan como fuente de soporte social por medio de relaciones que requieren de tiempo y atención para alimentarlas (Steinfeld, Ellison y Lampe 2007). El Social Graph también está constituido por lazos débiles que aportan mucha información y acceso a nuevo conocimiento, este tipo

⁴ El trabajo de Mark Granovetter (1998, citado por Strahilevitz 2005, 956) sobre la fuerza de los lazos débiles se ha convertido en un estudio fundamental para entender el funcionamiento de las redes sociales. “Lo que hace posible la difusión cultural es el hecho de que los pequeños grupos cohesionados que son responsables de compartir una cultura, no sean los suficientemente cohesionados como para cerrarse del todo; de modo que las ideas puedan penetrar desde otros grupos a través de lazos débiles [...] permitiendo vehicular ideas e información distintas a las de los propios grupos. Las ideas que originalmente fluyen desde otro grupo son probablemente nuevas. Las culturas homogéneas no surgen instantáneamente sino que son el último punto de difusión de un proceso”.

de relaciones es mucho más fácil de mantener (Granovetter 1983). Con tan solo una nota y un clic se puede pedir ayuda o información y las conexiones funcionan, no necesariamente porque conozcan sobre el tema, sino porque están dispuestas a ayudar. Se ha construido un vínculo que actúa como norma social de reciprocidad dentro de una red que mientras más grande es, más acceso logra a sus conexiones y a las oportunidades de contacto. Las redes sociales se han convertido en una extensión de los mundos sociales y funcionan también como el límite de las personas que pueden contactarnos. Facebook promueve el crecimiento de las redes personales, que no se limiten, la energía que las personas le dedican es un signo de los beneficios que adquieren (boyd 2006).

Facebook es un híbrido donde se mezclan las fotos de los amigos, las causas políticas, las películas recomendadas y los perfiles institucionales y políticos. Es el espacio de la convergencia, reúne todo aquello que antes pertenecía a esferas diferenciadas. Una de las cosas más fascinantes de esta red es que mezcla los mensajes personales con aquellos enviados a nadie en particular (Meikle 2010), y ha cambiado nuestra experiencia del mundo antes de que seamos capaces de tener una lectura crítica de lo que acontecía (Bogost 2010). El *performance* de los sujetos dentro de la interacción de Facebook tiene que ver con negociar con audiencias desconocidas, mientras que en el mundo presencial se puede mantener mayor control sobre lo que se dice en un momento particular, en línea no se sabe quién podría acceder a aquello que se expresa en los perfiles. Desarrollar e interpretar un contexto en la virtualidad es un diálogo en sí mismo, en Facebook se espera que los usuarios se enganchen en procesos de intercambios lúdicos y autogratificantes de información. La exposición de las personas se da dentro de un contexto de interacción semipúblico⁵ donde los sujetos interpretan su identidad a través de claves culturales que muestran características individualmente situadas. Los perfiles funcionan como guiones de texto que pueden en cualquier momento ser respondidos por alguien a través de solicitudes de amistad, comentarios en su estatus, etiquetas de fotos.

Decidir cómo manejar las solicitudes de amistad ha sido una piedra más en el camino de la identidad virtual; tiene que ver con la manera en que una persona espera ser percibido por los otros y con actuar según

⁵ Espacio destinado a los miembros de la red, hasta que empezó a funcionar Facebook Connect, volviendo pública la información que los usuarios no habían protegido manualmente en sus perfiles.

Ilustración 6. Foto con comentarios



Fuente: <https://bit.ly/2l3Nc3l>

las normas sociales que la red impone. Esta acción, en particular, ha vinculado el mundo virtual con el digital porque las personas enfrentan la posibilidad del rechazo. Las personas aceptadas aparecen automáticamente en la lista de amigos, por ello es fácil que alguien conozca que ha sido rechazado. No es posible inventar excusas, el propio artefacto se encarga de recordar las invitaciones pendientes cada vez que se ingresa a él. Por ello, muchos usuarios sienten la presión de aceptar personas que no quieren tener en su Social Graph, para evitar la presión de tener que enfrentar las consecuencias presenciales del rechazo.

Desde los inicios de la red, las fotos han sido uno de los componentes más potentes de los perfiles de los usuarios, ya que les permiten actualizar las representaciones del ser y el *performance* individual. La propia foto tiene propiedades conversacionales: quién la subió, quiénes están en ella, dónde, además del sistema de etiquetas y comentarios que la acompañan. Son parte de la estructura de participación del *software* social⁶ que reúne las distintas audiencias en un solo lugar y produce negociaciones de los límites sociales entre usuarios y artefactos (ilustración 6).

⁶ *Software social* es una categoría de los programas digitales; funciona principalmente para permitir la colaboración y la comunicación entre usuarios, como mensajes instantáneos, correo electrónico, wikis, servicios de redes sociales, <http://www.techopedia.com/definition/424/social-software>.

Timeline y las historias de vida

Te presentamos tu biografía.
Cuenta la historia de tu vida
con un nuevo perfil.

En octubre de 2011 Facebook lanzó una nueva característica de la red, denominada Timeline. Esta versión del antiguo perfil de los usuarios está diseñada para contar historias y mapear digitalmente todo lo que alguna vez se ha hecho. De una presentación más plana se pasa a un diseño interactivo, listo para que las personas lo llenen de contenido. Con Timeline y sus nuevas aplicaciones Open Graph fue posible añadir actividades a tus noticias sin tener nunca más que presionar OK. Además de naturalizar la exposición de la información, la idea fuerte detrás de Timeline fue conocer “cosas nuevas a través de los amigos”, esto es, generar flujos de información sobre tendencias, modas, intereses y, así, poder rastrear cada una de estas huellas de los perfiles digitales que se van alimentando con estas nuevas herramientas (ilustración 7).

Esta forma de representación del usuario favoreció el diálogo entre perfiles. En News Feed aparecía quién está escuchando qué música con Spotify, la foto tipo *vintage* que subió alguien más con Instagram, o el libro que se leyó en Goodreads. Desde hace años se ha dicho que los

Ilustración 7. Timeline



Fuente: <https://www.facebook.com/belen.albornoz>.

medios sociales giran alrededor de la conversación y Timeline potenciaba esta característica en el ámbito virtual. Las aplicaciones de Open Graph tenían una sola página que te ayudaba a “permitirlas” todas de golpe; a este nuevo sistema de autorización Zuckerberg lo llamó “Frictionless Experiences and Real-Time Serendipity” (Experiencias sin fricción y serendipia en tiempo real). Al ver que uno de tus amigos escuchaba una canción en tiempo real, podías escucharla con él, haciendo clic en *play* y esto era compartir con los amigos en un nuevo nivel. Los estilos de vida empiezan a volverse mucho más visibles desde qué comen y cómo lo preparan; un ejemplo de ello es Foodspotting.

Timeline dividió el espacio en tres niveles: la portada, tus historias y las aplicaciones. La portada mantenía la foto, pero añadía otra imagen como fondo. Facebook propuso subir la imagen que mejor te representara puesto que resaltaría tu perfil. Facebook definió “Tus historias” como “la biografía que puedes compartir y destacar en tus publicaciones, junto con fotos inolvidables, así como los acontecimientos importantes. Aquí puedes contar tu historia desde el principio hasta hoy mismo”. Y en “Tus aplicaciones” propuso ubicar las preferencias en cuanto a películas, canciones y actividades que te apasionan, un modo de expresarte tal como eres con las cosas que haces”.⁷

Esta nueva versión de Facebook reorganizaba las formas de representación de los sujetos y motivaba el intercambio de más información sobre sus estilos de vida. Ahora podían ver en directo qué cocinan sus amigos y compartir las recetas al instante, mirar el recorrido en el parque y los kilómetros que trotó su mejor amiga. Facebook apostó por incorporar el mundo físico a la pantalla, de forma más efectiva, a través de un clic. La representación estaba cada vez menos mediada por el texto y más por las aplicaciones que se comparten. Con ello se fueron incorporando capas de regulación sobre cómo habitar Facebook y naturalizar la exposición de la vida en detalle, en vivo y en directo. Con ello también se logró el uso indiscriminado de la información individual y de las trayectorias colectivas sin ninguna restricción.

⁷ “Timeline: Now Available Worldwide”, *Blog Facebook*, 15 de diciembre de 2011, <https://about.fb.com/news/2011/12/timeline-now-available-worldwide/>

Ahora todo el mundo se ha acostumbrado a estar conectado y esto no es tan interesante. Si yo tuviese que indicar por qué sitios como Facebook son tan populares diría que no se trata de la conectividad para nada. Es voyerismo y exhibicionismo. A las personas les gusta expresarse y tienen curiosidad sobre los otros [...]. Equivale a pasear por el centro comercial sin ningún propósito en particular y sirven para mirar y ser mirado. Estás con tus amigos pero también creas la posibilidad de encontrarte con alguien más. No se trata de hacer redes (que es la parte instrumental), ni siquiera de conseguir citas (que es mucho más específico), en realidad se trata de mezclarse con los otros.

Esto no significa que no sea una idea poderosa, dado el tiempo que le dedican los jóvenes a “estar” en el sitio... puede ser que sea el modelo de negocios que ahora se necesita (Duncan Watts, sociólogo de las redes sociales, citado por Cassidy 2006, en línea).

Desde sus inicios como Thefacebook, esta red otorgó a sus usuarios páginas en blanco para que las colorearan. Así, puso el peso en los sujetos, en su capacidad de producir contenidos; este artefacto sociotécnico perfeccionó, paulatinamente, mecanismos tecnológicos para que sus usos sociales se estructuraran cada vez en más ámbitos. Facebook ha ido construyendo su función simbólica, a través de la interacción con sus miembros; las formas de habitar la red han co-construido el artefacto retroalimentando a los escritores de código para moldear el sentido del artefacto y, con ello, permitir *performances* de identidad y negociaciones de estatus (Oudshoorn y Pinch 2005).

Los usuarios de Facebook han domesticado su tecnología mediante la apropiación, objetivándola, incorporándola y adecuándola a sus intereses (Silverstone 1992). Cada mes Facebook incorpora millones de usuarios que se adhieren a la red y se apropian de todas sus tecnologías. Al mismo tiempo los usuarios la objetivan otorgándole un lugar en sus vidas y hogares,⁸ un capital simbólico que les permite incorporarlas de forma situada a su cotidianidad. La domesticación de Facebook cierra su ciclo cuando moldea las relaciones de sus usuarios y del resto del mundo fuera de la economía moral del hogar. Ello se refleja no solo en su capacidad para atravesar esferas diferenciadas del mundo fuera de la

⁸ La convergencia tecnológica de *hardware* y de *software* potencia la objetivación de Facebook en el mundo.

pantalla, sino también en su posibilidad de ocupar la web sin las fronteras de la red social. Esta domesticación tecnológica me permite explicar cómo las acciones de los usuarios activan procesos multidinámicos de recolección de datos, de registro de acciones, de venta de información y de consumo de los estilos de vida, provocando nuevas normas sociales y nuevas capas técnicas del artefacto sociotécnico.

Es en esta co-construcción del artefacto sociotécnico donde la privacidad se cimienta sobre el fundamento de los datos personales. Una vez que el artefacto actúa regulando las conductas de los usuarios a través de su arquitectura, estos responden generando normas sociales que favorecen el principio de transparencia radical y nuevas formas de voyerismo. La división entre lo público y lo privado va adaptándose a aquella formulada en la capa tecnológica como el News Feed. Asimismo, los comportamientos de los usuarios se domestican a través de la sobreexposición y de la interacción. Como lo referí anteriormente, Hughes menciona que si no estás en Facebook, no tienes una identificación en línea y no puedes socializar con tus amigos; es imposible no estar ahí (Cassidy 2006, en línea).

Esta narrativa de lo inevitable es parte del proceso de domesticación de la privacidad, *si quieres seguir a tus amigos debes entrar a Facebook*. Esto cambia el modo en que las personas aprenden a lidiar con la privacidad, especialmente de los más jóvenes, que desarrollan un sentido de lo privado en medios digitales ubicuos. Las normas sociales plantean el reto de pensar la privacidad no solo en términos individuales, propios de la versión liberal de la privacidad, sino en términos sociales, como el producto de la co-construcción de las prácticas, los códigos y las regulaciones. El artefacto sociotécnico se ha encargado de cambiar las expectativas de privacidad de sus usuarios, las ha vuelto inversamente proporcionales a la intensidad del despliegue tecnológico, pues a más tecnología menor privacidad (Poulet y Rouvroy 2009).

Dossiers digitales

Timeline sofisticó el modo de recolectar la información de los perfiles de forma cronológica y mejor compartimentada, ayudando a los usuarios a organizar mejor los datos que le entregan a la compañía. Lo que no era

evidente es que todas las acciones de las personas en Facebook producen valor para la compañía y para los ‘terceros’ operando dentro de la red social. “Los mercados laborales se han desplazado a lugares donde el trabajo no es visto del todo como trabajo” (Scholz 2010, 242).

Los usuarios de Facebook no solo interactúan lúdicamente, también participan con sus datos en el surgimiento y desarrollo de grandes negocios alrededor de su actividad social virtual, al entregar información valiosa a los auspiciantes, redes de datos, investigadores y publicistas. Los perfiles funcionan como grandes pancartas en las estrategias publicitarias sin que apenas sus dueños se den cuenta, sirviendo, sin sentido de participación, a un plan de negocios del que están excluidos económicamente. Se mercadea con los estilos de vida, con las preferencias, con las modas que la socialización virtual transporta, produciendo *dossiers* digitales a través de la agregación de los datos que los usuarios entregan. News Feed, Facebook Connect, Timeline han sido tan solo los primeros componentes que interrelacionan la información de los miembros de la red y la potencian para que sea utilizada por la industria. Estos elementos permiten construir patrones de comportamiento y de tendencias que derivan en teorías sobre el consumo y la predicción de comportamientos.

Timeline es la cúspide de las autobiografías, ya no hace falta que las compañías realicen análisis inferenciales de las conductas de los sujetos en línea para conocer sus preferencias de consumo, como cuáles son sus restaurantes favoritos, en qué aerolíneas viajan, los libros que leen; ahora solo tienen que contratar con Facebook el acceso a las bases de datos que la compañía tiene de más de 1000 millones de personas en el mundo. Bases de datos alimentadas lúdicamente por los usuarios que han crecido con Napster y con iPod dentro del fenómeno del *peer production* o el *me media*. Al fin se ha logrado el modelo de publicidad que Sandberg pretendió crear con su ingreso a Facebook: “Te odio Facebook, no puedo parar” (Cassidy 2006, en línea).

SECCIÓN 3
LA PRIVACIDAD
EN FACEBOOK

Capítulo 7

La construcción de la privacidad en Facebook

Los juegos de simulación no son objetos para pensar sobre el mundo real sino para provocar nuestra reflexión sobre cómo el mundo real se ha convertido en sí mismo en un juego de simulación.
—Paul Starr

La vida simulada tiene dimensiones éticas, políticas y artísticas; vehicula nuevos diseños epistemológicos, ofrece paradojas como que lo virtual parezca, a veces, más real que la realidad. Turkle (2009, 5) analiza los problemas de la simulación a partir de los descontentos que esta genera algo particularmente útil para entender los fastidios de los usuarios frente a Facebook cuando el mundo simulado afecta sus nociones de privacidad. Si somos capaces de analizar los procesos de simulación a través de los descontentos que ocasiona, podremos descubrir problemas más profundos.

La simulación demanda un mundo paralelo lleno de posibilidades en el que la gente debe sumergirse. La inmersión, sin embargo, no es gratuita; conlleva un estadio de vulnerabilidad del cual no es consciente el individuo: la simulación hace más fácil amar y difícil dudar de la realidad virtual. Algo importante se escapa de los mundos simulados porque es difícil recordar todo lo que dejan afuera, todo lo que no han capturado de lo real. De algún modo construimos la tecnología y la tecnología nos construye. Como Churchill un día dijo: “Nosotros hacemos nuestros edificios y, más tarde, ellos nos hacen a nosotros, ellos regulan el curso de nuestras vidas” (Turkle 2009, 9). Convivir con la tecnología implica vivir en la tensión de usarla y de recordar desconfiar de ella.

Cuando en 2006 Facebook introdujo News Feed y, en 2007, Beacon, en 2009, los cambios en sus condiciones de servicio y la configuración “todos”, los usuarios empezaron a descubrir su fragilidad dentro de la red social y la del sistema de confianza que se había establecido con el artefacto sociotécnico. Facebook como espacio simulado ofrece mundos preconstruidos donde la configuración de la realidad virtual impide dejar entrar otras posibilidades presentes en la vida real a los mundos virtuales: las herramientas de configuración de Facebook, por ejemplo, solo permiten el tipo de relacionamiento social que el espacio virtual ha diseñado, dejando afuera la diversidad de formas de socializar que existen más allá de la pantalla, usando herramientas opacas que impiden cualquier tipo de verificación (los Términos de Privacidad que cambian sin aviso al usuario, los controles de la configuración de la privacidad se presentan como herramientas de control de información, cuando en realidad obtienen una mayor cesión del control del usuario a la red social). La trampa de la simulación es la necesidad de confiar en ella, lo que significa que hay que fiarse de las personas que diseñaron esos mundos virtuales. Los procesos de simulación se convierten, de este modo, en “cajas negras”¹ donde la representación adquiere un estatus de autoridad² (Turkle 2009, 29).

Timeline y sus aplicaciones Open Graph son tecnologías autoritarias pero con gran capacidad de seducción. Esta seducción cada vez más *sexy* oscurece los modelos que utiliza la tecnología para limitar las interacciones y las constantes cesiones a la privacidad. La cesión de la autoridad del sujeto a la simulación significa la aceptación de la opacidad del medio, ningún usuario se pregunta hasta dónde está cediendo su privacidad por seguir las reglas del juego, del mismo modo que los sujetos adhieren a las condiciones políticas y a las estructuras del mundo real (Starr 1994).

¹ Término usado por los ingenieros para describir algo que ya no está abierto al entendimiento; al tiempo que las técnicas se estabilizan, ellas mismas se convierten en cajas negras (Turkle 2009, 33-63). Los científicos jóvenes se sienten muy cómodos con las simulaciones basadas en las cajas negras porque crecieron con los juegos de computadoras que ofrecen interactividad sin transparencia.

² Al introducir computadoras y *software* en el proceso de enseñanza en varios departamentos del Massachusetts Institute of Technology (MIT), las facultades se preocupaban de la facilidad con la que los estudiantes, que en un momento determinado comprendían la diferencia entre representación y realidad, una vez dentro de los mundos simulados perdían tal claridad. El debate entre demostración y simulación se centraba en el riesgo de que los alumnos que se dedicaban a realizar experimentos simulados se acostumbraran a mirar la naturaleza en representaciones que ellos no podían entender del todo –la simulación deja afuera gran parte de lo real– (Turkle 2009, 40).

En tal sentido, la privacidad tiene una doble problemática: la convergencia tecnológica y la convergencia social. Por una parte, vemos cómo Facebook ha estructurado una plataforma en la que convergen múltiples tecnologías y todo tipo de pantallas de simulación; pero, por la otra provoca el colapso de los aspectos de las identidades de los sujetos, reservados para grupos particulares en un solo contexto donde todas estas barreras se sobreponen unas sobre otras, lo que impide diferenciar –como en la vida fuera de la red– a los amigos de los conocidos o de los compañeros de trabajo.

Uno de los problemas que los usuarios de Facebook reconocen con respecto a la privacidad no es solo la dificultad de intentar levantar muros entre contextos sociales diferenciados, y poder ejercer en su sociabilidad virtual de modo similar a como se hace fuera de la pantalla. El modo en que las personas se comportan está mediado por las normas sociales que rigen contextos específicos. La convergencia social exige a las personas que se manejen en público, ante audiencias simultáneas, sin tener un guion; con este tipo de convergencia, el sentido de control se diluye.

El problema en realidad tiene que ver con el control sobre las acciones de los usuarios, la materialización de estas en datos, el contexto en que las acciones tienen lugar y la audiencia a la que están dirigidas. “La información no es privada porque nadie sabe, es privada porque ese saber es limitado y controlado” (boyd 2008a, 18). La privacidad, más allá de ser considerada un derecho, es un privilegio que se mantiene mientras existan estructuras tecnológicas y sociales que la protejan. Cuando Facebook lanzó News Feed, alteró la estructura de la socialización de sus miembros; así, los usuarios debieron aprender a desarrollar habilidades para comportarse en un espacio de convergencia social, renunciar a sus expectativas de privacidad, convivir con la idea de que Facebook ya no era el espacio público construido entre amigos y naturalizar la exposición que preforman ante los otros. Conforme avanzaba la aplicación del principio de transparencia radical más difícil se volvió, para los usuarios, reclamar privacidad en medio del “trance”³ vivido dentro de Facebook. “Si quieres mantener algo privado, no lo saques de tu cabeza” (Moskovitz, citado por Kirkpatrick 2010).

³ “Trance” es el término que acuñaron Zuckerberg, Parker y Moskovitz para describir la experiencia hipnótica que viven las personas que utilizan el sitio cuando empiezan a recorrer la información que circula en él.

Organizaciones dedicadas a mantener la privacidad

TRUSTe

TRUSTe es un proveedor de soluciones de privacidad en línea, con un amplio abanico de servicios para las empresas. Ayuda a construir un sistema de confianza entre los clientes y las compañías, con el fin de aumentar su fidelidad a través de varios canales en línea: aplicaciones de telefonía móvil, sitios web, publicidad y servicios de nube. Además, realiza análisis de empresas y mercadotecnia por correo electrónico. Se basa en valores como la transparencia, la opción y la confianza en la recolección y uso de datos personales. Su misión es construir políticas de privacidad, noticias y opciones con mayor transparencia, de modo que sean más fáciles y asequibles para el entendimiento de los usuarios; provee opciones y control a los consumidores sobre el uso de su información personal, al igual que ayuda, a las compañías y organizaciones, a lograr la confianza en las obligaciones de privacidad que hacen a sus consumidores.

En los inicios de Facebook, trabajaba para más de 5000 empresas en línea, entre las que se cuentan Apple, AT&T, Disney, eBay, Microsoft y, por supuesto, Facebook. Entre sus servicios está el TRUSTe Privacy Seal, que le otorgó a Facebook una vez que verificó que su política de privacidad cumplía con los requisitos del programa TRUSTe. En su sitio web, Facebook indicó “[e]sta política de privacidad se aplica al sitio web www.facebook.com. El programa TRUSTe solo incluye información recopilada a través de este sitio web, y no otros datos, como información que pudiera recopilarse a través de *software* descargado por Facebook”.

Dentro de la estructura de Facebook, TRUSTe fue como una consultora que le asesoraba en el andamiaje legal a desarrollar para proteger a la empresa y como evaluadora de los procesos que debían cumplir para certificarse como una institución respetuosa del derecho de privacidad de sus usuarios.

Electronic Privacy Information Center, EPIC

EPIC es un centro de investigación de interés público ubicado en Washington D. C. Inició su trabajo en 1994 para proteger la privacidad y las libertades civiles. El centro publica informes, libros y declaraciones

gubernamentales sobre privacidad. Se trata de una organización no gubernamental que se precia de no tener clientes, consumidores o inversionistas. Entre los temas más importantes que convocan a EPIC tenemos *Patriot Act*, la privacidad en línea de los niños, Facebook, la directiva de la Unión Europea de protección de datos, Google Street View, privacidad situada, privacidad y récords médicos, privacidad en redes sociales, privacidad de los estudiantes, entre otras.

EPIC se ha preocupado de las redes sociales, en general, porque ha detectado que mucha de la información que los usuarios han publicado, con la intención de que sea vista por sus amigos, ha terminado en manos de las autoridades, de extraños, de la prensa y, en general, de públicos a los que no fue originalmente destinada, como jefes o reclutadores de trabajo. Aunque Facebook tiene más controles de privacidad que otras redes sociales, mantiene los perfiles de sus usuarios expuestos a la búsqueda de cualquiera; Facebook requiere, así, que los propios usuarios definan quién puede o no ver su información.

Sin embargo, desde el año 2006 Facebook hizo una serie de cambios en su política de privacidad que han requerido una respuesta por parte de la sociedad civil. Ello motivó a que EPIC realizara dos demandas ante la Comisión Federal de Comercio (FTC, por su sigla en inglés) sobre las prácticas injustas de intercambio de información de los usuarios con terceros, como los desarrolladores de aplicaciones. La primera demanda “In re Facebook” se realizó el 17 de diciembre de 2009, con un complemento el 14 de enero de 2010. Esta demanda sostuvo que Facebook obliga a sus usuarios a volver pública aquella información que, previamente, había sido protegida, lo que en sí mismo es una práctica injusta. También se reclamó que los códigos de personalización instantánea son confusos y engañosos y que no informan adecuadamente a los usuarios sobre las *cookies* que utiliza Facebook para rastrear la actividad de sus usuarios en internet. Finalmente sostuvo que la decisión de Facebook de permitir que los desarrolladores de aplicaciones mantengan la información de los usuarios, de forma indefinida, contradice lo que garantiza a sus usuarios en sus políticas. La segunda demanda contra Facebook se presentó el 5 de mayo de 2010 y se centró en las prácticas de entrega de información de los usuarios a terceros.

Luego de la segunda demanda a Facebook y de la fuerte crítica pública que recibieron sus políticas de privacidad, esta compañía volvió

a cambiar sus políticas en mayo de 2010. Entonces otorgó al usuario mayor control sobre su información personal, incluida la información básica (lista de amigos, educación, trabajo, ciudad, páginas de interés) y también sobre su biografía, estatus, comentarios, puntos de vista políticos y religiosos, relaciones, cumpleaños, correo electrónico, número de teléfono y dirección. Facebook permitió a los usuarios salir de aplicaciones, juegos y sitios web de terceros ayudando a prevenir que ellos tengan acceso a su información personal. Sin embargo, en la opción de búsqueda pública, los usuarios debían optar con el sistema *opt-out*, al exponer su información personal en las plataformas de aplicaciones, juegos y sitios web. No ha cambiado el que los desarrolladores puedan usar la información de los usuarios de forma indefinida, tampoco ha transparentado su política de *cookies*, lo que destruye la posibilidad de los usuarios de navegar en la web de manera anónima. Ello mantiene el hecho de que la información que, en principio, fue protegida, siga expuesta a terceros, de forma masiva e indefinida.

A EPIC le preocupa particularmente las políticas de privacidad de los sitios web y de las redes sociales, porque son instrumentos que difícilmente le permiten al usuario tomar decisiones. Son muy difíciles de leer y entender, y aunque su lectura es parte del proceso de registro, muchas veces no se presentan de forma específica en el formato de registro y apenas son mencionadas en los términos del servicio. Otro problema es que las políticas pueden cambiar de forma unilateral, transformando la relación entre el sitio y el usuario, sin que este último tenga voz o voto, al igual que puede cambiar la arquitectura del sitio y las preferencias de los usuarios.

Tal fue el caso de Facebook, que cambió la configuración automática que originalmente era privada (destinada a la red de amigos) a “todos”, volviendo la información pública por *default*. Facebook utiliza los servicios del programa de privacidad de TRUSTe y paga para tener su licencia. Sin embargo, el programa para EPIC tiene muchas fallas y no ha castigado a las compañías a quienes les ha otorgado su licencia cuando estas han comprometido la privacidad de sus consumidores.

En general, las políticas de privacidad deberían ser fáciles de leer y de seguir. En el caso de Facebook, los usuarios tienen una serie de referencias cruzadas entre el texto legal y los controles de privacidad que vuelven muy complejo definir qué mantener protegido de los públicos no deseados.

La trayectoria de la privacidad en Facebook

Una de las críticas más importantes que han tenido los análisis de la privacidad en Facebook es que se caracterizan por trabajar sobre una privacidad fetichista. Hay que tener en cuenta que la información y la comunicación no son las únicas dimensiones de la privacidad. De hecho, la privacidad informacional es uno de cuatro tipos de privacidad (Tavani 2008, 2010); las otras son privacidad fundada en la accesibilidad física, la privacidad decisional y la privacidad psicológica o mental. Del mismo modo, Solove (2008) propone que la comunicación es uno más de los contextos de la privacidad, además del hogar, la familia, el cuerpo y la sexualidad.

En el contexto virtual de Facebook, el acceso a las personas se extiende de los espacios físicos a los de información; crea una relación entre la privacidad informacional y la basada en el acceso. Así se hace necesario distinguir las tres teorías de la privacidad que pueden ayudar a estructurar el marco tecnológico de Facebook desde la voz de los grupos sociales relevantes.

La teoría del acceso restringido en la privacidad informacional está dirigida a terceros, el “derecho a ser dejado en paz” es la base doctrinal de dicha teoría. Además de basarse en la propuesta de Warren y Brandeis del derecho a la privacidad, está ligada al pensamiento liberal del estereotipo del propietario (Bloustein 1964; Rule 2007; Schoeman 1984; Solove 2008), por lo que es altamente individualista, centrada en el sujeto y sus libertades. En tal sentido, la noción del secreto es fundamental en esta teoría (Solove 2008), pues contribuye a separar la esfera pública de la privada. La privacidad es un valor antagónico que funciona universalmente para proteger la propiedad privada y, en términos individuales, para resguardar al individuo dentro de los muros del hogar.

La teoría del control de la privacidad la entiende como el dominio de la autodeterminación informacional (Westin 1984; Withman 2004). En dicha teoría, el control de la privacidad se mantiene incluso si las personas voluntariamente difunden información sobre sí mismas. El secreto no es parte fundamental de esta propuesta y el énfasis recae en la importancia de la autodeterminación para compartir información en contextos diferenciados. El capitalismo necesita del anonimato y la privacidad para funcionar, sobre todo en el ámbito financiero; cuánto gana una persona es considerado un tema privado en muchas sociedades

contemporáneas pero, al mismo tiempo, la construcción de la confianza dentro del sistema requiere que los usuarios compartan datos entre ellos. De esta manera se crean instrumentos de control para autenticar a quienes se puede confiar la información. Así, esta tensión entre protección de la privacidad y la vigilancia es propia del capitalismo (Fuchs 2011).

La teoría del acceso restringido y control limitado combina las dos anteriores, pues concibe la privacidad en función del acceso restringido, pero basa su manejo en el control limitado que tienen los sujetos de su información. La privacidad como un derecho colectivo es fundamental para proteger a las personas de la dominación de las grandes corporaciones que acumulan capital a través de la recolección de información de extensos grupos de individuos y de consumidores (Fuchs 2011).

Fetichismo de la privacidad en Facebook

Las teorías liberales constantemente apelan al valor de la privacidad para los seres humanos y su relevancia antropológica en cuanto a integridad, amor, tolerancia, personalidad, confianza o dignidad (Schoeman 1984). Sin embargo, no enfrentan el reto de analizar el rol particular que juega la privacidad en la sociedad capitalista. La asociación a los valores positivos universales recoge poco los efectos negativos de la privacidad y la relación entre la concepción moderna de esta y la propiedad privada (Fuchs 2011).

Marx caracterizaba la aparición de la “relación social definitiva entre los hombres” como “una forma fantástica de la relación entre las cosas” y como pensamiento fetichista (*El capital*, citado por Fuchs 2011, 145). El fetichismo confunde el fenómeno creado por los seres humanos, que tiene un carácter social e histórico, como algo natural que ha existido siempre en todas las sociedades. Fenómenos como la mercancía son declarados verdades sempiternas. Las teorías de la privacidad que no consideran la dimensión histórica, no toman en cuenta la relación entre privacidad y capitalismo y pueden ser caracterizadas como privacidad fetichista. En contraste con esta, Moore (1984) propone la privacidad como una “necesidad creada” que varía históricamente. El deseo de privacidad se desarrolla en las sociedades que tienen una esfera pública caracterizada por complejas relaciones sociales que son consideradas peligrosas.

Una forma específica de fetichismo se encuentra en las investigaciones acerca de la privacidad en Facebook y en las redes sociales en general, las cuales se enfocan en la difusión de la información (Acquisti y Gross 2006; Barnes 2006; Dwyer, Hiltz y Passerini 2007). Dichos estudios consideran que la privacidad está en riesgo porque se muestra demasiada información sobre los sujetos y con ello se vuelven blanco de la vigilancia y del crimen. La privacidad es entonces concebida como un fenómeno que depende del comportamiento de los individuos y de cuánto revelan sobre sí mismos; concluyen con una condena moral a la exposición pública de los datos personales. La privacidad es pensada, así, desde un discurso de victimización, donde los responsables son los sujetos que no se informan adecuadamente de las plataformas donde exponen sus datos, de sus prácticas de revelación de información personal y de la falta de uso de los mecanismos de control de sus datos, que ofrecen las plataformas tecnológicas. Las tecnologías, en este mismo sentido, se consideran negativas y peligrosas para la seguridad individual y colectiva.

Los temas relacionados con la economía política de Facebook son ignorados, como la publicidad y la acumulación de capital, la apropiación de los datos de los perfiles con fines comerciales o la explotación de los usuarios. Los teóricos críticos, en cambio, no condenan moralmente a los usuarios por subir datos a plataformas como las redes sociales, porque comprenden que dentro del sistema capitalista hay formas de afirmación del ser que condicionan tipos de comportamiento. Marx posicionaba la privacidad en relación con la propiedad privada. Para él, el concepto liberal del sujeto privado y de la privacidad conciben a la persona como un sujeto aislado, retraído sobre sí mismo. Arendt ([1958] 2005)⁴ considera este tipo de privacidad, una privacidad de la ausencia de los otros y de la carencia de relaciones sociales. Mientras el pensamiento liberal coloca al individuo como antecedente a la sociedad, y a la privacidad como un valor del individuo; una aproximación más pragmática resalta la relación

⁴ “Una vida enteramente privada significaba, por sobre todo, la privación de las cosas esenciales a una verdadera vida humana: de la realidad que se deriva de ser visto y escuchado por otros [...] de la posibilidad de alcanzar algo más permanente que la vida misma. [...] El hombre que vivía solo una vida privada, que como los esclavos no estaba autorizado a entrar en la arena de lo público, o como los bárbaros había escogido no establecer tal arena, no era completamente humano. Ya no pensamos más en privación cuando usamos la palabra ‘privado’, y esto es gracias al enorme enriquecimiento de la esfera privada a través del individualismo moderno” (Arendt [1958] 2005, 38-58).

del individuo con la sociedad, y se rehúsa a aceptar el derecho a la privacidad como un derecho individualista, sino como uno constitutivo de la sociedad (Cohen 2000; Dewey 1936; Schwartz 1999).

Privacidad y economía política en Facebook

Para analizar la privacidad en Facebook es relevante salir del encasillamiento de la privacidad como control y autodeterminación informacional e incluir las estructuras de propiedad de los datos personales dentro de la economía política de la red social. A pesar de la inicial retórica de Zuckerberg de crear una nueva forma de socialización basada en la interacción de los sujetos, sin que ello necesariamente implique la monetización de sus datos, vemos que Facebook se fue consolidando con los años en una empresa capitalista que generó nuevos modelos de negocios, de dominación en la interacción social y del flujo de la información en la web, en amplia competencia con el modelo de Google. Facebook ha generado un entorno ideal para la publicidad dirigida a través de la vigilancia de las acciones de los usuarios, la traducción de las acciones en datos, su sistematización, la creación de bases de datos, la apropiación del contenido de sus usuarios a través de licencias PI y la venta de la información a terceros. Ello implica una vigilancia de dos vías, la dirigida a cada usuario para ver las tendencias que va adquiriendo en su socialización en línea y la colectiva, destinada a agrupar a los miembros en grupos que comparten comportamientos en línea y el valor derivado⁵ que produce el Social Graph. Para entender la economía política de Facebook es necesario revisar su marco político-legal dentro de su modelo de acumulación.

Los Términos de Privacidad de Facebook corresponden a los clásicos parámetros norteamericanos de protección de datos basados en la autorregulación de las empresas y en sintonía con un sistema legal nacional que protege los datos personales recolectados por el Estado, pero que regula menos los acopiados por las empresas para favorecer sus modelos de negocios (Rule 2007). Puesto que como hemos visto, el Estado se considera la primera amenaza a la privacidad en los Estados Unidos, el

⁵ La reorganización de la audiencia en términos demográficos produce un superávit del valor informacional de cada miembro de Facebook que se utiliza en la publicidad dirigida.

mercado obtiene una gobernanza más flexible. El segundo punto que es necesario revisar es la trayectoria de regulación de las políticas comerciales de los sitios de internet, que usualmente están escritas en un lenguaje inteligible, pero que asegura, en sus primeros párrafos, el interés de las compañías en proteger la privacidad de sus clientes/usuarios cuyo objetivo es enmascarar las prácticas de venta de sus datos personales (Turow 2003). En la introducción a su política de privacidad, Facebook asegura a los usuarios que

ha sido diseñado para que te resulte sencillo compartir información con quien tú quieras. Tú decides cuánta información deseas compartir en Facebook, y tú controlas su distribución a través de tu *configuración de privacidad*. Debes comprobar la *configuración de privacidad* predeterminada y cambiarla si es necesario para adaptarla a tus preferencias. También debes tener en cuenta esta configuración siempre que compartas información.⁶

No emplea una nomenclatura explícita para indicar a los usuarios que venderá sus datos personales o que utilizará información que han catalogado como privada (como fecha de nacimiento, entre otras). Ello se utilizará con fines comerciales para rastrear trayectorias de consumo y comportamiento en la red; no obstante, utiliza eufemismos como “compartir información con terceros”.

Información que compartes con terceros

Para ofrecerte anuncios personalizados. No compartimos información tuya con anunciantes sin tu consentimiento. (Un ejemplo de consentimiento sería que nos pidieses que suministrásemos tu dirección de envío a un anunciante para recibir una muestra gratuita.) Permitimos a anunciantes elegir las características de los usuarios que verán sus anuncios y podemos utilizar cualquiera de los atributos que hayamos recabado que no te identifiquen personalmente (como información que puedas haber decidido no mostrar a otros usuarios, por ejemplo, el año de nacimiento) para seleccionar el público apropiado para dichos anuncios. Por ejemplo, podríamos utilizar tu interés por el fútbol para mostrarte anuncios de equipamiento de fútbol, pero no le decimos a la empresa

⁶ “Herramientas para ayudarte a controlar tu privacidad y seguridad en Facebook”, www.facebook.com/privacy/

que vende el equipamiento quién eres. Puedes consultar los criterios que pueden seleccionar los anunciantes visitando nuestra *página de publicidad*. Aunque no compartimos tu información con anunciantes sin tu consentimiento, cuando hagas clic en un anuncio o interactúes de otro modo con este, existe la posibilidad de que el anunciante pueda colocar una *cookie* en tu navegador y tomar nota de que cumple los criterios que ha seleccionado.

Para ofrecer anuncios sociales. En ocasiones, emparejamos los anuncios que ofrecemos con información pertinente que poseemos sobre ti y sobre tus amigos para que los anuncios resulten más interesantes y se adapten mejor a ti y a tus amigos. Por ejemplo, si te haces admirador de una página, podemos mostrar tu nombre y la foto de tu perfil al lado de un anuncio de dicha página que verán tus amigos. Solo compartimos la información personal visible en el anuncio social con el amigo que puede ver el anuncio. Puedes optar porque tu información no sea utilizada en anuncios sociales en esta *página de ayuda*.⁷

Así, las políticas de privacidad desde los inicios de Facebook asumen que es razonable realizar publicidad dirigida y que los usuarios están, en principio, de acuerdo. Aunque aclara que no compartirá información de sus usuarios sin su consentimiento, dentro de la estructura del diseño de la red la publicidad dirigida está activada automáticamente, sin que los usuarios tengan una opción de negarse a dar su consentimiento. Una vez que aceptan los Términos de Privacidad, también admiten que los contenidos con los que se describen, aquellos que comparten con sus amigos, incluso aquella información que sus conocidos suben sobre ellos podrán ser vendidos a todo aquel que desee comprarlos. De este modo, Facebook obliga a sus miembros a someterse a unas reglas de juego donde nunca se les pregunta si están de acuerdo en que sus datos sean vendidos a anunciantes, por lo cual es muy difícil afirmar que el usuario tenga derecho a “consentir o no” el uso de su información. Al igual que utiliza el término “compartir información con terceros”, en vez de venta de datos personales, también recurre al “consentimiento de uso” para invisibilizar la monetización de la información subida a la red por los usuarios.

⁷ Herramientas para ayudarte a controlar tu privacidad y seguridad en Facebook”, www.facebook.com/privacy/

Las políticas de privacidad demuestran que este instrumento de autorregulación de la red social instala un régimen de capital que subsume la vigilancia que Facebook realiza de sus usuarios, mercantilizando los contenidos que producen. Facebook utiliza un lenguaje amigable de sociabilidad en línea para describir prácticas comerciales, fruto de la interacción social de los miembros de la red, y enmascara que no solicita, en la práctica, el consentimiento de sus usuarios para utilizar los datos que producen. Las políticas de privacidad tienen un doble nivel de funcionamiento: el texto legal y el código informático que ordena los comportamientos sociales. El consentimiento del usuario tiene un plano discursivo en la política y un plano restrictivo en la arquitectura de Facebook. Retóricamente se busca el consentimiento del usuario, pero se lo niega en la práctica. “Así, las regulaciones y las tecnologías tienen una relación estrecha en relación al control social” (Vercelli y Thomas 2008, 21). La privacidad en Facebook monetiza los datos sobre el comportamiento de sus miembros dentro de la red y en otros sitios web. En primer lugar, mercantiliza a sus usuarios en las plataformas corporativas de operadores que venden publicidad a sus clientes y esto conlleva una lógica de comercialización mediante la exposición del sujeto. Por tanto, los usuarios son considerados mercancías en permanente exposición en línea, a través de la publicidad (Fuchs 2011).

El proceso de monetización y de acumulación de capital de Facebook, según Fuchs (2011, 155-6), obedece a un modelo donde los usuarios son excluidos de la rentabilidad que genera la comercialización de la información subida a este artefacto. Así:

M = Facebook invierte dinero en comprar capital: tecnología y mano de obra pagada (estas son las variables constantes de gastos de capital). Los empleados, que crean el entorno virtual al que acceden los usuarios de Facebook, producen parte del valor de superávit. Los usuarios generan contenido que suben a la plataforma cuando la utilizan, producen información de forma individual y colectiva a través de su interacción social. Facebook vende esta información como mercancía a los anunciantes de publicidad, a un valor mayor que el invertido en las variables constantes de capital. El valor de superávit contenido en la mercancía es parcialmente creado por los usuarios y, en parte, por los empleados de

Facebook. La diferencia es que los usuarios no son pagados y, por ende, son infinitamente explotados.

$$M - C \quad \begin{array}{l} C \text{ (tecnología, infraestructura)} \\ \dots P.C' - M' \\ V \text{ (empleados, usuarios = 0)} \end{array}$$

C' = mercancías producidas por los usuarios productores de información y consumidores de contenidos publicitarios, transacción de datos y tiempo y espacio de publicidad.

De esta manera, Facebook monitorea toda la información y la actividad que producen sus miembros, nada queda escondido ante la vigilancia de la empresa. Los usuarios no saben cómo Facebook usa sus datos, a quiénes se los vende, cuánto gana con ellos. Así la principal forma de privacidad de Facebook es la opacidad de la apropiación de los datos de los usuarios. La relación público-privado tiene otra dimensión en Facebook ya que todo aquello que es producido y preformado, privadamente, es mercantilizado. Facebook comercializa los datos privados de sus usuarios y, así, acumula capital para la empresa; como resultado, los usuarios son excluidos de cualquier tipo de ingresos o de compensación monetaria por la creación del superávit de valor que producen. La vigilancia informática de Facebook tiene propósitos económicos y promueve una relación compleja entre diversión y trabajo, mientras más largo es el “trance” de los usuarios en Facebook más valor generan para la empresa.

Capítulo 8

La privacidad desde una mirada sociotécnica

La privacidad ha muerto, asúmanlo.
—Scott McNealy, CEO de Sun Microsystems,
citado por Matt Hamblen, 2001

Desde su inicio, el asunto de la privacidad tuvo un papel muy importante en esta red social. Para Chris Kelly (2009), el director de privacidad de Facebook, “si tienes dudas de con quién te estás comunicando en internet, tu privacidad está en riesgo; pero si sabes con quién te estás comunicando puedes, autoritariamente, determinar quién no puede ver tu información”. La privacidad puede ser protegida a través de la infraestructura de amigos que otorga una identidad genuina. En Facebook, el anonimato no funciona porque son los amigos quienes validan la identidad de las personas y para lograr un proceso de validación circular es necesario armar perfiles con los nombres verdaderos. Para Kelly, Facebook es una plataforma que privilegia la vida de las personas, y es mucho más que una nueva forma de comunicación, como lo fueron los mensajes instantáneos, el correo electrónico, el teléfono o el telégrafo.

La red social desarrolla tres instrumentos para guiar el uso de Facebook: los Términos del Servicio (más tarde denominados Declaración de Derechos y Responsabilidades), que consisten en un requisito para todos los usuarios de Facebook; los principios, que es la base jurídica de la plataforma; y las políticas, que es el texto jurídico de la plataforma.

Principios

Crea una experiencia positiva para todos los usuarios

- Crea aplicaciones sociales e interactivas.
- Ofrece a los usuarios la posibilidad de controlar el contenido y tomar sus propias decisiones.

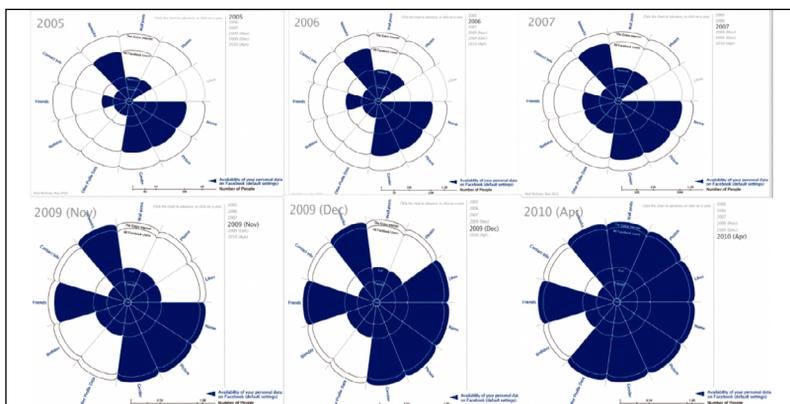
- Ayuda a los usuarios a compartir contenido relevante y comunicativo.
- Haz que todos puedan confiar en ti.
- Respeta la privacidad.
- No engañes, confundas, defraudes ni sorprendas a los usuarios.
- No envíes correo basura y fomenta la comunicación genuina.

En la construcción de Facebook, la transparencia es una noción que atraviesa el proyecto en todas las dimensiones que demanda de sus miembros; el “efecto Facebook” ha logrado incrementar la vida pública y la exhibición de las personas, así muchos la ven como una plataforma que fomenta el narcisismo. Zuckerberg, Moskovitz y Hughes han añadido “transparencia al mundo a través del acceso y el intercambio de la información” (Kirkpatrick 2010, 14). Según ellos, esta transparencia era capaz de transformar el funcionamiento del mundo y cómo las instituciones son gobernadas. Este modelo de relacionamiento social se basa en la voluntad de las personas y en su capacidad de tomar decisiones –la primera, aceptar las solicitudes de amistad–, obligándose a un flujo de intercambios voluntarios de información con otros usuarios.

Se trata de un código que se centra en la voluntad de las personas de aceptar a sus amigos. Al tratarse de una cadena de confianza que funciona para entregar información personal era preciso encontrar un mecanismo que sostuviera este esquema: dejar que los usuarios armaran sus propias redes y siguieran validando la información de sus amigos. La edad mínima de ingreso son los trece años; en abril de 2006 ya contaba con un millón de estudiantes de colegio secundario. Las opciones de privacidad determinan quién puede acceder a la información y se diferencia de otras redes sociales como Friendster y MySpace porque controla, rigurosamente, quién accede a qué información.

En Facebook constantemente mostramos información que es utilizada en los “sistemas de confianza” que procesan dichos datos. Son justamente estos sistemas de confianza los encargados de recolectar toda la información posible sobre nuestras preferencias, navegaciones, compras e intereses. Cada clic realizado materializa una huella que puede ser rastreada por esos sistemas. Este constante monitoreo, capaz de alimentar los perfiles digitales de los usuarios, debe ser cada vez más eficiente, pues ello implica

Gráfico 5. Exposición de la información de los usuarios: 2005-2010



Fuente: Matt McKeon, en <http://mattmckeeon.com/facebook-privacy/>.

recolectar más información para venderla a las compañías que hacen negocios con Facebook. La falta de anonimato que los sistemas de confianza ocasionan tiene que ver con el derecho de las personas a no ser rastreadas sin su consentimiento. La libertad de contactar, navegar, leer o hablar en línea debería ser protegida legalmente (Cohen 2000; Lessig 2006; Solove 2004) porque es un elemento de libertad intelectual que estos sistemas anulan. El cambio tecnológico de sistemas analógicos a digitales afectó directamente la privacidad de las personas, pues la recolección de datos es un subproducto de la tecnología que se acciona cada vez que los usuarios dejan algún tipo de rastro en los sistemas digitales.

En el gráfico 5 muestran cómo Facebook modificó, paulatinamente, la exposición de la información de sus usuarios, gracias a dos estrategias: el cambio del diseño de su arquitectura través del código, y la redefinición de los Términos de Privacidad que firman sus usuarios.

Los cambios a la privacidad se generan en el código. Así, las tecnologías digitales han cambiado las expectativas de privacidad de la ciudadanía al transformar las protecciones establecidas. Ya no es posible mantener a otros fuera de nuestro espacio privado, puesto que se han perdido las barreras físicas que antes funcionaban y ha entrado en escena el oxímoron *privacidad en público*. Dentro del mundo virtual, en el momento en que actuamos en un lugar público perdemos la capacidad de controlar la

información que entregamos, podemos ser monitoreados pero también podemos dejar huellas. Una vez que ingresamos a los espacios públicos de los mundos virtuales, ya no solo somos vigilados, dejamos inscripciones cada vez que hacemos algo, huellas que pueden ser rastreadas y registradas. Generamos récords que pueden ser guardados por otros, por lo que el monitoreo para buscar datos se ha convertido en la arquitectura del espacio público tal como los semáforos en las calles. El problema con esta arquitectura es que casi nunca es obvio que otros estén registrando lo que hacemos, y que el uso de nuestras imágenes y palabras está totalmente fuera de nuestro control. Nuestras acciones se están archivando para siempre y podrán ser usadas en cualquier momento.

Paulatinamente, Facebook ha ofrecido plazas públicas, cuidadosamente diseñadas para que sean habitadas por sus usuarios. En todas, la consigna es compartir. El muro es la plaza personal de cada usuario, en él se publican desde los estados de ánimo, noticias, poemas, críticas, fotografías, hasta mensajes religiosos o políticos. Esta plaza está controlada por la persona usuaria, quien tiene el poder de la edición; si no le gusta algo que un amigo publicó en su muro puede borrarlo, puede hacer desaparecer todo aquello que le desagrada o que ya no le parece pertinente, pues su muro es parte de la imagen que desea proyectar. Cuando un amigo entra en su perfil además de la información personal lo primero que ve es el muro del usuario. Aquí también están presentes sus amigos, todo aquel que ingresa a esta página además del muro puede ver la lista de amigos de su amigo.

La segunda plaza pública es News Feed. En este espacio aparece el flujo de información que Facebook considera puede ser de su interés, a partir de lo que produce su Social Graph. Al lado del perfil hay un recuadro donde se puede encontrar a todos los amigos que están en línea, tiene la opción de chatear con ellos o de iniciar una videoconferencia con un sistema adaptado desde Skype. Este espacio promueve la interactividad por sobre todos los otros. Desde 2010, los usuarios necesitan entender mejor sus controles de configuración en la cuenta de Facebook, pues solo así son capaces de escoger quién puede aparecer en su muro o qué tipo de información prefieren que News Feed les entregue.

Dentro del perfil de cada usuario se encuentra una plaza más restringida. Esta es la que se encarga de convencerlo de que tiene el control sobre su información. En dicho espacio las personas deciden qué foto

colgar en su perfil, qué contarle a los otros, qué fotografías publicar y quién puede verlas (proceso que para cada foto o álbum tiene que hacerse manualmente, lo que hace que mucha gente ni siquiera se dé la molestia de configurar la privacidad de las imágenes). Este tercer nivel es el espacio de la representación, del yo virtual. Como mostraré más adelante, es aquí donde se juega gran parte de la sociabilidad de las personas usuarias. Por otro lado, Facebook ideó una forma de reunir a los amigos más allá de la marea de información que reparte, a través de intereses personales. Para ello creó los “grupos” que llevan al usuario a un nuevo lugar virtual donde se encuentra con otros que pueden estar o no en su Social Graph. El espacio de los grupos fue uno de los primeros en ser ocupado por las empresas con fines comerciales.¹ Finalmente tenemos los mensajes internos, los *inbox*, los únicos que como el chat pueden considerarse privados o fuera de la vista de los otros.

De los cinco niveles de intercambio de información, tan solo los mensajes privados pueden considerarse íntimos. Facebook ha diseñado una red que cumple su cometido: compartir, compartir y compartir. Se trata de una arquitectura que configura conductas, donde los usuarios “solo pueden hacer aquello que les es permitido”, pues todo lo que hacen es constantemente monitoreado. Moskovitz no solo estaba atento a los gustos de sus usuarios, también se fijaba detenidamente en sus comportamientos, porque los consideraba una fuente muy valiosa de insumos para el diseño de Facebook.

Para distinguir los niveles de cuán pública puede ser la información que se sube a la red social, Facebook propone alternativas como “todos”, “red”, “amigos de los amigos” y “amigos”. La categoría “todos” se traduce en que la información que se publica puede ser vista por cualquiera dentro y fuera de Facebook; la opción “red”² se establece por la ubicación geográfica de las personas y puede abarcar desde una ciudad hasta un país; “amigos de amigos” en cambio permite que los lazos débiles de los amigos tengan acceso a la información del usuario, lo cual amplía el

¹ Un lugar virtual equivalente a los grupos son las “Causas”. Pero no se distinguen en este texto de los grupos porque son parte de la misma arquitectura dentro de Facebook.

² Muchos usuarios encuentran confusa la noción de red en los controles de privacidad, pues tienden a confundir esta categoría con su red de amigos, cuando, al escogerla, lo que están haciendo es abrir su perfil para que desconocidos accedan a su información.

campo de publicidad de la información a desconocidos que son amigos de los amigos; en cambio, “amigos” le da acceso al Social Graph, a la información del usuario. Cada categoría en realidad es menos pública que las otras.

Desde que Facebook se inició en Boston, sus Términos de Privacidad han variado notablemente. De hecho, quienes adquirieron una cuenta en esa época firmaron unas condiciones que han cambiado de forma unilateral durante todos estos años sin que puedan hacer nada al respecto. Las redes sociales solicitan a las personas leer los términos del servicio, entenderlos y firmarlos para que puedan ingresar a la red. De hecho, consideran que no pueden obligar a sus usuarios a leer los términos ni a entenderlos. Pero resulta muy difícil para los usuarios mantenerse bien informados si los términos del servicio cambian con tanta frecuencia. No olvidemos que el porcentaje que lee dicha información es en realidad muy bajo (Cordova 2010). En sus políticas Facebook publica “podemos modificar estas Normas de la plataforma en cualquier momento y sin previo aviso si lo estimamos oportuno. El uso ininterrumpido por tu parte de la plataforma supondrá la aceptación de estas modificaciones”;³ y en sus avisos de cambio:

Si realizamos cambios en esta política de uso de datos, te lo notificaremos a través de la publicación en esta página y en la página Facebook Site Governance. Si los cambios son sustanciales, mostraremos un aviso prominente si las circunstancias lo requieren. Puedes asegurarte de recibir la notificación directamente si haces clic en el botón *Me gusta* de la página Facebook Site Governance.⁴

En enero de 2009, Facebook indicó que los usuarios perderían el control sobre todos los contenidos que eran de su propiedad si decidían borrar sus cuentas. Al siguiente mes cambió los términos del servicio señalando que cualquier cosa que los usuarios publicaran en Facebook podía ser utilizado por la compañía, dependiendo de los controles de privacidad aplicados. Los usuarios habían perdido toda posibilidad de mantener privado aquello que fue concebido para públicos íntimos y en contextos muy

³ “Data Use Policy”, *Blog de Facebook*, acceso el 23 de agosto de 2014, <https://bit.ly/3cnt2DX>

⁴ <https://www.facebook.com/fbsitegovernance>

específicos, como el de los estudiantes de Harvard. A pesar de apropiarse del contenido de sus usuarios, la red social no aceptó ninguna responsabilidad sobre lo que sus miembros hicieran dentro de la red.

Si alguien interpone una demanda contra nosotros relacionada con tus acciones, tu contenido o tu información en Facebook, te encargará de indemnizarnos y nos librarás de la responsabilidad por todos los posibles daños, pérdidas y gastos de cualquier tipo (incluidos los costes y tasas legales razonables) relacionados con dicha demanda. Aunque proporcionamos normas para la conducta de los usuarios, no controlamos ni dirigimos sus acciones en Facebook y no somos responsables del contenido o la información que los usuarios transmitan o compartan en Facebook. No somos responsables de ningún contenido que se considere ofensivo, inapropiado, obsceno, ilegal o inaceptable que puedas encontrar en Facebook. No somos responsables de la conducta de ningún usuario de Facebook, tanto dentro como fuera de Facebook.⁵

A pesar de la distancia legal que Facebook adopta respecto de las acciones de sus usuarios, ha generado mecanismos para que estos denuncien contenidos inapropiados. Dentro de las “normas comunitarias de Facebook” se identifican las conductas susceptibles de denuncia: violencia y amenazas, conductas autodestructivas, acoso, lenguaje que incita al odio, contenido gráfico, desnudos y pornografía, identidad y privacidad, propiedad intelectual, además de *phishing* y *spam*.

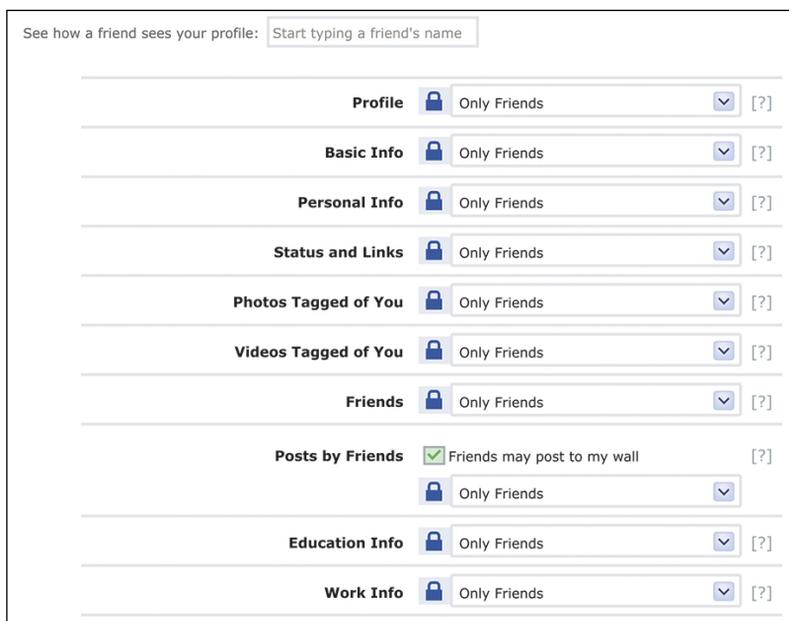
Por ejemplo, para denunciar proponían:

Si ves algo en Facebook que consideras que infringe nuestras condiciones, infórmalos. Ten presente que denunciar un contenido no garantiza su eliminación de Facebook. Nuestra comunidad de usuarios es muy diversa; por ello, es posible que algo que te resulte desagradable no infrinja ninguna de nuestras normas y no pueda ser eliminado ni bloqueado. Por esa razón ofrecemos a los usuarios la posibilidad de controlar qué ven en Facebook. Si quieres, puedes ocultar a las personas, páginas o aplicaciones que te parecen ofensivas o romper tu conexión con ellas sin que se les notifique.⁶

⁵ “Declaración de principios y responsabilidades”, <http://www.facebook.com/legal/terms>

⁶ “Normas comunitarias”, www.facebook.com/communitystandards

Ilustración 8. Controles de privacidad en octubre de 2009



Utilizar los controles de privacidad puede ser algo complicado para los usuarios por la complejidad de la plataforma a la que se enfrentan. En el año 2009 se permitía controlar la información del perfil, la información básica, personal, el estatus y sus vínculos, las fotos etiquetadas, los videos en donde aparece el usuario, sus amigos. También se permitía configurar quién podía escribir en el muro. Los controles de privacidad automáticamente estaban configurados para que solo los amigos pudieran ver la información. Esto es, se requería que el usuario ingresara a la configuración de su privacidad y cambiara manualmente si quería volver parte o toda la información más pública (ilustración 8). Hasta el año 2009 la arquitectura del sitio mantenía la información de los usuarios clausurada al espacio público destinado a sus amigos. Con el cambio Everyone, realizado a finales de 2009, también cambió, notablemente, la exposición de la información de los usuarios. De esta manera, se modificaron las expectativas de privacidad dentro de Facebook (ilustración 9).

Ilustración 9. Controles de privacidad en enero de 2010

← Back to Privacy	Preview My Profile...
About me About me refers to the About Me description in your profile	🔒 Everyone ▾
Personal Info Interests, Activities, Favorites	🔒 Everyone ▾
Birthday Birth date and year	🔒 Friends of Friends ▾
Religious and Political Views	🔒 Friends of Friends ▾
Family and Relationship Family Members, Relationship Status, Interested in, and Locking For	🔒 Everyone ▾
Education and Work Schools, Colleges and Workplaces	🔒 Everyone ▾
Photos and Videos of Me Photos and Videos you've been tagged in	🔒 Friends of Friends ▾
Photo Albums	🔒 Everyone ▾
Posts by Me Default setting for Status Updates, Links, Notes, Photos, and Videos you post	🔒 Everyone ▾
Allow friends to post on my wall	<input checked="" type="checkbox"/> Friends can post on my Wall
Posts by Friends Control who can see posts by your Friends on your profile	🔒 Friends of Friends ▾
Comments on Posts Control who can comment on posts you create	🔒 Only Friends ▾

Lo primero que el cambio de arquitectura logró ampliar automáticamente fue el espectro del espacio público de los usuarios. Había que recorrer el camino inverso, ingresar a los controles de privacidad para limitar el acceso de los otros a la información que hasta el momento se había proporcionado, teniendo como telón de fondo una “audiencia” específica. Lo segundo que se transformó fue el detalle de la información; adquirió relevancia publicar el cumpleaños, permitir que otros vean o no los puntos de vista políticos y religiosos, el detalle de los *posts* o mensajes publicados, los comentarios a las publicaciones y los álbumes de fotos. Otro punto sobre el que se otorgó el control fue permitir a los amigos publicar en el propio muro; el problema es que una vez que se escoge la opción “no permitir”, nadie puede publicar ahí. Varios instrumentos de control fueron removidos impidiendo que las personas puedan decidir, con un solo clic, a qué información pueden acceder sus grupos de amigos, o cada amigo en particular. Los usuarios perdieron la posibilidad de ver su perfil tal cual lo ven sus amigos al quitarles la herramienta “mira cómo tus amigos ven tu perfil”. Si un usuario quiere controlar quién ve sus fotos debe cambiar “fotos que ven de mí”, “álbumes de fotos” y “mensajes publicados sobre

mí”. Esto se vuelve todavía más difícil si se intenta personalizar cómo cada usuario puede ver su información.

Conforme se iban incrementando los controles de privacidad, menos amigable se volvía la plataforma y más difícil resultaba, a los usuarios, proteger su información privada. Las herramientas de configuración de las cuentas y de la privacidad son los espacios donde se puede practicar la ilusión del control sobre la información, pues incluso aquellos usuarios que han realizado el proceso de personalizar, cuidadosamente, su información pueden estar expuestos a que la vean terceros no autorizados si no cambiaron los instrumentos de uso de las aplicaciones (tabla 1). Las aplicaciones se convierten, de este modo, en caballos de Troya que boicotean las opciones de privacidad, ya que vuelven pública la información de los usuarios. Lo que mucha gente probablemente no sabe es que cada vez que acepta bajar una aplicación a su perfil otorga acceso a la información de los perfiles de sus amigos. Una muestra es la inexistencia de la opción “rehusar” en la plataforma de aplicaciones (ilustración 10).

Tabla 1. Controles de privacidad vs. posibilidades de control

Quién y qué tiene acceso					
Opciones	Amigos	Amigos de amigos	Personas en la red	Cualquier usuario de Facebook	Cualquier usuario de internet
Información pública	Sí	Sí	Sí	Sí	Sí
Todos	Sí	Sí	Sí	Sí	Sí
Amigos y red	Sí		Sí		
Amigos de amigos	Sí	Sí			
Solo amigos	Sí				

Quién y qué tiene acceso			
Opciones	Aplicaciones en las que está registrado	Aplicaciones en las que otros están registrados	Búsquedas de Facebook o Google
Información pública	Sí	Sí	Sí
Todos	Sí	Sí	Sí
Amigos y red	Sí	Sí	
Amigos de amigos	Sí	Sí	
Solo amigos	Sí	Sí	

Fuente: Cordova 2010, 38.

Ilustración 10. Ausencia de la opción “rehusar”, uso de información en aplicaciones

Overview **Settings**

What Other Users Can See via the Facebook Platform

When a friend of yours allows an application to access their information, that application may also access any information about you that your friend can already see. [Learn more.](#)

You can use the controls on this page to limit what types of information your friends can see about you through applications. Please note that this is only for applications you do not use yourself:

Share my name, networks, and list of friends, as well as the following information:

<input checked="" type="checkbox"/> Profile picture	<input checked="" type="checkbox"/> Event's I'm invited to
<input checked="" type="checkbox"/> Basic info	<input checked="" type="checkbox"/> Photos I've taken
<input checked="" type="checkbox"/> Personal info (activities, interests, etc.)	<input checked="" type="checkbox"/> Photos taken of me
<input checked="" type="checkbox"/> Current location (what city I'm in)	<input checked="" type="checkbox"/> Relationship status
<input checked="" type="checkbox"/> Education history	<input checked="" type="checkbox"/> Online presence
<input checked="" type="checkbox"/> Work history	<input type="checkbox"/> What type of relationship I'm looking for
<input checked="" type="checkbox"/> Profile status	<input type="checkbox"/> What sex I'm interested in
<input checked="" type="checkbox"/> My wall	<input type="checkbox"/> Who I'm in a relationship with
<input checked="" type="checkbox"/> My notes	<input type="checkbox"/> Religious views
<input checked="" type="checkbox"/> Groups I belong to	<input checked="" type="checkbox"/> Website

Do not share any information about me through the Facebook API

Sin embargo, con las condiciones que Facebook estableció a fines de 2009 esto desaparece completamente. Ya no es posible optar por “no compartir ninguna información sobre mí”. Todos los miembros de Facebook están obligados a compartir información. Si no desean hacerlo, entonces deben recorrer un intrincado camino de controles de privacidad y negarse a bajar aplicaciones en su perfil (ilustración 11).

Ilustración 11. Ausencia de controles para optar por “no compartir información sobre mí”

← Applications and Websites

What your friends can share about you through applications and websites

When your friend visits a Facebook-enhanced application or website, they may want to share certain information to make the experience more social. For example, a greeting card application may use your birthday information to prompt your friend to send a card.

If your friend uses an application that you do not use, you can control what types of information the application can access. Please note that applications will always be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone.

- Personal info (activities, interests, etc.)
- Status updates
- Online presence
- Website
- Family and relationship
- Education and work
- My videos
- My links
- My notes
- My photos
- Photos and videos of me
- About me
- My birthday
- My hometown
- My religious and political views

Save Changes

Ilustración 12. Nuevos controles no permiten ver qué se muestra a los otros usuarios

The image shows a screenshot of the Facebook 'Privacy > Search' settings page. At the top, there is a header 'Privacy > Search'. Below it, the 'Search Discovery' section explains that users can control who can find them through search, with a note that friends will always be able to find them. A 'Search Visibility' dropdown menu is set to 'Everyone'. The 'Search Result Content' section explains that users can control what people can see in search results. It lists five items that can be seen: 'My profile picture', 'My friend list', 'A link to add me as a friend', 'A link to send me a message', and 'Pages I am a fan of'. All five items have checked checkboxes. The 'Public Search Listing' section explains that users can control whether their search result is available outside of Facebook. A checkbox for 'Create a public search listing for me and submit it for search engine indexing (see preview)' is checked. A note at the bottom states that minors do not have public search listings.

Privacy > Search

Search Discovery
Use this setting below to control who on Facebook can find you through search. Your Friends will always be able to find you.

Search Visibility Everyone

Search Result Content
People who can find you in search can click through to a very limited version of your profile. Use these checkboxes to control what people can see in addition to your name.

People who can see me in search can see:

- My profile picture
- My friend list
- A link to add me as a friend
- A link to send me a message
- Pages I am a fan of

Public Search Listing
Use this setting to control whether your search result is available outside of Facebook.

Create a public search listing for me and submit it for search engine indexing (see preview)

Please note that minors do not have public search listings - listings created by minors will activate only when they are no longer minors.

Hasta ese momento, las personas podían especificar qué información compartir. Desde entonces, al usar una aplicación abren esta posibilidad automáticamente y sin opción a negativa; entonces el nombre, la foto del perfil, género, ciudad donde vive, su red, la lista de amigos y las páginas de las cuales el usuario es *fan* son compartidas. Para volver todavía más frágil la capacidad del usuario de determinar cómo compartir su información, es decir, qué considera que es público y qué no, Facebook Connect permite que sus amigos puedan rastrear algunas de sus acciones fuera de Facebook, cada vez que hacen clic en la nueva característica *like*, o que Google publique en su motor de búsqueda toda la información del perfil y aquella que el usuario no la haya restringido previamente, a través de sus controles de privacidad. En las antiguas herramientas de control de quién y cómo podía acceder a nuestro perfil se podía personalizar la información que mostraba Facebook de sus usuarios y se proponía que los perfiles estuvieran disponibles para la búsqueda automática.

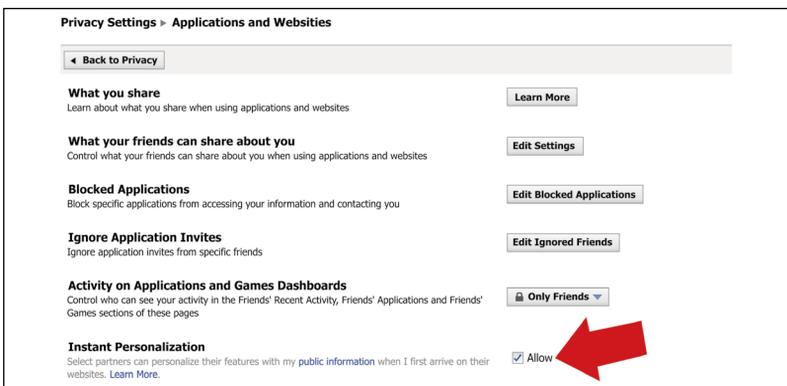
En el cambio de términos del servicio se mantiene la disponibilidad pública del perfil, pero se eliminan los controles para escoger qué volver público, pasando a un modelo de indexación automático (ilustración 12).

El problema, además, era que Facebook indexa información personal como el muro, los comentarios y las actualizaciones. Si las personas ingresan a Facebook pensando que se enrolan en una red privada, se equivocan. Facebook ha ido eliminando el control de sus usuarios sobre su información, obligándolos a ceder datos que antes no estaban dispuestos a compartir. Pero también está condicionando a las personas a mantener conductas que antes la reservaban a los amigos en espacios que cada vez son más públicos, logrando que sus expectativas de privacidad se arrinconen ante el presupuesto de Zuckerberg de transparencia radical.

Facebook funciona con un sistema *opt-out* de control de privacidad. Ya he demostrado que este tipo de arquitectura es capaz de condicionar las opciones que hacen sus usuarios. Cuando ofrece una opción automática, esta tiene más posibilidades de ser escogida por sus miembros, pues una opción diferente requiere someterse a un proceso más largo y complejo de toma de decisiones, muchos miembros simplemente no pueden seguirle el ritmo al set de controles.

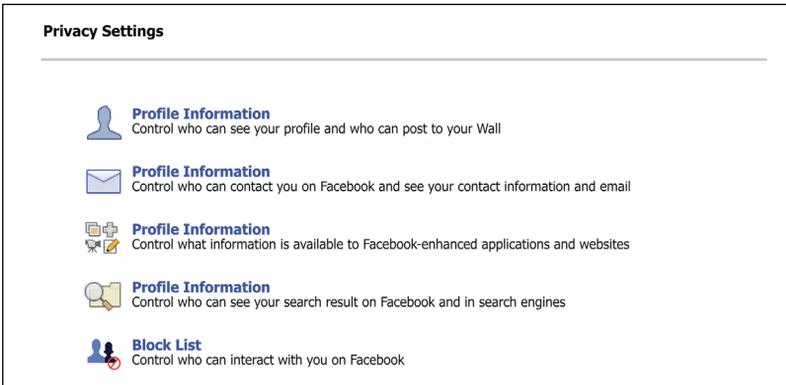
Cuando en abril de 2010 Facebook lanzó “personalización instantánea”, en realidad propuso un sistema *opt-out* muy difícil de normar por parte de los usuarios (ilustración 13). Si alguien optaba por desactivar la personalización instantánea, entonces aparecía un mensaje que lo desestimulaba a realizar esta acción preguntando: “¿Está seguro?”; si tomaba esta opción, el usuario tendría que personalizar sus opciones

Ilustración 13. Sistema *opt-out* de personalización instantánea



Fuente: Axon 2010.

Ilustración 14. Escalamiento de controles de configuración de cuenta



manualmente en cada una de las aplicaciones que fuese a utilizar, pues, de lo contrario, su red de amigos todavía podría utilizar su información pública para enriquecer sus propias experiencias (ilustración 14).

Una vez que el usuario decidía personalizar su información manualmente, Facebook le ofrecía cinco páginas para que empezara su experiencia. En cada escalón se volvía más difícil para los usuarios escoger los cambios.

Facebook describe los instrumentos de privacidad con la palabra “control” [...]. Y aunque Facebook indica que entrega herramientas de control de privacidad a sus miembros, estos están perdiendo el control consistentemente a lo largo del tiempo y están afrontando barreras más altas para ejecutarlo (Cordova 2010, 51).

No olvidemos que, al final, Facebook se reserva el derecho a cambiar las normas de privacidad de la plataforma, de forma unilateral, y que el uso ininterrumpido por parte del usuario se constituye en una tácita aceptación de tales cambios. Además, el artefacto solo notifica a sus miembros los cambios que Facebook considera sustanciales.

El poder de la arquitectura que Facebook diseña para regular las conductas de sus usuarios y las formas en que su exposición se vuelve más pública cuando habitan la red social, se plasman, en gran medida, en la función que cumplen sus sistemas de configuración *opt-out*

de la privacidad. El diseño de código muestra cómo los usuarios han perdido paulatinamente la capacidad de escoger cómo son vistos por los otros, o el nivel de publicidad de sus acciones dentro y fuera de Facebook. Los cambios en la arquitectura al crear el muro, News Feed o Facebook Connect van naturalizando la exposición de los sujetos en una plataforma que los vuelve cada vez más públicos, sin que muchas veces apenas se den cuenta. Cuando las personas optan por los controles automáticos que les ofrece su cuenta, rara vez son conscientes de cuánto está cambiando el grado de visibilidad al que están expuestas sus prácticas dentro de la red; tampoco están al tanto de que el “control” prometido sobre su información difícilmente puede cumplirse, en particular cuando las opciones desaparecen del menú de controles. La función del diseño de Facebook va volviendo cada vez más jerárquica su relación con los usuarios, busca crear un espacio virtual transparente donde las personas actúen para públicos diversos como si estuvieran en un espacio restringido a los amigos. Facebook parte de una premisa radical: una inevitable transparencia va a alcanzar a la vida moderna. Solo que esa transparencia siempre atañe al usuario y no a la compañía, aunque en sus términos del servicio indique cómo son utilizados los datos de sus usuarios.

El diseño transparente que ha escogido Facebook para mostrar el modo en que sus usuarios habitan la red también ha vuelto más difícil a los usuarios encontrar los modos de volverse más privados, en particular si el camino que Facebook les proporciona para alcanzar mayores niveles de privacidad es tan tortuoso. Pues mientras más botones se deba interrelacionar, más complejo se vuelve proteger su privacidad. Es extraño el contraste que presenta esta parte del diseño frente a la función minimalista escogida para el resto de la plataforma.

Facebook ofreció, desde su inicio, en Harvard una “privacidad limitada”, es decir, una razonable expectativa de privacidad sobre los datos compartidos dentro de la red social. La privacidad limitada es posible cuando una persona entrega sus datos a otra y espera que los mismos no sean difundidos en el futuro. Existen grados en el reconocimiento social de las expectativas de privacidad: la que una persona espera no es completa o absoluta, pero ello no significa que sea poco razonable esperar obtenerla. Así, “el mero hecho de que una persona pueda ser vista por alguien no significa

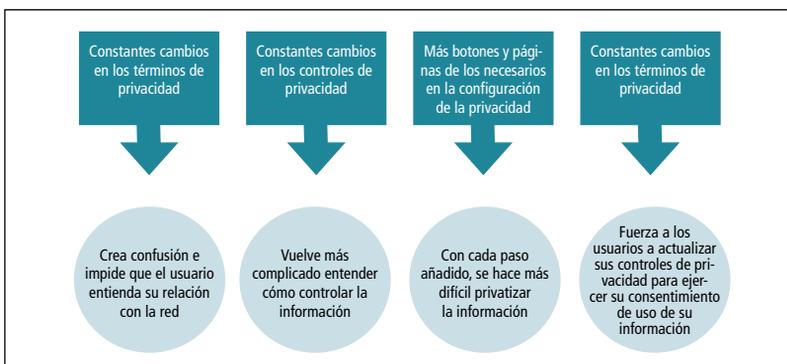
que automáticamente pueda ser forzada legalmente a ser vista por todos” (McCarty 1998, citado por Strahilevitz 2005, 939-49).

En su primer estadio Facebook funcionó como una red privada; su política garantizaba a sus miembros que todo lo que hicieran se mantendría en privado dentro de la red. Este tipo de protecciones contribuyó a generar confianza entre los usuarios y Facebook. Sin embargo, la red ha ido evolucionando hacia un sistema abierto de intercambio de información, los usuarios pueden actuar en internet desde sus identidades Facebook elevando el tráfico de información que producen y que se almacena dentro de la red. De la mano de estos cambios, las políticas de privacidad se han modificado constantemente hasta el punto de volverse autoritarias y poco flexibles. Algunas veces Facebook ha cambiado su arquitectura antes de notificar a sus usuarios, comprometiendo información que los miembros consideran privada:

Notificar a los usuarios cómo la información será usada, luego de que ya ha sido expuesta a terceros –como en el caso de las aplicaciones y de la personalización instantánea– no cumple con los estándares de la notificación. Además, usar información que los usuarios no pensaban compartir, sino dentro del contexto en que fue originada, también viola los estándares de uso (Cordova 2010, 74).

Las barreras impuestas al usuario, con respecto al control de su información, provocan consecuencias negativas en las verdaderas posibilidades que tiene de proteger la información (gráfico 6).

Gráfico 6. Posibilidades de ejercer el control de la información



Los sujetos son capaces de representarse de modo distinto, dependiendo del contexto frente al cual se constituyen. Esta capacidad de edificar perfiles específicos y situados como profesionales, amigos o padres de familia se anula en Facebook. El espacio virtual las reúne a todas y expone quiénes somos sin diferenciación, revelando mucho más de nosotros mismos. Zuckerberg diseñó Facebook con ese propósito, mostrar la identidad única de las personas; para él los días en que se podía presentar una imagen en el trabajo y otra entre los amigos estaban terminando. Facebook le da consistencia a las personas y el tipo de transparencia que la red provoca puede ayudar a construir una sociedad más saludable, pues en un mundo transparente y abierto las personas deben hacerse cargo de sus actos y comportarse responsablemente (Kirkpatrick 2010, 199). Se crea entonces una intersección entre lo que las personas proyectan y lo que los otros contestan a esas proyecciones identitarias. Según Zuckerberg, con el tiempo las personas se sienten más cómodas compartiendo todo tipo de información de forma más abierta y con más gente, “la norma social ha evolucionado con el tiempo [...] hemos decidido que estas deben ser las normas sociales ahora y simplemente fuimos por ellas” (citado por McCullagh 2010, en línea). Facebook presiona cada vez más para evitar que los usuarios privaticen su información personal al restringir o eliminar la habilidad de construir una distinción entre lo público y lo privado, a través del código de la red.

Privacidad y publicidad

Del modelo de ingresos basado en anuncios de empresas expuestos en *banners*, al estilo original de Google, Facebook pasó a uno más personalizado y extensible a toda la web, lo cual transformó el modo de hacer publicidad en línea. A través del cambio de la arquitectura del artefacto sociotécnico, Facebook ha ido promoviendo la vinculación más estrecha entre los *dossiers* digitales que sus miembros producen y el uso de esta información por parte de las empresas. El estímulo para crear perfiles de estilos de vida ha resultado sumamente valioso en el mercado de la publicidad y la transformación del código ha caminado paralelamente con las regulaciones legales que facilitan la recolección y uso de la información de los miembros de la red social.

Desde la creación de grupos y fans de los perfiles de las empresas, el ingreso de las aplicaciones a la red, así como su transformación en la plataforma, el usuario ha perdido la posibilidad de controlar la información que los desarrolladores de aplicaciones y los anunciantes recolectan de sus perfiles. Así, se conoce que varios desarrolladores venden a terceros la información que recopilan, sin que sea necesaria una autorización de los usuarios (Rotenberg 2010).

Los tipos de anuncios que se han diseñado dentro del estilo de Facebook (Sponsored Pages, Social Ads, Engagement Ads) han utilizado el Social Graph para crear publicidad viral y luego Facebook Connect se hizo cargo de expandir sus fronteras a la web en general. Solo en Facebook es posible crear publicidad dirigida usando la información que las personas entregan “voluntariamente” dentro de su interrelación social. Es únicamente en este entorno virtual donde las empresas pueden comprar *self-service advertising* para generar publicidad situada. Y solo en Facebook los usuarios pueden comprar bienes virtuales a la compañía, cada vez con menos mediación de terceros a través del crédito Facebook. Este nuevo esquema publicitario ayuda a encontrar los productos que las personas estaban buscando, pero también da un paso más adelante y produce necesidades de consumo a través de la información orgánica del sitio; entonces, vuelve comercial cada dato subido a la red desde los estilos de vida que los miembros de Facebook producen en sus representaciones del ser y sus interrelaciones con otros. Para Zuckerberg la identidad de las personas está construida, en gran medida, por las cosas que les gustan, y ello tiene valor comercial (citado por Kirkpatrick 2010, 260). El siguiente paso de este visionario fue establecer un esquema de monetización del consumidor, para lo que utilizó los datos personales de los perfiles y de los recorridos de los usuarios fuera de las fronteras de la red social.

Los medios sociales tienen como centro la conversación, y el Timeline cierra esta controversia: ya no es posible funcionar en un medio social digital sin participar en la conversación [...] Timeline por fin le permite a la industria añadir profundidad a la marca y lograr su tarea más fundamental: *contar una historia* (Owen 2012).

En este proceso, la privacidad resulta seriamente comprometida. El modelo de publicidad diseñado por Facebook está construido sobre espacios virtuales regulados que condicionan la exposición del sujeto. La opacidad de la tecnología como regulación, disfrazada de gratificación inmediata, esconde una estructura de negocios basada en un sujeto ajeno a la monetización de sus acciones. Aunque Facebook tiene publicada mucha información en su sitio web sobre el uso de los datos personales de sus miembros, he mostrado que alrededor de un 50 % no ha leído o no ha comprendido cabalmente a lo que se compromete cuando ingresa a la red social; tampoco el riesgo de uso que tiene “todo” el contenido que publican y que no está adecuadamente protegido a través de la configuración de la privacidad del perfil. Dentro del punto 2 de “Compartir el contenido y la información” de su Declaración de Derechos y Responsabilidades, Facebook propone que

Eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte a través de la configuración de privacidad y aplicaciones. Además:

1. Para el contenido protegido por derechos de propiedad intelectual, como fotografías y video (en adelante, “contenido de PI”), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de privacidad y aplicaciones: Nos concedes una licencia no exclusiva, transferible, con posibilidad de ser subotorgada, sin royalties, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (en adelante, “licencia de PI”). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido con terceros y estos no lo han eliminado.
2. Cuando eliminas contenido de PI, este es borrado de forma similar a cuando vacías la papelera o papelera de reciclaje de tu computador. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros).
3. Cuando utilizas una aplicación, tu contenido e información se comparten con la aplicación. Si bien exigimos que las aplicaciones respeten tu privacidad, será tu acuerdo con la aplicación en cuestión el que regirá la forma en que esta utilizará, almacenará y transferirá dicho contenido e información. (Para obtener más información sobre la plataforma, lee nuestra Política de privacidad y la página *acerca de la plataforma*.)

4. Cuando publicas contenido o información utilizando la configuración “Todos”, significa que permites a todo el mundo, incluso las personas que no estén en Facebook, acceder y utilizar dicha información y asociarla contigo (es decir, tu nombre y foto de perfil).
5. Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello –del mismo modo que tú no tienes obligación de ofrecerlos–.⁷

Los usuarios le entregan a Facebook una licencia PI que le permite a la compañía utilizar todo aquello que publiquen en Facebook o en conexión con Facebook, esto es, a través de Facebook Connect cuando utilizan los botones *like* o *share*, entre otros. También responsabiliza a los usuarios a hacerse cargo de las condiciones de privacidad que establecen con la aplicación cuando aceptan utilizarla. Sin embargo, Facebook no muestra cuándo una aplicación es propia o es de terceros. Tampoco existe una alerta que lleve a los usuarios a conocer los Términos de Privacidad de la aplicación cuando esta no es de Facebook. En la práctica, es casi imposible que los usuarios puedan decidir utilizar una aplicación basados en las condiciones de privacidad que ella estipula, con lo cual se redondea el modelo de salida de datos personales de los usuarios al mercado de la publicidad.

En la misma Declaración de Derechos y Responsabilidades, Facebook indica:

Nuestro objetivo es ofrecer anuncios que no solo sean valiosos para los anunciantes, sino también para ti. Para lograrlo, aceptas lo siguiente:

1. Puedes utilizar tu configuración de *privacidad* para limitar cómo se pueden asociar tu nombre y fotografía de perfil al contenido comercial o patrocinado que ofrecemos. Nos das permiso para utilizar tu nombre y foto de perfil en conexión con ese contenido, de acuerdo con los límites que tú establezcas.
2. No proporcionamos tu contenido o información a anunciantes sin tu consentimiento.

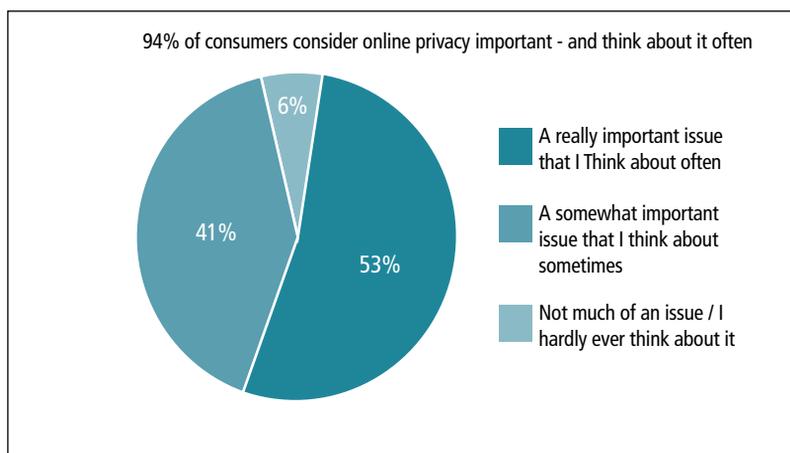
⁷ “Declaración de principios y responsabilidades”, *Blog de Facebook*, acceso el 23 de agosto de 2014, <https://www.facebook.com/legal/terms>

3. Entiendes que es posible que no siempre identifiquemos las comunicaciones y los servicios pagados como tales.⁸

Facebook no garantiza la privacidad de los usuarios desde la propia arquitectura. Lo que hace es volver a responsabilizar al usuario de su salida de datos cuando no establece una configuración de privacidad en su cuenta y, aunque señala que no entregará el contenido de la información a los anunciantes sin su consentimiento, hace uso de la información del perfil de la persona.

Según el estudio sobre las percepciones de la publicidad en línea, en 2011 realizado por TRUSTe, asesor de Facebook en el área de privacidad, el 94 % de consumidores consideró que la privacidad en línea es importante y piensa en ella constantemente (gráfico 7). Los consumidores creían que son varias las organizaciones responsables de salvaguardar la privacidad; el primer lugar lo ocupan los propios consumidores, a ellos les siguen las redes sociales, los publicistas, las máquinas de búsqueda y, sorprendentemente, al final, los gobiernos y sus regulaciones (gráfico 8).

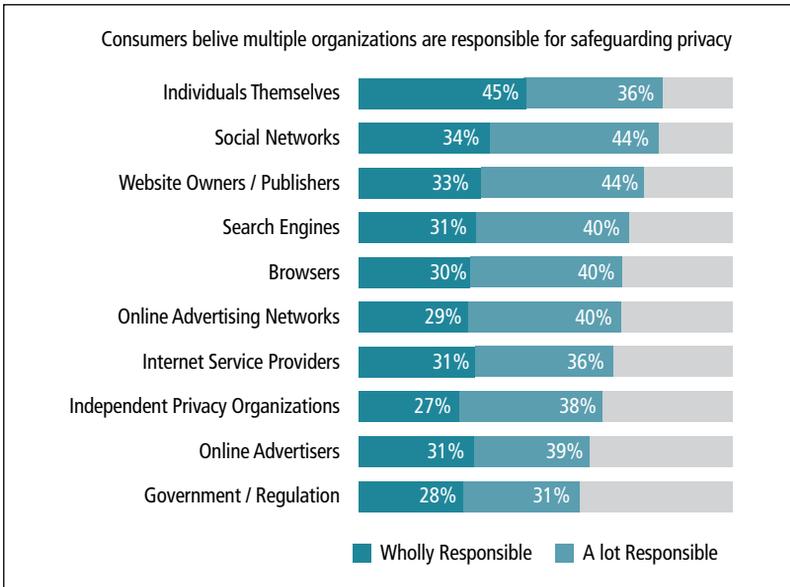
Gráfico 7. Porcentaje de consumidores que consideran importante la privacidad



Fuente: TRUSTe, <http://www.truste.com/ad-privacy/> (contenido no disponible).

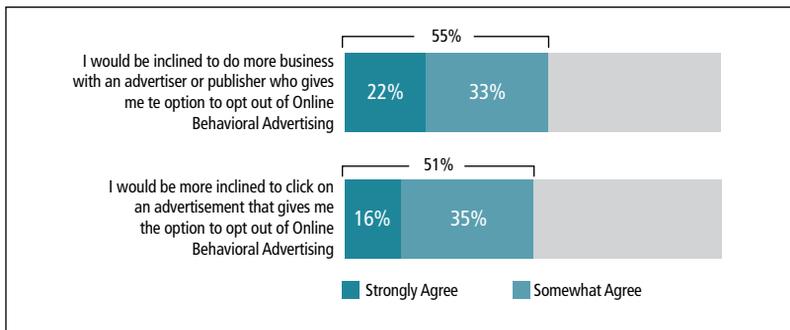
⁸ “Declaración de principios y responsabilidades”, *Blog de Facebook*.

Gráfico 8. Responsables de salvaguardar la privacidad



Fuente: TRUSTe, <http://www.truste.com/ad-privacy/> (contenido no disponible).

Gráfico 9. Confianza en los Términos de Privacidad



Un 70 % de los cibernautas tenía conciencia de las prácticas de publicidad en línea, un 54 % no estaba de acuerdo con ellas y tan solo un 8 % las apoyaba. Más de la mitad de consumidores (52 %) creía que la información personal, vinculada a la publicidad, en realidad no era la

suya, y están dispuestos a confiar más en la publicidad si la información personal no estaba vinculada.

Más de la mitad de cibernautas estaba dispuesto a hacer clic en un anuncio si consideraba que se puede controlar el uso de la información personal. En ese mismo porcentaje, los usuarios estarían inclinados a hacer negocios con esas compañías (gráfico 9).

En el caso de Facebook es importante revisar su política de crédito y de compras de bienes virtuales directamente a la compañía en relación con el estudio de TRUSTe, pues un 57 % de cibernautas escogía anuncios de marcas en las que confía.

El marco tecnológico de Facebook

Para comprender cómo se ha pasado de unas expectativas limitadas de privacidad ofrecidas por la audiencia de los amigos en Harvard de Thefacebook, a unas bajísimas expectativas de privacidad en Facebook fundamentadas en el cambio tecnológico y regulativo de la red social, voy a explicar el funcionamiento de Facebook como artefacto sociotécnico. En vez de explicar linealmente la transformación de un pequeño emprendimiento de estudiantes universitarios en una compañía con un valor de miles de millones de dólares, he preferido adentrarme en la red de relaciones que distintos grupos sociales han elaborado alrededor del artefacto sociotécnico para configurarlo. El camino de las determinaciones tecnológicas torna invisibles las acciones sociales que condicionan el avance tecnológico; del mismo modo, un estudio centrado en lo social no me permitiría mostrar el valor de la capa informática de la red social como un mecanismo de estructuración de conductas y de un nuevo tipo de socialización.

Un grupo social es un grupo de personas que se alían gracias a la interpretación que hacen de un artefacto (Bijker 1995). La construcción social de la tecnología toma como un primer nivel de análisis los conceptos que los grupos sociales relevantes elaboran sobre el artefacto (Bijker 1995; Bijker, Hughes y Pinch 1987). Constituyen mi punto de partida porque logran centrarnos en el artefacto (Thomas 2008), y al seguir los conceptos que manejan sobre el artefacto muestran su

flexibilidad interpretativa. En la evolución de Facebook están involucrados varios grupos sociales relevantes, cada uno con su visión particular sobre el asunto, que parecería que se refrieren a artefactos totalmente distintos. El concepto de flexibilidad interpretativa (Bijker 1995) es útil justamente porque profundiza en las interpretaciones del mundo que hace cada grupo social, y en el lugar que se le otorga al artefacto dentro de ese orden. El artefacto tiene la cualidad de vincular a los distintos grupos sociales relevantes y, en consecuencia, las prácticas y los sentidos que estructuran su funcionamiento.

Los grupos sociales relevantes que he rastreado alrededor del artefacto sociotécnico son los visionarios, los escritores de código, la empresa, los usuarios de Facebook y las organizaciones protectoras de la privacidad. En el entramado de sus trayectorias, la privacidad ha ido transformándose a través de regulaciones, prácticas y código. Cada grupo social ha producido una cadena de significaciones que ha configurado diferentes versiones del artefacto, pues no solo son capaces de ver diferentes aspectos del mismo, sino que también explican la existencia de distintos artefactos contenidos dentro de Facebook. Estas significaciones muestran que una cosa puede ser mejor comprendida si se considera como artefactos diferentes (Thomas 2008). Así, Facebook será descrito por cada uno de estos grupos sociales relevantes para mostrar los criterios a partir de los cuales ha sido co-construido, y cómo su funcionamiento es una evaluación socialmente construida y no una derivación de las propiedades intrínsecas del artefacto sociotécnico (Pinch y Bijker 2008).

La construcción social de un artefacto es producto de un fenómeno que combina los procesos de clausura y de estabilización del mismo (Bijker 1993). Cuando la flexibilidad interpretativa del artefacto disminuye se produce su clausura, los grupos sociales relevantes consensuan el sentido dominante del artefacto y la diversidad de estos disminuye; su grado de estabilización se traduce en la aceptación del artefacto por los grupos sociales relevantes. Cuanto más homogénea sea la aceptación del sentido, mayor es su grado de estabilización (Thomas 2008). La clausura y la estabilización aparecen cuando la flexibilidad interpretativa de un artefacto disminuye y uno de sus significados se impone sobre los otros; con ello el artefacto adquiere mayor grado de estabilización en uno o más grupos sociales relevantes (Bijker 1995).

Nye (1994) planteó que el sentido social de una nueva máquina es definido por su inventor. Sin embargo, esta relación causal del sentido no se cumple en los procesos de innovación tecnológica que superan el momento de la invención. El sentido de una tecnología termina construyéndose entre los usuarios, los mediadores y los productores a partir de los sentidos que la sociedad ha invertido en tecnologías ya existentes (Pacey 2001).

Tratar de explicar cómo funciona la privacidad dentro de Facebook desde la descripción de sus términos de servicio y políticas de privacidad impide incorporar la acción, las teorías y los intereses que consensuan un sentido estabilizado de Facebook como artefacto sociotécnico entre los distintos grupos relevantes que lo co-construyen. Puesto que el marco tecnológico no es una identidad fija (Thomas 2008), empezaré describiendo la flexibilidad interpretativa de dichos grupos, y los problemas que cada uno plantea sobre la privacidad y las soluciones que se articulan entre los sujetos, sus prácticas y las capas tecnológicas dentro de Facebook.

Los visionarios

Para los fundadores de las redes sociales que inspiraron a Facebook y sus aliados estratégicos a pasar de ser un emprendimiento a una empresa global, el objetivo era *conectar* a la gente en línea. Todos enfrentaban el reto de configurar la internet social a partir de los intereses de las personas: hacer amigos, conseguir citas, conectarse profesionalmente, jugar en línea. La privacidad no era un problema, pues muchos aplicaban la ética *hacker* que favorece el anonimato y la capacidad de los usuarios de interactuar en espacios públicos con los mínimos controles posibles. Zuckerberg es uno de los pocos que consideró la privacidad un elemento clave y diferenciador de su red social. Ofrecer a sus usuarios un espacio virtual exclusivo, compartido solo con aquellos que conocen y que tiene como telón de fondo el campus universitario fuera de la pantalla (esto es las conexiones cara a cara de sus usuarios) era un elemento innovador y distintivo de Thefacebook, que lograba definir las libertades y controlar el ciberespacio a través del código (Lessig 2006, 6). Desde un inicio, la privacidad se tradujo

en información factible de ser compartida a partir de los Términos de Privacidad y de las políticas de uso de la red social dentro de una lógica de 0 y 1.

Los escritores de código

Este grupo muestra el valor del código dentro de la estructuración y regulación del ciberespacio y de las posibilidades que ofrece para normar lo público y lo privado dentro de la red social. Asimismo, me permite explicar las relaciones sociotécnicas a partir de la metáfora del “tejido sin costuras” que compele a no realizar ninguna distinción, *a priori*, sobre el carácter tecnológico o social del artefacto (Bijker 1993). El código se irá desarrollando en un amplio ejercicio de co-construcción con los usuarios, los desarrolladores de aplicaciones, las empresas contratantes de publicidad y la necesidad de convertir Facebook en una plataforma dentro de internet, una especie de sistema operativo capaz de generar identidades en línea, y de construirse en el lugar de tránsito para la socialización virtual de los individuos: un punto de paso obligado del enlace entre personas.

El objetivo de este grupo era volver al mundo más pequeño y ponerlo al alcance de la mano de los usuarios. Para ello, Facebook terminó transformándose no solo en una red social cerrada en sí misma, sino en una forma de gobierno capaz de establecer políticas sobre inmensas comunidades. En este contexto la privacidad fue concebida como un mecanismo de confianza en el artefacto sociotécnico; los sujetos se representarían e interactuarían imaginándose frente a un público definido, para lo que se les exigió utilizar su verdadera identidad y entregar información personal. Una vez establecido el sistema de confianza, Facebook se transformó en un artefacto que promueve la transparencia radical; por ende cambió sus términos de servicio, sus políticas de privacidad y su arquitectura; volvió público el espacio virtual a través del nuevo código Everyone, que obligó al usuario a compartir más a través del nuevo orden (Kirkpatrick 2010). La homologación de los contextos sociales (convergencia social) amplificó el espectro de lo público (News Feed) y se respondió con más códigos cuando los usuarios protestaron por los cambios de la arquitectura.

La función del código desplazó hacia el usuario la responsabilidad por la privacidad del artefacto condicionando la formulación de nuevas normas sociales mientras esperaban que las personas se adaptaran a los cambios del código. Para Zuckerberg, Beacon se instaló demasiado pronto pues los usuarios todavía no estaban listos para exponer sus recorridos fuera de la web; Beacon hoy en día no sería rechazado del mismo modo pues el código ha regulado los comportamientos, modificándolos y permeándolos de otros valores, menos cercanos a la privacidad.

Las nuevas formas de representación que la capa tecnológica promueve permiten mapear y registrar la información de los usuarios. Para ello se delinea identidades más robustas, mientras se rastrea a las personas en sus recorridos a través de internet (*dossiers* digitales, según Solove 2004) con *cookies* instaladas por Facebook en el perfil de cada usuario. Una estrategia para lidiar con la privacidad es volver opacas las construcciones de lo público, a través del diseño, y enfatizar enérgicamente la noción de identidad única del sujeto.

La empresa

Además de ser una red social, Facebook es una compañía en interrelación con otras empresas dentro de la economía digital de internet. En tal sentido, busca volver rentable a la red social relacionando los perfiles de los usuarios y su interactividad en línea, con el negocio de la publicidad y la capacidad de utilizar la información de sus miembros como mercancía a ser vendida a publicistas y empresas, a escala global.

De esta manera, la privacidad se transforma en propiedad. La información de los usuarios, sus recorridos, sus intereses, sus gustos se vuelven datos que son vendidos a terceros. Bajo el eufemismo “compartir”, la empresa vende la información que producen sus miembros, pero además permite que otros (desarrolladores y empresas) utilicen los datos de sus usuarios cuando ingresan al ecosistema de Facebook. Así se registra quiénes son los usuarios, dónde viven, cuáles son sus amigos, qué les interesa y qué hacen en línea. Se promueve la producción de biografías digitales a través de Timeline para crear una relación entre las empresas y los *dossiers* digitales de los usuarios. Así logran que la relación

público-privado adquiera una nueva dimensión basada en la vigilancia de sus miembros y en la mercantilización de todo lo que dicen y hacen los usuarios.

Los miembros de Facebook

Para los usuarios de Facebook, la red social es el lugar en donde están sus amigos y conocidos. Para muchos constituye la extensión de su sociabilidad fuera de la pantalla, y para otros Facebook ha reemplazado a la antigua agenda de contactos, volviendo a las personas más asequibles. Facebook es concebido un espacio de representación que permite la interrelación con los otros; es también un poderoso lugar de producción de identidades individuales y colectivas, de nuevas normas de socialización y de gratificación inmediata. Los miembros de Facebook tienen a sus amigos al alcance de un clic y pueden contactarlos, mirar lo que han hecho, comentar sus fotos con solo ingresar a la pantalla. Sin embargo, Facebook plantea problemas importantes a los usuarios, un ejemplo es el de descubrir cómo funcionar con una identidad única para todas las audiencias que confluyen en la red. La convergencia social en Facebook aplana los contextos sociales presenciales donde funcionan las personalidades situadas de los individuos (Goffman 1981), sin que puedan diferenciar representarse para los amigos o para los colegas. Los usuarios de Facebook deben seguir el guion tecnológico del artefacto y en el camino encontrar el modo de negociar sus formas de representación y de interacción con los otros. En Facebook se redefine la “amistad” y el Social Graph se convierte en un elemento más de la identidad.

La privacidad en Facebook funciona como un sistema de verificación circular de la identidad de los usuarios, quienes se ven obligados a entregar datos personales que luego son corroborados como verdaderos por su Social Graph. Así, los sujetos actúan en el contexto de audiencias imaginadas negociando sus normas sociales y su representación con la capa tecnológica del artefacto. La privacidad en Facebook es parte de la simulación de los sujetos que fácilmente se descuidan del entorno (aplanamiento de las personas públicas del sujeto y audiencias invisibles) por apearse a la regla de conservación de la ilusión y a la obligación de representar una identidad única; se borran las barreras que se levantan

entre lo público y lo privado en el mundo presencial. La arquitectura de la red promueve la generación de información y el consumo de la producida por los amigos, el “trance” permite formas de voyeurismo que estimulan el consumo de las representaciones de los otros. Puesto que casi todo se vuelve visible con la producción de biografías en tiempo real (*Timeline*), se crean normas sociales de reciprocidad que negocian, constantemente, con las audiencias desconocidas, todo aquello que los sujetos vuelven público. La seducción de la tecnología y la simulación ocultan el funcionamiento del artefacto y las cesiones de privacidad que esto conlleva, al seguir el guion tecnológico de Facebook y las normas sociales que lo acompañan. Ello provoca una dificultad casi insalvable, ante la falta de muros entre contextos diferenciados, debido a la fuerza de la convergencia social y tecnológica del artefacto.

Así, los sujetos son obligados a disminuir sus perspectivas de privacidad, puesto que esta no solo se fundamenta en sus expectativas individuales, sino principalmente en las que la sociedad considera razonables (Pouillet y Rouvroy 2009). La sociedad en línea, que actúa en Facebook, se encuentra bajo el efecto de sistemas de vigilancia invasivos que le otorgan bajas expectativas legítimas de privacidad. A pesar de considerar que la privacidad es un elemento importante de sus vidas en Facebook, las personas terminan vendiéndose a sí mismas, no muestran ningún deseo de ser dejados en paz; todo lo contrario, intentan manipular su mundo virtual encontrando formas de presentarse a los otros (Solove, Rotenberg y Schwartz 2006).

Las organizaciones protectoras de la privacidad

Tanto para TRUSTe como para EPIC, Facebook es un sitio web, una empresa y una red social a la vez. TRUSTe intenta solucionar los problemas que las empresas tienen en cuanto a privacidad ofreciendo servicios que abarcan investigaciones, licencias y políticas de privacidad, basadas en valores como la transparencia empresarial, la opción de los usuarios o clientes, además de la confianza en la empresa con respecto a la recolección, difusión y uso de datos personales. Para EPIC, en cambio, la privacidad es un derecho que debe ser protegido; así, lidera a grupos de activistas para conseguir que las organizaciones, en particular las redes

sociales, vuelvan menos opacos sus términos legales y sus políticas de privacidad, para que sean los sujetos quienes escojan cómo compartir su información. En el caso de Facebook, EPIC ha solicitado que los instrumentos legales sobre privacidad, que mantiene la empresa, sean más fáciles de entender y más asequibles a los usuarios; tal cual están contruidos hoy en día, dichos controles no permiten al usuario tomar decisiones informadas sobre cómo distinguir entre la información pública destinada a todos los miembros de la red (e incluso de internet) y la información más privada, dirigida a audiencias específicas diseñadas por el propio usuario. EPIC también critica a Facebook sus prácticas de vigilancia, a través de sus *cookies*, de los recorridos que realizan sus usuarios fuera de la red social en internet y el que permita que los desarrolladores mantengan, indefinidamente, la información personal de los usuarios de Facebook.

En ambos enfoques empresariales se trata de la protección de la privacidad desde la teoría del acceso restringido a la información de los usuarios y el derecho a la autodeterminación informacional de las personas (control de los datos). Tanto TRUSTe como EPIC no se oponen al “trato propietario” sobre la privacidad, muy cercano al pensamiento liberal, que se debate entre defender al individuo o garantizar el valor universal de la propiedad privada. La información funciona como clausura de la privacidad para los visionarios, el código, la empresa y las organizaciones protectoras de la privacidad, excepto para los miembros de Facebook, quienes consideran que la privacidad, en este artefacto, es un fenómeno situado que se construye en la relación entre la arquitectura del código y la norma social.

De esta manera, la flexibilidad interpretativa traduce la racionalidad que está detrás de la construcción social del artefacto sociotécnico, pues permite verlo tal y como los grupos sociales relevantes lo entienden (Thomas 2008). Los distintos sentidos atribuidos al artefacto nos explican las versiones situadas que lo revelan y sacan a la luz artefactos distintos. Para los *visionarios*, la conectividad producida por el desarrollo tecnológico les impulsa a imaginar formas de redes sociales que atraigan a las personas a socializar en línea. Para las *empresas*, Facebook es un ecosistema de publicidad dirigida sin parangón, y un fenómeno de la comunicación y el intercambio de datos en internet. Para los *escritores*

de código, el artefacto es una plataforma capaz de organizar la sociabilidad de millones de personas en todo el mundo, de forma condicionada por la estructura de su arquitectura y capaz de normar conductas; es también un sistema de construcción de *dossiers* digitales que se traducen en estilos de vida que pueden ser comercializados, gracias a la mano de obra gratuita de sus usuarios. Para los *miembros*, Facebook es el espacio donde están los amigos, es una extensión de la socialización presencial, y un modo de entrar en contacto con los conocidos; asimismo, es una experiencia de simulación que obliga a imaginar nuevas normas sociales para mantener la interacción con los otros y las formas de representación de los sujetos. Finalmente, es una arena pública que no distingue entre contextos sociales diferenciados y que propone una exhibición cada vez mayor de los usuarios condicionados por las capas tecnológicas de la red social.

A pesar de la alta flexibilidad interpretativa del artefacto sociotécnico, Facebook tiene sentidos consensuados que le permiten trabajar, pues su función se ha establecido mediante una evaluación socialmente construida. Facebook es una red social que permite conectar al mundo, volverlo más pequeño, y es el espacio virtual más importante de representación voluntaria de los sujetos. Ello permite considerarlo el ecosistema ideal para conectar las personas y las cosas, las organizaciones y los políticos y las empresas con los clientes. Facebook es una red exitosa no porque funciona, sino por haber sido aceptada por los grupos sociales relevantes (Bijker 1993, 119). Una vez que los grupos sociales relevantes consensúan los sentidos de los artefactos, solo uno de estos se vuelve dominante, por lo que adquiere un alto nivel de estabilización en uno o varios de los grupos dominantes (Bijker 1995).

Un ámbito distinto al exclusivamente social constituye el llamado marco tecnológico. A través de este se evita el riesgo de reproducir la dicotomía sociedad-naturaleza, pues el marco tecnológico *es heterogéneo* ya que no se refiere exclusivamente a un dominio cognitivo social, es también artefactos, protocolos, código, teorías científicas, valores culturales y conocimiento tácito. Los marcos tecnológicos no son entidades fijas porque son el producto de los procesos de estabilización del artefacto tecnológico, forma parte del conjunto de interacciones individuales de los grupos sociales relevantes, lo que requiere que sean sostenidos,

constantemente, por las interacciones. Finalmente, los marcos tecnológicos plantean los objetivos y las herramientas para la acción, a través de las estrategias orientadas a resolver los problemas del artefacto y el disciplinamiento de los miembros de los grupos relevantes (Thomas 2008).

En el caso de Facebook, el código ha servido a la monetización de las prácticas sociales dentro del espacio virtual; asimismo, ha condicionado la socialización homologándola, estabilizando la función de la red social como negocio dentro de una socialización mediada por la transparencia radical. Así, de la diversidad de significados que le fueron otorgados al artefacto, varios empiezan a estabilizarse y clausurarse dentro de la gramática del marco tecnológico.

El marco tecnológico de Facebook nos permite entonces revisar cómo se construyen los problemas del artefacto y cuáles son sus posibles soluciones de acuerdo con los intereses de cada grupo social relevante. Este segundo nivel de análisis del constructivismo social abre la puerta a la estructura de las relaciones entre los grupos sociales y sus artefactos, así como a las estrategias de resolución de problemas gracias a las cuales los artefactos se vuelven funcionales. El carácter explicativo de este segundo momento hace énfasis en el análisis del investigador.

Problemas y soluciones de los grupos sociales relevantes

Los visionarios se enfrentan al problema de cómo conectar a las personas en línea; lo enfrentan diseñando espacios virtuales regulados, apelando al valor del código para normar comportamientos –comprendiendo la importancia de la arquitectura como política– y generando modelos de negocios que les permitan volver exitosas las redes sociales.

Los escritores de código se enfrentan a varios problemas. El primero es cómo regular el ciberespacio para que los usuarios hagan lo que Facebook quiere. Su solución es utilizar la arquitectura como política, toman ideas de otras redes sociales en línea para capitalizar los guiones cognitivos que los usuarios han desarrollado en el ciberespacio, es decir, los aprendizajes que los individuos han alcanzado en su interacción con los objetos tecnológicos (Akrich 1992; Latour 2002). Moskovitz y Zuckerberg escribieron el código con el fin de construir un artefacto

que inscribiera las representaciones de la sociabilidad virtual dentro de la capa tecnológica, de forma más o menos coercitiva, para lograr que los usuarios hagan lo que está prescrito. En tal sentido, el artefacto se convirtió en un proyecto de identidad en la cual programadores y usuarios se asumieron agentes activos del desarrollo tecnológico. En un primer momento, el código funcionó para generar un entorno que permitiera la reproducción de la sociabilidad fuera de la pantalla dentro del espacio virtual, regulando el espacio y la forma de habitarlo, a través de la función normativa de su arquitectura. Utilizó un diseño minimalista para promover la generación de contenidos de los usuarios. Se empezó invitando a construir una representación del ser que les permitiera a los usuarios conservar la ilusión (Giffin 1984), asumir su rol dentro de la red de relaciones sociales, fomentar controles de privacidad que permitan generar confianza en Facebook, así como incentivar la interactividad y la entrega de información.

El segundo problema que afrontan los escritores de código está relacionado con lo que deben aprender de los usuarios. Para ello, los arquitectos empezaron a prestar atención a la interactividad de estos y a reinventar la estructura del sitio con el fin de promover las consignas de conectividad e intercambio de información; a partir de estos aprendizajes aparecieron los muros, News Feed, las fotos, las etiquetas y el Timeline. El tercer problema es aprender de las transformaciones del propio artefacto. Zuckerberg y sus colaboradores principiaron a elaborar teorías sobre qué es Facebook y en lo que se podría convertir. Así apareció el concepto de transparencia radical, de identidad única, de economía del don dentro de Facebook y de abandonar el paradigma de red y adoptar el de plataforma para utilizarlo a modo de sistema operativo o “ecosistema” dentro de internet. De esta manera se aprovechó la convergencia social y tecnológica, por lo que el código de *software* se transformó en una forma de arquitectura social. Así, surgieron nuevos fenómenos como el Social Graph, que funciona como un sistema de distribución de la información y que contiene también objetos, organizaciones e ideas con las que la gente se conecta; el valor del tagging para aumentar la fuerza del Social Graph; alcance viral de News Feed y el concepto de “historias” para moldear las formas de representación de los sujetos, al igual que la construcción de nuevos modelos de publicidad dentro del sitio.

Para la empresa, el problema que afrontó Facebook una vez que empieza a ser una red social exitosa es volverse rentable, y convertirse en un negocio a gran escala. Para ello la compañía se instaló en California, aceptó inversionistas, profesionalizó la empresa y reinventó modelos de publicidad en línea (grupos, muro, *fans*; *flyers*; *self-advertising*; *social ads*; *engagement ads*; aplicaciones; historias; bienes virtuales; crédito Facebook). Pero el giro más importante fue monetizar al usuario. Facebook utiliza Free Labor o mano de obra gratuita para producir valor en la compañía, convirtiendo a sus usuarios en los nuevos artesanos digitales (Barbrook [1999] 2005) y reimponiendo el régimen de propiedad y la mercantilización de los bienes culturales que sus usuarios producen. Así, utiliza las licencias de PI, mediante las cuales obligan a sus usuarios a firmar su Declaración de Derechos y Responsabilidades. El trabajo inmaterial de sus miembros transforma el conocimiento colectivo en mercancía y lo compensa selectivamente (solo a la empresa y no a los usuarios). Facebook se convierte, de este modo, en un sistema de producción de bienes culturales comercializables y en el medio de venta de publicidad dirigida más importante del mundo o, como lo denomina Mike Lazerow, en el proyecto Genoma de Internet (Kirkpatrick 2010).

Para los miembros de Facebook el problema fue trasladar sus formas de socialización presenciales a la simulación del mundo virtual de la red social. Con esa finalidad debieron adaptarse al guion tecnológico del artefacto y negociar constantemente su sociabilidad entre la capa tecnológica y la capa cultural. Así se producen nuevas normas sociales para habitar Facebook. Con los desencantos que les provoca la simulación (Turkle 2009), los usuarios adquieren una mayor conciencia de la fuerza modeladora de conductas que tiene el código de Facebook.

Las organizaciones protectoras de la privacidad, como TRUSTe y EPIC, intentan resolver los riesgos que corre la privacidad, pero lo hacen desde dos ángulos totalmente distintos. TRUSTe protege a las empresas que la contratan y EPIC parte de los derechos y libertades de la ciudadanía. La solución al problema que aplica TRUSTe se canaliza a través de servicios a las empresas para proteger sus términos, prácticas y políticas de privacidad. La solución al problema de la privacidad que escoge EPIC es demandar legalmente a las compañías e instituciones

que violan los derechos a la privacidad de la ciudadanía, sean estos consumidores, cibernautas o usuarios.

El marco tecnológico me sirve para adentrarme en todo aquello que pueda intervenir en las relaciones entre los grupos relevantes y la construcción de los problemas y soluciones alrededor del artefacto sociotécnico (Bijker 1995). Para ello he analizado, en este capítulo, las teorías detrás del desarrollo de Facebook en sus inicios, las dinámicas de todos los actores para co-construir el artefacto, las prácticas y el código que van configurando a Facebook a través de la interrelación entre objetos, organizaciones, sujetos, lenguajes digitales y conocimiento tácito dentro del marco tecnológico.

SECCIÓN 4
CONTROVERSIAS
Y ENSAMBLAJES

Capítulo 9

Las controversias sobre la privacidad en Facebook

En este capítulo exploro los sentidos que se le otorgan a la privacidad, pues los distintos actores la significan de modo distinto y, por lo tanto, el nivel de flexibilidad interpretativa se eleva. Con este fin explico las controversias sobre privacidad que los actores han desarrollado en el proceso de co-construcción de la privacidad en la red social, y el cambio de la norma social en la interacción entre la capa tecnológica y la capa social de Facebook para redefinir “lo privado”.

A través del análisis sociotécnico de Facebook he develado varios momentos de la co-construcción del artefacto, particularmente relevantes para definir qué es lo privado en cada grupo implicado. Ahora, al privilegiar la voz de los actores explico las distintas posturas que mantienen sobre la privacidad, el momento de disputar los sentidos en varias etapas históricas del artefacto. Para ello he revisado los problemas y los consensos sobre privacidad a los que se llegó en los casos News Feed, en 2006, Beacon, en 2007; el cambio de los términos del servicio y en la configuración predeterminada de Everyone en 2009. También he revisado la demanda del gobierno de Canadá a Facebook, en 2009, por atentar contra la vida privada. Con esta finalidad utilizo el concepto de controversia y muestro cómo ciertas nociones de privacidad se estabilizan a través de la ideología que guía el código. Esta transforma las prácticas de socialización de los sujetos al naturalizar la exposición de las personas dentro de un nuevo sistema social en el ciberespacio.

Como mencioné, los estudios de ciencia, tecnología y sociedad se apropiaron del concepto “caja negra” de la ingeniería, para explicar cómo funcionan los artefactos, en particular, en las etapas controversiales de

su historia. Este término se ha utilizado para describir los resultados predecibles de un objeto cuyo funcionamiento interno no necesita ser conocido para que pueda ser utilizado (Kreimer 1999; Sismondo 2010; Whitley 1972). Así, tanto la ciencia como la tecnología producen cajas negras, sus hechos y artefactos se dan por sentados y no se cuestionan su origen ni sus trayectorias una vez que se establecen exitosamente. Whitley utilizó dicho concepto para describir el modo en que la sociología de la ciencia había restringido su investigación a los insumos que ingresaban al sistema y a los productos provenientes del mismo, sin estudiar los procesos internos que eran inobservables. De esta manera, una vez que un hecho o artefacto se convierte en caja negra, adquiere una cierta inevitabilidad que impide revisar su historia. Para entender cómo un artefacto funciona, los estudios de CTS se enfocan en dar cuenta de las etapas controversiales de su historia; al abrir la caja negra, la tecnología se convierte en objeto de análisis:

Lo que se necesita es una comprensión de la tecnología desde adentro, como un cuerpo de conocimiento y como un sistema social. En lugar de eso, la tecnología es habitualmente tratada como una “caja negra” cuyos contenidos y comportamientos pueden ser asumidos a partir del conocimiento común (Layton 1977, 198 citado por Pinch y Bijker 2008, 27).

El funcionamiento de los artefactos ha sido explicado, linealmente, relacionando sus propiedades técnicas con su propósito (uso focal, es decir, para lo que deben ser utilizados); esta explicación supone que se conoce, de antemano, su propósito. Sin embargo, es justamente el “propósito” del artefacto lo que disputan las controversias tecnológicas (Bruun y Hukkinen 2008); debido a que los propósitos son socialmente definidos entre los grupos sociales relevantes, a través de negociaciones, de la agencia de la tecnología y de los juegos de poder que terminan estabilizando un sentido del marco tecnológico y debilitando algunos de los significados otorgados por varios grupos sociales relevantes. Las controversias muestran los momentos de cambio tecnológico y la posibilidad que tienen los artefactos de ser interpretados de forma diversa. La flexibilidad interpretativa revela la construcción de significados distintos atribuidos al mismo artefacto y el modo en que uno, o una combinación

de ellos, se vuelve dominante. Si esto acontece, una función del artefacto predomina y, con ello, alinea interpretaciones sobre él mismo, que producen el debilitamiento de la controversia, estabilizando uno de los sentidos del artefacto.

Teóricamente, todos los artefactos son objeto de flexibilidad interpretativa y siempre son posibles nuevas interpretaciones. En la práctica, sin embargo, el fenómeno de clausura implica que algunas de las interpretaciones particulares se transforman en dominantes, y que así se crean y estabilizan las trayectorias de los artefactos [...]. El concepto de clausura es un complemento significativo de estos términos. Permite observar los procesos a través de los cuales se crean los paradigmas tecnológicos y las trayectorias (Bruun y Hukkinen 2008, 196-7).

Los estudios sobre controversias revelan los procesos que conducen a la construcción y funcionamiento del artefacto. A través de las controversias se pueden identificar los reclamos de los grupos sociales relevantes sobre las estrategias, las debilidades y las imposiciones de sus oponentes. Por ello, quienes investigan deben recopilar amplia información sobre los procesos en los periodos de controversia, para actuar, simétricamente, tanto con quienes tienen éxito al posicionar sus intereses, como con quienes fracasan y son excluidos de la resolución del problema (Sismondo 2010). Dichas controversias ofrecen, también, una ventaja metodológica, pues revelan rápidamente la flexibilidad interpretativa de los actores implicados y resulta más fácil recuperar las fuentes textuales (Pinch y Bijker 2008). Así, a medida que las controversias disminuyen es más difícil encontrar las huellas de los actores y su voz disidente. Collins (1981) denomina núcleo central (*core set*) a los grupos de controversia, con ello se refiere solo a los científicos que están involucrados activamente en la experimentación y observación de un fenómeno, y a los que realizan contribuciones a la teoría del fenómeno o al experimento.¹

¹ Aunque es difícil definir quién está dentro o quién está fuera del núcleo central, Collins evita hablar de grupos porque el término remite a la interacción necesaria que los actores deben mantener entre ellos y a un sentido de diferenciación con los que están afuera. En cambio, el término núcleo no implica necesariamente interacción frecuente, incluso permite que formen parte los actores que tienen posiciones contrarias, pero que actúan a través de terceros en estructuras formales. Los núcleos centrales son efímeros y funcionan mientras dura la controversia, el patrón usualmente tiene que ver con entrar en la disputa, hacer contribuciones (usualmente negativas) y salir rápidamente (Collins 1981, 8-13).

El principio de simetría desarrollado por el “programa fuerte” de la sociología del conocimiento científico plantea utilizar el mismo repertorio conceptual para cada lado de la controversia, e implementar el mismo tipo de causas o las creencias en los grupos en controversia. El investigador debe seguir el curso de la controversia hasta su clausura y recuperar los factores sociológicos que explican cuáles ideas se estabilizan como verdaderas y cuáles como falsas, estudiando los aspectos tecnológicos en el mismo nivel que se estudian los aspectos sociales de la controversia (Martin y Richards 1995).

El funcionamiento y la falla de los artefactos son construcciones sociotécnicas que deben ser estudiadas simétricamente, a través de los elementos heterogéneos, parte de los procesos de adecuación de respuestas/soluciones tecnológicas. En estos intervienen elementos heterogéneos como los sistemas, los conocimientos, las condiciones materiales, las regulaciones y el financiamiento (Thomas 2008).

El conocimiento generado en esos procesos problema-solución es en parte codificado y en parte tácito (o solo parcialmente explícito): signado por prácticas cotidianas, desarrollado en el marco de procesos cotidianos y no siempre formales de toma de decisiones [...]. El “funcionamiento” de un artefacto sociotécnico es un proceso de construcción continua, que se despliega desde el mismo inicio de su concepción y diseño. Aún después de cierto grado de “estabilización”, se continúan realizando ajustes y modificaciones que construyen nuevas y diversas formas de funcionamiento (Thomas 2008, 257-8).

Explicar los procesos de resolución de problemas es un aspecto esencial para comprender el cambio tecnológico como una construcción sociotécnica situada. Las controversias, además de mostrar la flexibilidad interpretativa y los procesos de solución de los problemas, también están relacionadas con procesos de aprendizaje de los actores, con la resignificación de la tecnología y con las trayectorias sociotécnicas.

Los actores involucrados en la controversia utilizan distintas herramientas para convencer a los otros del propósito del artefacto que defienden. La retórica es un instrumento poderoso para posicionar los intereses del núcleo central. En esta obra, sostengo que el código y la

norma legal funcionan como mecanismos eficaces para imponer los propósitos del artefacto desde el núcleo y dominar la controversia. La retórica tiene la función de convencer a los otros de la legitimidad de la posición del núcleo, y de la ilegitimidad de aquellos que se oponen; un modo de legitimar la posición del grupo es apelar a las normas de la conducta científica o tecnológica, cuestionando las posiciones obtusas de los oponentes ante los nuevos propósitos del artefacto. Deslegitimar al otro es parte fundamental de la retórica tecnológica, la estabilización del artefacto implica apelar a sus aspectos sociales, históricos, económicos y filosóficos.

No importa si se trata de ingenieros, inversionistas o consumidores, todos enfrentan opciones ante las tecnologías, no existe un contexto independiente que resuelva qué es mejor. Ellos enfrentan opciones que se debaten entre intereses, objetivos, reclamos, imágenes y potenciales artefactos. La elección se vuelve más compleja cuando hasta la más mínima característica técnica de los competidores entra en disputa [...]. Los asuntos tecnológicos tienden a involucrar al público de forma más directa que los asuntos científicos, y los actores externos pueden involucrarse rápidamente en controversias tecnológicas. Cuestiones particulares sobre las capacidades y características tecnológicas pueden convertirse en temas a ser resueltos por no expertos al igual que por expertos (Sismondo 2010, 128).

El fin del debate y de la controversia puede darse a través de varios mecanismos. Uno es fortalecer los acuerdos entre grupos (núcleo central), pues este consenso puede terminar oficialmente la controversia, incluso cuando algunos grupos no se alinean con los intereses de los grupos dominantes. En tal caso, los grupos disidentes pueden mantenerse y adoptar estrategias alternativas para definir el propósito del artefacto. Un segundo mecanismo utilizado para estabilizar una versión del artefacto es distinguir el valor pragmático y la legitimación. Una interpretación del artefacto puede volverse dominante porque el modelo de uso y de construcción se impone, sin importar cuán válido sea para los disidentes. Finalmente, otro modo de clausurar una controversia es enfatizar en que el problema de los disidentes no es representativo para la comunidad que co-construye el artefacto.

Las controversias develan las tensiones entre los individuos como sujetos autónomos y las necesidades de las comunidades; reflejan, asimismo, las relaciones ambivalentes entre la ciencia y la tecnología con otras organizaciones como los sistemas regulatorios, las empresas y los medios de comunicación (Nelkin 1995). Permiten también descubrir otras perspectivas de la política de la tecnología, como las tensiones entre los valores morales que se le atribuyen a los artefactos sociotécnicos, al igual que las prácticas de resistencia y domesticación ejercidas por los actores. Los fallos en el sistema de confianza, que la tecnología debió construir, desatan cuestionamientos de tipo político y moral sobre el rol del artefacto sociotécnico, especialmente en la clase media.² Estos cuestionamientos, además, tienden a organizar demandas legales que giran alrededor de la violación de los derechos de los individuos y a enrolar a los medios de comunicación dentro de la controversia. La retórica sobre la tecnología, cuando esta se considera un atentado contra los derechos de las personas, funciona muy bien como una estrategia que contribuye a volver más visible la demanda en la opinión pública, ganar apoyo político y elevar la base de la negociación (Nelkin 1995).

En cada una de las controversias presento la voz oficial de Facebook a través de su sala de prensa y su blog oficial; la voz de los usuarios opinando en los grupos de defensa de la privacidad de Facebook y el blog; la voz de los activistas, a partir de las demandas realizadas a Facebook en Estados Unidos y Europa; la voz de los gobiernos, reflejada en los casos canadiense e irlandés. Finalmente, empleo las notas de prensa sobre cada una de las controversias, una fuente para estudiar cómo representan la privacidad los actores que logran presencia mediática.

News Feed: la primera controversia sobre la privacidad en Facebook

La primera controversia sobre privacidad que se ocasionó en Facebook surgió a partir del cambio de la arquitectura de la red social. En el nuevo Facebook, en septiembre de 2006, se creó una página de ingreso, previa

² Según Nelkin (1995, 450), gran parte de los activistas involucrados en disputas de ciencia y tecnología son individuos educados de clase media, con suficiente seguridad económica y destrezas políticas para participar en movimientos sociales.

a los perfiles personales que publicaban información generada por el Social Graph de los usuarios. Esta nueva página puso al alcance de cada usuario información que antes solo era visible en los perfiles personales de los “amigos”, y que debía buscarse manualmente a voluntad.

Días antes de los cambios, Zuckerberg escribió a los miembros de Facebook:

Cuando hemos hecho cambios en el pasado, mucha gente nos ha escrito molesta pidiéndonos volver a la antigua versión de Facebook. Los cambios pueden ser desorientadores, pero los realizamos porque estamos seguros de que vuelven mejor al sitio. Puede que se sienta diferente al principio, pero cosas como fotos, eventos, grupos y el muro han vuelto a Facebook más útil e interesante. Nuestro objetivo es proveer herramientas que ayuden a la gente a comprender qué sucede a su alrededor y todo lo que añadimos está enfocado en este sentido. Las nuevas cosas que vamos a lanzar harán lo mismo.³

News Feed debía ser un éxito según el criterio de sus diseñadores, pues propiciaba un principio de transparencia que se expresaba en un flujo más eficiente de la información producida por los usuarios y compartida entre amigos.

¿De qué modo una información que se había producido en un contexto público podía ir en contra de la privacidad de los usuarios? Los usuarios tenían un “sentido” de la privacidad distinto al construido por el equipo de diseñadores de Facebook; lo que para los escritores de código era “transparencia”, para los usuarios era “acoso”. El código había cambiado el contexto en el cual las prácticas sociales tenían lugar. Si bien los contenidos que News Feed ponía en circulación habían sido previamente colgados en los perfiles de los usuarios, no se habían escrito en el contexto público-masivo que News Feed imponía a los miembros de la red. La prensa definió a News Feed como un mecanismo que permitía a los usuarios

rastrear los movimientos de sus amigos minuto a minuto [...], para muchos usuarios esto es demasiado [...] por naturaleza News Feed es intrusivo y eso es lo que molesta a los estudiantes, pues una cosa es chequear

³ En <https://blog.facebook.com/blog.php?q=Zuckerberg+2006>

lo que hacen los amigos entre clases y otra ser inundado con información no buscada [...] algunos periódicos universitarios tienen como portada “Facebook te está observando” o “Furiosos con Facebook”.⁴

En cuestión de horas, los usuarios se organizaron para protestar contra News Feed. Paradójicamente usaron la aplicación de grupos de Facebook para ello. “Facebook aparentemente decidió hace unas horas convertirse oficialmente en un libro de acoso; no hay que hacer ningún esfuerzo para rastrear a los amigos o conocidos en cada movimiento que hacen en internet. Gracias gran hermano, gracias”.⁵

Así, muchos estudiantes reclamaron que su privacidad había sido invadida porque el cambio de la arquitectura de Facebook afectaba sus expectativas de privacidad, circunscritas a sus perfiles, al muro y a los grupos. “Quedé conmocionado cuando vi la cantidad de información que News Feed entregaba y no estoy de acuerdo con el hecho que los usuarios no podamos cambiar lo que aparece en News Feed” (Stutzman 2006, en línea).

La primera reacción de Zuckerberg (2006b) fue de sorpresa; en el blog oficial de la compañía escribió su respuesta pidiendo tranquilidad. No obstante, el 5 de septiembre de 2006, más de 750 000 usuarios firmaron una petición en línea solicitando a los administradores de Facebook.com lo siguiente:

Visto que Facebook.com es el sitio web de la red social y una compañía privada iniciada por Mark Zuckerberg en febrero de 2004;

Visto que Facebook.com es una herramienta útil y entretenida para sus miembros;

Visto que los usuarios de Facebook.com apoyan la filosofía de la red de ayudar a la gente a compartir información a través de las redes sociales;

Visto que los usuarios de Facebook.com entienden los controles de privacidad y su rol de proteger la información personal y privada;

Visto que los cambios dramáticos que se hicieron el 5 de septiembre de 2006 en Facebook.com, incluidos la introducción de News Feed y de Mini Feed ponen en riesgo la seguridad y la privacidad de sus más de 9 millones de usuarios;

⁴ *Times*, 6 de septiembre de 2006.

⁵ En <http://under-pressure.livejournal.com/318712.html>

Visto que se ha producido una oposición sin precedentes a dichos cambios dentro de la comunidad;

Visto que muchos usuarios se sienten incómodos participando en Facebook.com por los cambios realizados, hasta el punto de que algunos han desactivado sus cuentas;

Nosotros, los usuarios de la comunidad de Facebook.com:

Pedimos a los administradores de Facebook.com comunicar activamente y consultar con los usuarios dentro de un diálogo democrático, los cambios actuales y los futuros.

Y demandamos el retiro inmediato de News Feed y de Mini Feed de Facebook.

O:

Permitir que los individuos se retiren del uso de News Feed y de Mini Feed en las páginas de otros.

Permitir que los usuarios den de baja su News Feed y su Mini Feed de sus perfiles personales.

Atentamente,

Los que firman a continuación.⁶

Con un texto más calmado, Zuckerberg contestó un día más tarde.

Carta abierta de Mark Zuckerberg

Esta vez sí que la fastidiamos. Cuando lanzamos News Feed y Mini Feed estábamos intentando entregarles un flujo de información sobre su mundo social. En cambio, hicimos un mal trabajo explicando las nuevas características, e hicimos un trabajo todavía peor al no entregarles control sobre ellas. Quisiera corregir estos errores ahora. Cuando creé Facebook hace dos años mi meta era ayudar a la gente a entender mejor lo que ocurría en su mundo. Quería crear un entorno donde la gente pudiera intercambiar la información que quería. Creo que gran parte del éxito que hemos tenido se debe a esos principios básicos. Hicimos el sitio para que los miembros fueran parte de redes pequeñas como las universidades, las compañías o las regiones, para que pudieran ver solo los perfiles de las personas que están en sus redes y sus amigos. Lo

⁶ "Petition: Facebook, stop invading my privacy", página de Facebook, acceso el 22 de marzo de 2011. <https://www.facebook.com/group.php?gid=5930262681&ref=share> (contenido no disponible).

hicimos así para asegurarnos que pudieran compartir la información con las personas que les importan. Es por ello que construimos controles de privacidad extensivos –para darles más control sobre la información que comparten y con quien–. De algún modo olvidamos este punto en News Feed y en Mini Feed y no construimos los controles de privacidad apropiados inmediatamente. Este fue un gran error de nuestra parte y lo siento mucho. Pero pedir disculpas no es suficiente. Quise asegurarme de tomar cartas en el asunto y no hemos dejado de escribir códigos por dos días para darles mejores controles de privacidad. Esta nueva página de privacidad les permitirá escoger qué tipos de historias pueden ir en su Mini Feed y en el News Feed de sus amigos. También crea listas de los tipos de acciones que Facebook no permitirá que otros conozcan. Si tienen más comentarios, por favor envíenlos. Puede parecerles tonto, pero quiero agradecer a todos los que han escrito y han creado grupos para protestar. Aunque espero no haberlos enojado demasiado, estoy muy contento de escucharlos. También estoy contento de que News Feed haya resaltado estos grupos de modo que la gente pudiera encontrarlos enseguida y compartir sus opiniones entre sí. Hace una semana creé un grupo llamado Libre flujo de información en Internet, porque creo que puedo ayudar a la gente a compartir su información. Les pido que lo vean y aprendan más sobre lo que guía a quienes hacemos Facebook. Hoy (viernes 9/8) a las cuatro de la tarde estaré en el grupo con un grupo de personas, y me encantaría discutir con ustedes. Gracias por tomarse el tiempo de leerme, Mark (Zuckerberg 2006a, en línea).

En la controversia de News Feed estaba en juego la comprensión del artefacto desde adentro. Para advertir cuál es el propósito del artefacto es necesario explicarlo como un sistema social y abrir su caja negra. News Feed había transformado el artefacto con el propósito de volver más visible la acción de los sujetos en Facebook; con ello condicionó los comportamientos de los usuarios dentro de la red al exponerlos a flujos más agresivos de contenidos sobre su Social Graph. De las palabras de Zuckerberg deduzco que Facebook, hasta ese momento, era imaginada como pequeñas redes de amigos, limitadas a contextos específicos (universidad, la compañía, la región). Las expectativas de privacidad que se ofrecía a los miembros tenían que ver directamente con este contexto. News Feed introdujo cambios sustanciales al propósito del artefacto (Bruun y Hukkinen 2008), pues lo

volvió más transparente y abierto. El uso focal del artefacto cambió, y con ello, también el acuerdo sobre cómo funcionaba la privacidad dentro del entorno virtual. La controversia apareció con el nuevo propósito del artefacto, justamente porque este fue definido socialmente entre los grupos que le otorgaban sentido (Pinch y Bijker 2008).

News Feed mostró el momento del cambio tecnológico y cómo este provocó una elevada flexibilidad interpretativa del artefacto. El nuevo código lo reconfiguró y ello conllevó a nuevas construcciones de sentido de la red social, lo que dio paso a una serie de negociaciones entre los actores, para consensuar el nuevo sentido que tendría la privacidad en Facebook. Esta controversia reveló los reclamos de los grupos sociales relevantes, sus estrategias y los nuevos sentidos del marco tecnológico, estabilizados por quienes tenían el poder de imponerse. Develó también qué se reclamaba, cómo se argumentaba y qué se negociaba sobre la privacidad en aquel momento.

El *contexto* que Facebook ofrecía, en palabras de Zuckerberg, era el de redes diferenciadas para grupos específicos. Sin embargo, este contexto se construye de modo diferente dependiendo del grupo social relevante. Para los escritores de código, Facebook era un artefacto móvil en crecimiento, que se rige por una premisa que mueve al mundo: la transparencia. Según Zuckerberg, Facebook no podía “resistirse a la trayectoria que el mundo está siguiendo porque podría volverse obsoleto” (Kirkpatrick 2010, 201). Para los usuarios, en cambio, se trataba de un espacio virtual de encuentro entre amigos con una referencia contextual fuera de la red: la universidad, los compañeros de clase, los amigos de la ciudad. La información producida se construía en ese contexto y no en cualquier otro. El cambio desde una red construida conscientemente por los miembros alrededor de sus interacciones, a un “libro de acoso”, muestra que el código genera un contexto nuevo frente al que los usuarios reclaman la exhibición de sus representaciones.

Esta primera controversia ocurrió entre programadores y usuarios. Los *reclamos* de los usuarios estuvieron relacionados, en primer lugar, con la *invasión a sus expectativas de privacidad*, la nueva arquitectura transformaba a Facebook en una gran vitrina de información de los otros y de sí mismos que se volvía *invasiva* y *acosadora*. El flujo de información de *News Feed* fue percibido como un riesgo a la privacidad y como una falta de

control sobre los contenidos producidos por los usuarios. Por su parte, los escritores de código reclamaron porque sí habían pensado en la privacidad de los usuarios desde el inicio y manifestaron estar orgullosos de haber apostado por la privacidad, a diferencia de otras redes como Friendster o MySpace, que produjeron un modelo de red social más abierta y pública.

Zuckerberg enfatizó que el éxito de Facebook se debe, en parte, a los “controles de privacidad extensivos” que se crearon para dar más dominio a los usuarios sobre qué información comparten y con quién, como lo afirmó en su carta abierta a propósito del incidente de News Feed. El problema radica en que se empezaron a crear las condiciones de transparencia a través de un estilo tecnológico que condiciona a los usuarios a adaptarse a nuevos parámetros. Según Zuckerberg, Moskovitz, Hughes y Kelly la transparencia contribuye a crear un mundo mejor y una sociedad más tolerante, porque es más difícil engañar al otro y esto vuelve más responsables a las personas: “Hemos sido capaces de construir una versión de internet más segura, al confrontar a las personas a hacerse cargo de las consecuencias de sus acciones al requerirles utilizar su verdadera identidad” (Kirkpatrick 2010, 201).

Tabla 2. Flexibilidad interpretativa de News Feed

Usuarios	Programadores
Faltan controles de privacidad.	No existe otra red social con más controles sobre la privacidad que Facebook.
News Feed invade las expectativas de privacidad porque cambia el contexto en el que se genera la información.	News Feed vuelve público lo que ya era público.
News Feed acosa y es invasiva.	News Feed es una oportunidad de compartir más información entre amigos.
Debe ser optativo usar News Feed.	News Feed es una característica de Facebook y es parte de su arquitectura.
Facebook debía consultar a los usuarios sobre cualquier cambio.	Facebook debía mejorar sus estrategias para comunicar los cambios.

Los usuarios se organizaron y *negociaron* su permanencia en el sitio. Primero, formaron grupos en contra de la nueva característica de la arquitectura de la red social y con ello alcanzaron publicidad, dentro y fuera de la red. Luego firmaron una petición a Facebook de volver optativo el News Feed, y tener mayor control sobre la información que circula en este nuevo espacio.

Esta primera controversia sobre privacidad fue el precedente de cómo iba a definirse, posteriormente, la privacidad en la red social. El centro de debate fue una característica del sitio que cambiaba las reglas del juego sobre los modos de habitar un lugar en el ciberespacio. El código define ese lugar, lo construye con una serie de elementos que distinguen entre lo público y lo privado; luego espera que los usuarios se adapten, que configuren normas sociales que ayuden a habitar estos lugares de forma colectiva. Si el perfil era público, News Feed lo volvía más público. Si los mensajes del *inbox* son privados, News Feed no los toca. Pero aquello que ya se ha consensuado como público puede ser actualizado minuto a minuto y con ello ser más visible para la red social. News Feed fue el punto de quiebre, desde una red cerrada a una abierta, en función de la norma social. Si los usuarios se adaptaran a que la información que producen circule sin su control, el principio de transparencia radical podría de ser implementado.

Los usuarios negociaron dos temas: tener más control sobre la información que circula en News Feed y que su participación en este sea voluntaria. “Tal vez para mañana tengamos una característica en Facebook que nos permita salir de News Feed, basada en las categorías. Este grupo se reserva su juicio hasta que las actualizaciones de privacidad se implementen. Creo que ganamos gente, creo que ganamos” (Parr 2008, en línea).

En el proceso de la negociación, los controles de privacidad fueron lo único que Facebook admitió que entrara en juego, pero no si News Feed fuera optativo o no. El código rediseñó el contexto del lugar virtual sin vuelta atrás, lo que tuvo consecuencias importantes sobre cómo imaginar la privacidad dentro de Facebook.

El proceso de co-construcción muestra que las normas sociales producidas dentro de Facebook son el producto de negociaciones entre las capas sociales y las tecnológicas de la red; usuarios, *software*, programadores y

Zuckerberg transan las configuraciones de la actividad social. Los códigos sociales que funcionaron en el momento de la controversia son los códigos de estudiantes universitarios que, como el propio Zuckerberg, poco distinguían entre vida social y vida profesional. Reid Hoffman, uno de los primeros inversionistas de Facebook y fundador de LinkedIn, sostuvo que Zuckerberg no cree que la vida social y la vida profesional sean distintas, lo cual es una visión clásica de un estudiante universitario. Del mismo modo, Charlie Cheever, antiguo empleado de la compañía, pensó que “Mark no cree en la privacidad, la concibe más bien como un paso previo, que Facebook ofrece, hasta que los usuarios no la necesiten más” (Kirkpatrick 2010, 202). Sheryl Sandberg, directora de operaciones de Facebook, tenía otra mirada.

Mark realmente cree mucho en la transparencia y en la visión de una sociedad más abierta y de un mundo más abierto, de modo que presiona a la gente hacia allá. Yo creo que él también entiende que el modo de llegar ahí es darle a las personas un control granular y confort. Él espera que te vuelvas más abierto y se alegra de ayudarte a serlo. Para él, es más un medio que un fin en sí mismo. Yo no estoy muy segura de ello (Kirkpatrick 2010, 207).

El código de News Feed cambió las convenciones sociales y los comportamientos de las personas, los usuarios intuyeron los riesgos de la transformación del contexto pero no lograron entender los controles que la nueva tecnología iba a ejercer. Son los programadores los que definen si la privacidad será protegida, porque son ellos quienes construyen la naturaleza de Facebook; el problema es que no estamos entrenados para pensar cómo la tecnología es capaz de controlarnos y esto es lo que confunde nuestra intuición peligrosamente (Lessig 2006, 31-2). Los usuarios son parte fundamental de los procesos de co-construcción de la evolución de Facebook como empresa, repositorio de estilos de vida y de socialización global. No obstante, en el caso de la privacidad, sus capacidades de co-construcción fueron dirigidas por el propio Zuckerberg.

Esta primera controversia se decidió con nuevos controles de privacidad. Los reclamos sobre acoso, intrusión, expectativas de privacidad o cambio de entorno se evaporaron una vez que los administradores y

codificadores de Facebook lograron estabilizar la noción de privacidad dentro del campo de la información, y de responsabilizar a los propios usuarios de su deseo de saber más sobre los otros.

Facebook tiene severos problemas de privacidad en una admirable y comprensible arquitectura de protección de la privacidad. La mayoría de problemas de privacidad son consecuencias naturales de los modos entusiastas en que la gente usa Facebook. Hay una tensión profunda y probablemente irreconciliable entre el deseo por un control confiable sobre la propia información y el deseo de una interacción social no planificada [...]. La violación de la privacidad que ocurre en Facebook se debe en gran medida al comportamiento de las personas y a sus prácticas de “peer-to-peer privacy violations” (Grimmelmann 2009, 1137).

Facebook ofrecía más controles de privacidad que cualquier otro sitio en línea. Según D’Angelo,⁷ representaba un “nuevo modelo de información, cada pieza de información en Facebook está protegida por restricciones que indican quién puede verlas y quién no. Ciertos grupos de personas pueden ver ciertas piezas de información, y este control granular no se encuentra en ningún otro lado de internet” (Kirkpatrick 2010, 208). Desde la compañía, se pensaba que Facebook no había atentado contra la privacidad de ningún usuario, el verdadero problema era la estrategia sorpresiva que precedió a News Feed. Zuckerberg reconoció que se hizo un mal trabajo explicando las nuevas características y ofreció el elemento sobre el que estaba dispuesto a negociar: el control sobre la nueva característica. Es decir, el usuario tendría control sobre la información que considerara pública, pero no la opción de entrar o salir de News Feed.

La privacidad no es el estado de un objeto inanimado o de un grupo de bytes, la privacidad es un sentido de vulnerabilidad que un individuo experimenta cuando negocia su información. Los usuarios de Facebook se sintieron expuestos, si no invadidos, por el cambio de arquitectura sin tener una buena vía de articulación porque los hacía sentir raros (boyd 2008a, 14).

⁷ Amigo de Zuckerberg desde el colegio y socio programador desde la adolescencia.

La diferencia entre datos publicados y agregados era muy grande en News Feed, porque los usuarios debían cambiar sus patrones de conducta dentro de la red social y esperar que aquello que antes podía pasar desapercibido, ahora sería anunciado a todos, que cualquier acción podría ser transmitida a todos sus amigos digitales. Cuando el sistema es hiperpúblico, las personas no deben escoger simplemente qué es lo que quieren exponer, también deben definir todo lo que quieren esconder. El cambio del código transformó varios elementos en el “sentido” de privacidad que experimentaban los usuarios, como el contexto y la audiencia en el que se compartía información. En el ciberespacio el contexto es fundamental para producir normas sociales que guíen qué se puede compartir y con quién. Facebook, con este giro en la arquitectura, afectaba uno de los elementos fundamentales para construir un sentido de control sobre lo privado.

La idea de una identidad única, promovida por Zuckerberg para construir un mundo mejor, deja fuera las prácticas sociales en las que las personas se han entrenado para distinguir lo público de lo privado, al apelar a personalidades situadas en contextos diferenciados (Goffman 1981). Él promovía una convergencia social que los medios digitales han favorecido a gran velocidad, pero esta correlación anulaba las diferencias entre los comportamientos en el hogar o en la escuela. Desaparecía con ello la oportunidad que tenían las personas de comportarse de modo diferenciado como respuesta al contexto social en donde se encontraban. La convergencia social exige a las personas que se ajusten a distintas audiencias, de forma simultánea, sin tener un guion social para hacerlo; en este sentido, el código se convierte en un elemento de sostén de la norma social, en una directriz de lo que se puede, o no, en el ciberespacio y su función reguladora puede contribuir a generar nuevos sentidos de lo privado.

La convergencia social nos exige preguntarnos si la privacidad es algo que la sociedad todavía desea abrazar (boyd 2008b). Pocos años después de la controversia de News Feed, Ben Parr, el antiguo fundador del grupo “Estudiantes en contra del News Feed de Facebook” escribió:

El mayor cambio en estos dos años es que nos sentimos más cómodos compartiendo nuestras vidas y pensamientos instantáneamente a miles

de personas, amigos cercanos y extraños. El desarrollo de las nuevas tecnologías y el golpe de barco que dio Zuckerberg han provocado este cambio [...]. News Feed inició una revolución que requiere que demos un paso atrás para apreciarla. La privacidad no ha desaparecido, se ha vuelto más fácil de controlar, lo que quiero compartir lo comparto con cualquiera, lo que quiero mantener en privado lo mantengo en mi cabeza (Parr 2008, en línea).

Beacon: la segunda controversia sobre la privacidad en Facebook

Beacon fue un programa creado por Facebook y lanzado dentro de la red social el 6 de noviembre de 2007. Formaba parte del sistema de publicidad de la red y funcionaba como un servicio de alerta para las actividades de sus usuarios: juegos preferidos, compras en línea realizadas por los amigos en los sitios web que eran socios comerciales de Facebook (*tickets*, libros, *jeans*, cualquier cosa). Facebook utilizaba la información de los recorridos y las compras de los usuarios como una forma de publicidad que llegaba al Social Graph de cada usuario, alertándolos de las visitas y las compras que habían realizado en los sitios web socios de Facebook a través de Beacon. Una de las mayores fallas del servicio fue no solicitar la aprobación explícita del usuario para enviar la información de la compra al News Feed. Lo que mostraba era un menú con la opción de “no enviar la información”; si el usuario no paraba la alerta se la enviaba inmediatamente. El resultado fue que muchos usuarios ni siquiera notaron la alerta.

Beacon fue un programa diseñado de forma impecable, pues iba condicionando al usuario a tomar una decisión: que Beacon funcionara sin restricciones. Cada paso del código conducía a que el usuario permitiera que las compañías publicaran en su perfil la información de las compras que realizaba fuera de Facebook y se daba carta blanca a estas empresas para cosechar información pública dentro de Facebook (edad, lista de amigos, ciudad, sitios que visita, su estilo de vida). Beacon no ofrecía a los usuarios una opción “amigable y transparente” para impedir que funcionara. Todo lo contrario, si el usuario no deseaba usarlo, cada vez que realizaba una compra en línea debía seguir un procedimiento largo y tedioso hasta lograr que Beacon se desactivara.

El controversial sistema Beacon va mucho más lejos de lo que nadie hubiera imaginado al rastrear las actividades que los usuarios de Facebook hacen en internet. Beacon reporta a Facebook lo que sus usuarios hacen fuera de la red social, incluso cuando no están conectados a Facebook y han declinado que sus actividades se publiquen entre sus amigos [...]. Uno de los puntos que más preocupa es que los usuarios no saben que su información ingresa a Facebook y que no se les ha dado la opción de bloquear la información que Beacon transmite (Pérez 2007, en línea).

Las consecuencias no se hicieron esperar, en la prensa salieron cientos de historias sobre el carácter invasivo de la privacidad de sus usuarios. Listas de regalos de Navidad completas fueron publicadas en News Feed; muchas veces incluso añadían los descuentos conseguidos en cada producto. No solo la intrusión era mal vista, también preocupaba profundamente el mal uso que se estaba haciendo de la información de las personas. “Tal vez lo que más me sorprendió fue el modo en que se describía cómo Kongregate enviaba mi información sin preguntar por mi permiso, no hace falta decir que no estaba nada contento con que mis hábitos de navegación se mostraran en mi perfil de Facebook” (Martin 2010).

En agosto de 2008 se presentó una demanda contra Facebook y las compañías socias del sistema Beacon por el uso e intercambio de información personal sin la autorización de los usuarios. En tal sentido, Facebook ha sido poco transparente con sus miembros en el uso de la información con la que ellos nutren la red. Desde Beacon, los usuarios empezaron a fijarse, críticamente, en las políticas de privacidad de la red y a desarrollar un sentido legal que antes no poseían: “Ningún usuario de Facebook debería ver publicadas sus compras en línea sin un permiso explícito *opt-in*” (McCarthy 2007).

Los principios sobre los que centró Facebook la privacidad hasta ese momento fueron: los individuos deben tener el control sobre su información personal y deben tener acceso a la información que los otros quieren compartir. Estos principios delinearón el tipo de información que Facebook recogía y quién tiene acceso a ella.

La pregunta que deberíamos hacernos es si consideramos aceptable que alguien que está detrás de uno mientras navega en internet anote todo lo que ve y mantenga estas notas. ¿Confiarían en esa persona? Un ejemplo

del proceso es: 1. El usuario renta una película en línea en Blockbuster. 2. Blockbuster le pregunta en línea a Facebook si esa persona es su usuario. 3. Facebook responde que sí. 4. Blockbuster envía la película que el usuario solicitó en línea. 5. Facebook guarda esa información. Todo esto podría terminar si Blockbuster pregunta ¿es usuario de Facebook? Y si es así ¿le gustaría compartir la película que acaba de rentar con sus amigos? (Weiner 2007).

El grupo liberal político MoveOn.org lideró la protesta y miles de usuarios se sumaron. Otros grupos de activistas también empezaron su propia campaña en contra de *Beacon*, con demandas legales ante la Comisión de Comercio Federal. Buscaban que Zuckerberg ofreciera disculpas y que Beacon desapareciera. Adam Green, vocero de MoveOn.org, planteó:

Si el argumento de Facebook es que compartir información privada con cientos o miles de amigos no es lo mismo que volver “pública” la información, esto muestra que Facebook tiene un argumento muy débil [...]. Los usuarios de Facebook están muy molestos con que los libros, películas y regalos que ellos compran privadamente se desplieguen públicamente sin su permiso y ya es hora de que Facebook dé marcha atrás en esta violación de la privacidad (McCarthy 2007, en línea).

A diferencia de News Feed, Beacon fue un producto que permitió el mal uso de la información irrespetando los controles de privacidad de los que Zuckerberg estaba tan orgulloso. Sin embargo, por más de tres semanas no hubo respuesta de la compañía, pues estaban ocupados mirando cómo los usuarios reaccionaban dentro del sitio; se dieron cuenta de que Beacon no afectaba el comportamiento dentro del servicio. “No respondimos lo suficientemente rápido, estábamos acostumbrados a que la gente se quejara y que luego se diera cuenta de que habíamos estado en lo correcto. Pensábamos: ‘bueno, como sea, ¡con el tiempo lo superarán!’. Pero luego fue ¡ey no, esta vez sí que lo hicimos mal!” (Zuckerberg, citado por Kirkpatrick 2010, 249). Un mes más tarde de lanzado Beacon, el 5 de diciembre Zuckerberg escribió el siguiente comunicado.

Hace un mes lanzamos una característica llamada Beacon para ayudar a las personas a compartir información con sus amigos sobre lo que hacen en

línea. Cometimos muchos errores construyendo esta característica, pero nos hemos equivocado todavía más en cómo hemos atendido este problema. Simplemente hicimos un mal trabajo con este producto y pido disculpas por ello. Estoy desilusionado con nuestros errores y agradecemos toda la retroalimentación que hemos recibido de ustedes. Me gustaría discutir sobre qué hemos aprendido y cómo vamos a mejorar a Beacon.

Cuando pensamos en Beacon nuestro objetivo fue construir un producto que permita a las personas compartir información entre distintos sitios con sus amigos. Tenía que ser liviana de modo que no se interpusiera en el camino de las personas mientras navegaran en la web, pero también lo suficientemente clara para que las personas fueran capaces de controlar fácilmente lo que compartían. Estábamos emocionados con Beacon porque creemos que mucha de la información que la gente compartía no estaba en Facebook, y si lográbamos encontrar el balance adecuado, Beacon podía dar a las personas un modo fácil y controlado de compartir información con sus amigos.

Pero no logramos el balance adecuado. Al principio quisimos hacerlo muy liviano para que la gente no tuviera que tocarla para que trabajara. El problema con esta aproximación inicial para hacerla un sistema *opt-out* en vez de *opt-in* era que si alguien se olvidaba de negarse a compartir algo, Beacon lo compartiría con sus amigos. Nos tomó demasiado tiempo cambiar el producto luego de que las personas empezaron a contactarnos, de modo que ellas explícitamente aprobaran lo que querían compartir. En vez de actuar rápido, nos tomamos mucho tiempo en decidir la solución correcta. No me siento orgulloso del modo en que manejamos la situación y sé que lo podemos hacer mejor.

Facebook ha tenido éxito, en gran medida, gracias al control que les da a las personas sobre qué y cómo compartir su información. Esto es lo que hace a Facebook un buen producto, y para seguir siendo un buen producto Beacon necesita hacer lo mismo. La gente necesita poder escoger explícitamente lo que quiere compartir, y debe tener la posibilidad de eliminar a Beacon si no lo quieren utilizar.

Esta ha sido la filosofía detrás de estos cambios recientes. La semana pasada cambiamos Beacon a un sistema *opt-in* y ahora estamos volviendo a lanzar un control de privacidad para eliminar totalmente a Beacon.

Ustedes lo pueden encontrar aquí. Si seleccionan que no quieren compartir algunas de las acciones de Beacon, o apagan completamente a Beacon, entonces Facebook no guardará esas acciones incluso cuando nuestros socios las envíen a Facebook.

A nombre de todos quienes trabajan en Facebook, quiero agradecer la retroalimentación que hemos recibido sobre Beacon en las últimas semanas y espero que los nuevos controles de privacidad se hagan cargo de todos los temas que ustedes nos han solicitado.

Gracias por tomarse el tiempo para leer esto. Mark (Zuckerberg 2007a, 2007b, en línea).

Beacon afectó el crecimiento de Facebook en los siguientes meses. A la compañía de Zuckerberg le tomó un tiempo volver a tener los índices de ingreso de usuarios que mantenía antes del lanzamiento de esa conflictiva “característica”. El proyecto fue devastador para la compañía “para el tiempo en que arreglamos Beacon, ya se había corrido la voz que la gente no controlaba el flujo de su información; realmente lo arruinamos, le tomó mucho tiempo a nuestra marca crecer luego de ello” (Dan Rose, jefe de marketing de Facebook, citado por Kirkpatrick 2010, 250).

Las compañías socias del sistema Beacon dieron un paso atrás, Blockbuster, Sony Online Entertainment, eBay, New York Times, entre otras, sostuvieron que “hay un umbral que el programa debe alcanzar, en cuanto a privacidad, antes de que lo volvamos a activar” (Pérez 2007, en línea). Como compañías asociadas también tienen una responsabilidad sobre los usos de la información de sus propios usuarios, y esto llevó a gran parte de estas a analizar a Beacon y a no utilizarlo hasta que los problemas de privacidad se resolvieran.

Blockbuster fue demandada por Cathryn Elaine Harris por violar el Acta Federal de Privacidad de Video, al no solicitar su consentimiento escrito para compartir la información de las películas rentadas con su red de amigos de Facebook. Facebook tuvo que afrontar una demanda similar en California donde se falló el caso con 9,5 millones de dólares de reparación, el apoyo de Facebook para la creación de una organización no gubernamental de protección a la privacidad, y el cierre definitivo de Beacon. Desapareció de la red, pero muchas de sus características

se retomaron con la introducción de las aplicaciones y con el intercambio automático de información en Yelp, Pandora y Docs.com. Otras volvieron a reproducirse dentro de los controles de privacidad (tabla 3). Y la última herencia de Beacon fue el mecanismo complejo a seguir por parte de los usuarios para mantener menos pública su información.

Tabla 3. Controles de privacidad a raíz de Beacon

Información del usuario	Control público “todos”
Sobre mí	Opt-out
Actividades	Opt-out
Intereses	Opt-out
Favoritos	Opt-out
Miembros de familia	Opt-out
Estado de relación	Opt-out
Interesado en	Opt-out
Buscando	Opt-out
Colegios y universidades	Opt-out
Lugar de trabajo	Opt-out
Vínculos	Opt-out
Notas	Opt-out
Fotos	Opt-out
Videos	Opt-out

La controversia de Beacon incluyó a más actores que la de News Feed. No solo los usuarios intervinieron en los reclamos, también las compañías socias de Beacon afrontaron las consecuencias de las demandas legales y, con ello, entran a la controversia las cortes, las organizaciones de defensa de la privacidad y los medios de comunicación.

Las nociones que se empezaron a clausurar alrededor de la privacidad tienen que ver con la información y el control de los datos. Las

versiones vinculadas a un problema técnico y a las expectativas de privacidad no son compartidas por todos los grupos sociales relevantes, lo cual está relacionado, en gran medida, con la forma en que los usuarios significan sus acciones en el ciberespacio (tabla 4).

Tabla 4. Nociones de privacidad a raíz de Beacon

Grupos sociales relevantes	Nociones de privacidad				
	Información	Intrusión	Problema técnico	Control sobre los datos	Expectativas de privacidad
Facebook	x		x	x	
Usuarios	x	x		x	x
Activistas	x	x	x	x	x
Cortes	x		x	x	
Medios	x	x		x	x

Habitar el ciberespacio implica generar y compartir contenidos; Facebook es, básicamente, un espacio hipertextual mediado por la escritura y la imagen. Cada acción de los individuos en el ciberespacio debe materializarse en un soporte para existir. La novedad de Beacon fue que intervino en las acciones que realizaban los individuos, sus trayectorias en el ciberespacio, sus preferencias de búsqueda y sus elecciones sobre lectura, música, videos... Ya no concernía solo a la información generada por los usuarios dentro de sus perfiles, grupos, muros o aplicaciones favoritas; Beacon intervino en la materialización de los recorridos, las huellas específicas, los rastros de los que la mayoría de usuarios no tenía conciencia. Para ellos Beacon no fue un problema técnico, fue un atentado al sistema de confianza construido con la red social, un problema de expectativas de privacidad, porque aquello que Facebook desvelaba no tenía nada que ver con sus acciones dentro de la red social, sino de sus actividades afuera. Sin embargo, hay un guion cognitivo (Akrich 1992) importante que salta en esta controversia y que es parte del cierre de la polémica desatada por News Feed: cómo los usuarios instalan en sus sistemas de creencias

la noción de privacidad vinculada al control de su información. Por ello, parte importante de la negociación fue lograr que Facebook les otorgara herramientas de control sobre su información.

Los activistas y las cortes manejaron códigos similares, fundamentados en la jurisprudencia y en las leyes sobre privacidad. En este sentido, el problema de Beacon estuvo relacionado con la violación de la ley del Acta Federal de Privacidad de Video, y con el hecho de no diferenciar entre la información compartida y la información que publica. Según los términos de las mediaciones legales de Beacon, los usuarios no deseaban compartir la información que Facebook publicaba en las redes de sus amigos sin su consentimiento explícito. El problema era técnico y legal porque se vinculaba con la recolección, uso y difusión de datos personales a través del sistema Beacon y porque atentaba contra el derecho a la privacidad de las personas. Una noción de privacidad fundamentada en la autodeterminación informacional.⁸

Los medios recogieron básicamente las versiones de los usuarios, los activistas y Facebook, sin abordar el problema de la privacidad desde su base tecnológica. Así recalcaron los riesgos que Beacon representaba para la libertad de las actividades que los usuarios realizaban en línea.

El proceso de *negociación* de Beacon fue judicial, se cerró en 2009, de la mano de una mediación en una demanda legal. El principio que estaba detrás de Beacon fue implementado, al poco tiempo, a través de Facebook Connect, sin que ello fuera una fuente de controversia para los usuarios: compartir información dentro de Facebook sobre acciones realizadas fuera de este artefacto. Beacon es un punto de referencia de cuando los usuarios todavía consideraban importante que sus hábitos y sus intereses no se desplegaran ante sus amigos sin su consentimiento explícito. Hasta Beacon, este nivel de transparencia era considerado una violación de la privacidad de los individuos.

Sin embargo, la arquitectura de Beacon abrió la puerta a otras formas de habitar la red social que se tornaran atractivas para los usuarios.

⁸ Es interesante anotar que parte del acuerdo que Facebook realizó para terminar con Beacon, el año 2009, con la entrega de 9,5 millones de dólares para crear una fundación de protección de la privacidad, fue que Facebook tenía la capacidad de colocar un director en la junta de la fundación y de lograr construir la agenda sobre privacidad que la organización tenía a su cargo (Caso n.º 5:08-cv-03845-RS United States District Court Northern District of California San Jose Division).

Del mismo modo que News Feed atacó un sentido de lo privado, que luego fue superado por los miembros de Facebook a favor de las regulaciones que el artefacto propuso, Beacon fue un límite que Zuckerberg le imprimió al artefacto sociotécnico para probar hasta dónde los usuarios eran capaces de ceder en sus expectativas de privacidad. La negociación de esta controversia implicó el cierre de Beacon, pero aseguró la permanencia de las normas que iban a regir los comportamientos de los usuarios para implementar el principio de transparencia radical. Facebook cambió una característica técnica por otra y con ello intentó convencer a sus usuarios de que eran escuchados; sin embargo, en realidad, lo que Facebook hizo fue balancear la forma en que circulaba la información, y el sentido de control que debían tener los usuarios sobre sus contenidos. No cambió qué se compartía, sino cómo se hacía: a través Facebook Connect, un sistema más opaco revestido de controles de privacidad.

La noción de privacidad se transformó cuando el artefacto logró que las normas sociales dentro de Facebook se volvieran más permisivas y aliadas a la exhibición de los contenidos que generaban los usuarios, pero también a las actividades que realizaban, a sus hábitos, a sus gustos, expresados en datos dentro de la red social. El reclamo original dentro de esta controversia se resolvió al cambiarlo por otro (Bijker 1995; Thomas 2008).

Existe una íntima relación entre los procesos de aprendizaje, de resignificación de tecnologías y las trayectorias sociotécnicas [...]. El conocimiento generado en estos procesos problema-solución es en parte codificado y en parte tácito (o solo parcialmente explicitado): signado por prácticas cotidianas, desarrollado en el marco de procesos cotidianos y no siempre formales en la toma de decisiones (Thomas 2008, 257).

Facebook intentó circular información sobre los individuos más allá de la generada por mano de los usuarios en sus perfiles, muros y grupos. Los usuarios se resistieron al cambio porque sintieron invadida su privacidad y que sus razonables expectativas de privacidad habían sido afectadas. Mantener el sistema de circulación de la información propuesta por Facebook, y evitar que los usuarios sintiesen violentada su privacidad es una contingencia que Facebook debe construir en términos sociales, tecnológicos y culturales. Para funcionar en este nuevo escenario, las características del

artefacto deben estar relacionadas con las subjetividades de los actores implicados en la controversia. El cierre de una controversia tecnológica no requiere la “resolución del problema” en sentido literal, sino que los grupos sociales relevantes consideren el problema resuelto (Pinch y Bijker 2008). Con el cierre de Beacon los usuarios pensaron que se superaba el problema de invasión de la privacidad. Uno de los grupos sociales relevantes alcanzó a clausurar la controversia al alinear las interpretaciones del artefacto (Bijker 1995).

Puesto que Facebook logró reducir al mínimo la noción de privacidad, el cierre de Beacon fue la solución adecuada para que las cortes, los activistas, los medios de comunicación y los usuarios considerasen que se podía resolver el problema sobre privacidad que se había generado. Lo que se vuelve opaco en esta clausura es la manera en que Facebook persistió en el objetivo que ocasionó la controversia: redefiniéndolo a través de Facebook Connect y del Social Graph de cada usuario. La variante en la subjetividad de los usuarios es lo que permitió que Facebook Connect pasara desapercibido porque se logró un cambio en la interpretación que los grupos sociales relevantes hacían de los artefactos (Brunn y Hukkinen 2008). Del mismo modo que en la controversia anterior, Facebook puso en el centro del problema los controles de la privacidad que los usuarios podían utilizar, pero no puso en evidencia los bordes, antes porosos de la red social, habían empezado a desvanecerse, dos lugares del ciberespacio que antes estaban separados por el código: el adentro y el afuera de la red.

Para entender cómo funcionó la clausura de Beacon, es necesario adentrarse en los términos de la negociación de las nociones de privacidad que operaron dentro de la controversia. Para Facebook, sus usuarios no son solo sus clientes, son también sus productos; ello en un marco en el cual se ha logrado que las personas compartan información de todo tipo, de forma cada vez más indiscriminada y abierta. La privacidad en el contexto de transparencia radical es prácticamente inviable. “Si tú tienes algo que no quieres que se conozca, es mejor que no lo hagas en primer lugar” (Eric Schmidt, CEO de Google, citado por Dwyer 2011, 59). Facebook construye el contexto de privacidad al entregarle al usuario un sentido de control sobre su experiencia en la red social (qué foto colocar en el perfil, a quién aceptar como amigos, invitación a compartir

aplicaciones, entre muchas otras opciones), pero este sentido de privacidad es tramposo una vez que el usuario se adapta al entorno de Facebook. Para Hoofnagle y Zimmer (2010, en línea) las controversias de News Feed y Beacon no son errores del manejo de la privacidad de Facebook; todo lo contrario, se trata de estrategias exitosas donde “Facebook sigue un patrón en el que da dos pasos agresivos hacia delante sobre el mal uso de la información y luego solo da un pequeño paso atrás cuando la crítica aparece”. Pues cuando las compañías tienen como centro de su negocio la información es muy difícil que la privacidad se vuelva una prioridad, como en el caso de Facebook, que promueve un mundo más abierto, más conectado se beneficia monetariamente de la información que comparten sus usuarios.

Otras nociones de privacidad sin equivalencia directa con la información o control de los datos no intervienen en la controversia. No se consideró, por ejemplo, que la privacidad es clave para proteger las libertades religiosas, políticas e intelectuales, o la dignidad de las personas. Solo entre enero y junio de 2010, Google recibió en Estados Unidos 4287 peticiones de acceso a la información de sus usuarios por parte de las autoridades. La información solicitada incluía toda la actividad en línea que Google hubiera podido registrar sobre dichos usuarios (Dwyer 2011, 63). El cambio tecnológico y la regulación legal han erosionado el derecho a la privacidad como un derecho vivo, pues la exposición del sujeto se ha vuelto parte del sistema de confianza que la sociedad establece. Facebook comprendió que apelar a la identidad real de las personas le permitiría crear una red donde los sujetos pudieran escribir sus propias bitácoras exponiendo aspectos de su personalidad antes no visibles para públicos tan amplios. Abrir la esfera privada ayudó a crear un sentido de conexión entre la gente y, con ello, las expectativas de privacidad disminuyeron notablemente, pues cuando los sujetos internalizan una privacidad reducida, difícilmente pueden mantener expectativas más amplias.

La gente empieza a adecuarse a entornos donde la privacidad prácticamente es inexistente [...] el mensaje es que no controlamos más quién ve nuestros datos [...]. La privacidad es un concepto que ha sido constantemente interpretado y reinterpretado por siglos en función de las expectativas de

privacidad. La esfera general privada se ha vuelto más pequeña porque hemos aceptado la intrusión de más y más técnicas de monitoreo sofisticadas. Los miembros de la sociedad hoy en día, particularmente aquellos nacidos en la Era de la Información, no saben lo que significa la vida sin vigilancia. Sus vidas no son libres porque no creen que están solos y que no pueden tomar decisiones autónomamente (Alpert 2006, 70-1).

Términos de servicio, año 2009: la tercera controversia sobre la privacidad en Facebook

Podemos hacer lo que queramos con
tu contenido para siempre.
—The Consumerist, 2009

El cambio en febrero del 2009 de los Términos de Privacidad en Facebook originó un gran revuelo entre los usuarios sobre la propiedad de los contenidos subidos a la red social. Los antiguos términos señalaban que al momento de cerrar una cuenta, cualquier derecho que la red pudiera reclamar sobre el contenido de la misma expiraba con su cierre, pero introdujeron una modificación que aclaraba que cualquier contenido que se subiera a la red podría ser usado por Facebook indefinidamente, incluso cuando la cuenta fuese cerrada. La Unión de Consumidores de Estados Unidos publicó, en su blog *The Consumerist*, un artículo sobre los nuevos Términos de Privacidad en el que copiaban algunos de los párrafos de las nuevas condiciones.

Usted otorga a Facebook una licencia mundial irrevocable, perpetua, no-exclusiva, transferible, totalmente pagada (con el derecho a sublicenciar), para (a) usar, copiar, publicar, difundir, almacenar, retener, mostrar públicamente, transmitir, escanear, reformatear, modificar, editar, enmarcar, traducir, extraer, adaptar, crear trabajos derivados y distribuir (a través de múltiples niveles), cualquier contenido que como usuario haya publicado (i) en conexión con el servicio de Facebook, (ii) permitido que otro usuario publique, incluidos vínculos a sitios web y (b) usar su nombre o imagen para cualquier propósito, incluidos usos comerciales o de publicidad, cada uno de (a) y (b) en o en conexión con el Servicio de Facebook o su promoción (*The Consumerist*, 15 de febrero de 2009).

Si bien el lenguaje era muy similar al de los antiguos Términos de Privacidad, se renovó el párrafo en el que se basa la controversia.

Usted puede remover su contenido de Usuario del sitio en cualquier momento. Si escoge remover su contenido de usuario, la licencia garantizada más arriba, expirará automáticamente, aunque debe conocer que la Compañía retendrá copias archivadas de su Contenido de Usuario (*The Consumerist*, 15 de febrero de 2009).

La modificación en esta cláusula cambiaba los términos del conjunto. La Unión de Consumidores centró su *reclamo* en el campo de la privacidad, pues lo que estaba detrás de lo que se considera “información pública” en los contenidos de los usuarios dependería de cómo ellos protegieran sus contenidos con los controles de privacidad. Aquello que no estuviere protegido en algún nivel como “privado”, se consideraría automáticamente como información pública de la cual Facebook podría apoderarse para los usos que ya hemos visto especificados en sus términos de servicio. La Unión publicó en su blog: “Asegúrense de no subir nunca contenidos que les hagan sentir incómodos, ahora ya no son suyos, son de Facebook” (*The Consumerist*, 15 de febrero de 2009).

Una ola de críticas siguió a esta publicación. La respuesta de Zuckerberg fue mucho más rápida que en la controversia pasada, publicó un comunicado titulado: “En Facebook la gente es dueña y controla su propia información”.

Hace un par de semanas actualizamos nuestros términos de uso para aclarar algunos puntos para nuestros usuarios. Algunas personas se han preguntado sobre los cambios, así que me gustaría tratarlos aquí. También aprovecho la oportunidad para explicar qué pensamos sobre la información de las personas. Nuestra filosofía es que la gente es dueña de su información y controla con quién la comparte. Cuando una persona comparte información en Facebook, primero le otorga una licencia para usar su información, de modo que podamos mostrársela a aquellos que nos solicitan compartirla. Sin esta licencia nosotros no podríamos ayudar a la gente a compartir su información. Uno de los cuestionamientos sobre los nuevos términos de uso es si Facebook puede utilizar la información para siempre. Cuando una persona comparte un mensaje con un amigo, dos copias de esa información son creadas –una para la

persona que envía el mensaje (*box*) y otra para quien la recibe (*inbox*). Incluso si esa persona desactiva su cuenta, su amigo todavía tiene una copia del mensaje. Creemos que este es el mejor modo de trabajar es consistente con otros servicios como el correo electrónico. Una de las razones por las que actualizamos nuestros términos de referencia fue para aclarar este tipo de cosas. En realidad, no compartiríamos la información de ustedes de un modo que no les gustaría su confianza en nosotros como un lugar seguro para compartir información es la parte más importante que hace funcionar a Facebook. Nuestro objetivo es construir grandes productos, comunicar más claramente y ayudar a la gente a compartir su información en un ambiente seguro. Todavía tenemos trabajo en comunicar lo que hacemos de manera más clara sobre estos asuntos, nuestros términos son un ejemplo de ello. Nuestra filosofía es que la gente es dueña de su información y controla con quien la comparte, ella se ha mantenido como una constante. Gran parte del lenguaje utilizado en los términos es extremadamente formal y protector de los derechos que debemos ofrecerles en este servicio. Con el tiempo seguiremos aclarando nuestra posición y volveremos los términos más simples. Lo que es interesante de este cambio en nuestros términos es que subraya la importancia de este asunto y su complejidad. La gente quiere total propiedad y control sobre su información para poder cortar el acceso en cualquier momento. Al mismo tiempo, la gente también quiere ser capaz de compartir información que otros les han entregado —como correos electrónicos, números de teléfono, fotos y otros— con otros servicios y garantizar el acceso de esos servicios a la información de esas personas. Estas dos posiciones son contradictorias. No hay un sistema hoy en día que me permita compartir mi correo electrónico o mi dirección, y que me dé la posibilidad de controlar simultáneamente los servicios que ustedes comparten. Estamos en un punto interesante del desarrollo de un mundo en línea abierto, donde estos asuntos se están trabajando. Es un terreno difícil de navegar y vamos a cometer algunos errores, pero como el servicio líder de compartir información, tomamos estos asuntos muy en serio, al igual que nuestra responsabilidad para resolverlos. Este es un punto grande este año y expresaré mis ideas sobre apertura y otros temas muy pronto (Zuckerberg 2009a, en línea).

En su mensaje, Zuckerberg recalca que los problemas de privacidad estaban centrados en la propiedad de la información producida por los usuarios y en qué hacían con esa información. Seguía siendo

muy opaco el lenguaje, aunque aparentemente más fácil que el utilizado en los términos del servicio. En primer lugar, Facebook redujo la privacidad a la información y al uso de la misma. Luego, relacionó el entorno seguro que la empresa había creado con las expectativas de privacidad de sus usuarios y apeló a la confianza de las personas en el espacio virtual de la red para seguir compartiendo información. En tercer lugar, asumió que los usuarios desean compartir la información de sus amigos y conocidos con las empresas que operaban dentro de Facebook. Y, finalmente, afrontó el reto de compartir la información del modo que los usuarios deseaban.

Los funcionarios de Facebook indicaron que nunca se había reclamado la propiedad de los contenidos por ellos generados, lo que se intentaba era tener unos Términos de servicio más claros y consistentes con el comportamiento del sitio. Por ejemplo, cuando un usuario envía un mensaje a un amigo (o publica en su muro), el contenido puede que no sea removido por Facebook si el usuario cierra la cuenta, pero puede que sí sea borrado por su amigo. Algo que se debe recalcar es que la licencia que Facebook aplica a los contenidos de los usuarios está sujeta a la configuración de privacidad que ellos realicen sobre la información que suben a la red social. Facebook respeta todos los contenidos que tienen alguna limitación para ser expuestos públicamente.

Otro punto resaltado por *The Consumerist* acerca de las declaraciones de los funcionarios de Facebook es que ellos enfatizaban las conductas de los usuarios y las expectativas de privacidad que construyen con respecto a la tecnología: un usuario que ha crecido con el correo electrónico, por ejemplo, no espera que el servicio de *webmail* borre los mensajes que ha enviado a terceros, en los *inbox* de los terceros, cuando el usuario decide cerrar su cuenta.

Los usuarios se organizaron en múltiples grupos para proteger su privacidad, entre ellos People Against the new Terms of Service (TOS), que alcanzó 148 000 miembros en los primeros días. Al conocer que la compañía daba marcha atrás con los nuevos términos, publicó: “Nosotros hablamos y Facebook escuchó (tabla 5). En medio de la protesta Facebook reestableció los antiguos términos del servicio e, incluso, fue más lejos: estableció una Declaración de Derechos y

Responsabilidades”.⁹ La prensa se refirió a esta controversia como una brecha de confianza entre los usuarios y Facebook.

La gente tiene todo el derecho a estar indignada. Pues la compañía se ha burlado de los compromisos que hizo para proteger la privacidad de los usuarios y para mejorar los controles de sus miembros [...]. Mark Zuckerberg, el fundador y jefe de Facebook, tiene que aprender del peor modo que una red social no se parece al correo electrónico (*BBC News 2009*, en línea).

EPIC anunció que iniciaría una demanda a Facebook frente a la Comisión Federal de Comercio de Estados Unidos para solicitar el retorno a los antiguos términos de servicio. El centro de la demanda era el cambio de lenguaje que permitía a Facebook el control perpetuo del contenido que los usuarios subieran a la red (Terdiman 2009). EPIC empezó su acción solicitando información a la Administración de Servicios Generales (GSA, por sus siglas en inglés) sobre los acuerdos entre esta y las compañías de redes sociales, con las empresas de nubes de computación que facilitaban la recolección de datos personales de los ciudadanos norteamericanos. Así argumentó su pedido:

Los sitios de redes sociales dan a los usuarios un camino fácil para compartir información sobre sí mismos. En todo caso, muchos usuarios encuentran fácilmente que la información que intentan compartir con sus amigos también llega a manos de las autoridades, extraños, prensa y público en general. Por ejemplo, las agencias de trabajo están mirando estos sitios para evaluar a sus aplicantes. El gobierno accede a la información personal de los usuarios de Facebook lo que levanta todavía más preocupación entre los usuarios. Se necesita conocer más sobre el acuerdo al que ha llegado la GSA a nombre de las agencias federales, con las redes sociales y los servicios de nubes de computación, incluidos los verdaderos términos de los acuerdos, cualquier opinión legal preparada por la agencia (o en posesión de la agencia) que considere el impacto que estos acuerdos ocasionan en la privacidad y en el gobierno abierto, y cualquier procedimiento desarrollado por la agencia con respecto al despliegue de estos servicios (EPIC, 30 de abril de 2009).

⁹ People Against the new Terms of Service (TOS), grupo de Facebook, 2009, <https://www.facebook.com/groups/77069107432/>

Tabla 5. Flexibilidad interpretativa de los términos de servicio de Facebook

	Intencionalidad	Propiedad de la información	Usos de la información
Usuario	<p><i>Compartir</i> información con los amigos.</p> <p><i>Controlar</i> la privacidad de la información decidiendo quién ve qué.</p>	<p>La información es <i>propiedad del usuario</i>.</p>	<p>Las personas escogen cómo compartir su información.</p>
Facebook	<p>Generar efectos virales de la información.</p> <p><i>Vender</i> esa información a terceros (compartir la información con aquellos que la solicitan).</p> <p><i>Ofrecer controles</i> de privacidad, pero más complicados de utilizar.</p>	<p>Los usuarios ceden a Facebook sus derechos sobre la información que producen. A través de las licencias PI le otorgan la posibilidad de usar, copiar, publicar, difundir, almacenar, retener, mostrar públicamente, transmitir, escanear, reformatear, modificar, editar, enmarcar, traducir, extraer, adaptar, crear trabajos derivados y distribuir (a través de múltiples niveles), cualquier contenido que el usuario haya publicado sin protección de privacidad.</p> <p>La información que los usuarios consideran de su propiedad es vendida cuando los sujetos no usan los controles de privacidad para protegerla.</p>	<p>Facebook desarrolla códigos para utilizar toda la información que no está protegida por el propio usuario con controles de privacidad, y la usa en transacciones que desconoce el usuario.</p> <p>Mientras más difícil es proteger la información, más fácil es utilizarla para entregarla a terceros.</p>

Si Facebook podía utilizar los datos de sus usuarios como hasta ese momento lo había hecho era porque existía un sistema legal que permite que la información que se generaba en un contexto cerrado dentro del Social Graph se extienda a terceros no solo con fines comerciales, sino también de control gubernamental y social. Además de los datos, EPIC

buscaba conocer los mecanismos por los que el sistema permitía estas fugas de datos del contexto en el que fueron generados.

Facebook *negoció* una salida a los nuevos Términos del servicio con una estrategia que pretendía reestablecer la confianza de sus miembros: la gobernanza de Facebook. Zuckerberg (2009c) anunció que se llevaría a cabo un proceso participativo para que los usuarios contribuyeran a mejorar los nuevos términos, que se denominarían Principios de Facebook y Declaración de Derechos y Responsabilidades.

Desde hoy les estamos dando una gran oportunidad de tener voz y voto sobre el gobierno de Facebook. Estamos empezando por publicar dos nuevos documentos para su retroalimentación y comentarios. El primero es los Principios de Facebook, donde se definen sus derechos y que sirve como marco para cualquier política que acordemos —o la razón por la cual no consideraremos otras—. El segundo documento es la Declaración de Derechos y Responsabilidades, que reemplazará a los existentes Términos de Uso. [...] Nos honra que millones de personas hayan decidido utilizar Facebook en sus vidas con sus amigos y sus seres queridos. Entendemos que esto nos da una tremenda responsabilidad hacia nuestros usuarios. La historia nos muestra que los sistemas de gobierno más justos son los que tienen un diálogo abierto y transparente entre la gente que toma las decisiones y aquellos que son afectados por ellas. Creemos que la historia un día nos mostrará que este principio es válido también para las compañías y, es en esa dirección que queremos movernos con ustedes (Zuckerberg 2009b, en línea).

Se empezó por crear el sitio de gobernanza de Facebook en el que se podía votar por los antiguos Términos de servicio o por una propuesta nueva (ilustración 15).

Para ello, se estableció un mínimo de 7000 comentarios para que un artículo fuera retirado y el 30 % de la participación de los usuarios para que su voto decidiera el nuevo texto. En definitiva, había que alcanzar 7000 comentarios por artículo y 60 millones de votos para el documento acordado. El resultado fue que solo el 0,32 % de los usuarios activos votaron (666 000 personas) y un 74 % estuvo de acuerdo con la nueva Declaración de Derechos y Responsabilidades. Facebook generó, así, un laboratorio para conocer hasta dónde podía presionar a sus miembros

Ilustración 15. Sitio de gobernanza de Facebook



a compartir información de forma más pública, y que pasaran desapercibidos los mecanismos para realizar cambios sustanciales (Kirkpatrick 2010).

Dentro de la Declaración de Derechos y Responsabilidades, Facebook señaló:

Tu privacidad es muy importante para nosotros. Hemos diseñado nuestra política de privacidad para ayudarte a comprender cómo puedes utilizar Facebook para compartir contenidos con otras personas, y cómo recopilamos y podemos utilizar tu contenido e información. Te animamos a que leas nuestra política de privacidad y a que la utilices con el fin de poder tomar decisiones fundamentadas. [...] Eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte a través de la configuración de privacidad y aplicaciones. [...] Hacemos todo lo posible para hacer que Facebook sea un sitio seguro, pero no podemos garantizarlo. Necesitamos tu ayuda para lograrlo [...]. Los usuarios de Facebook proporcionan sus nombres e información reales y necesitamos tu colaboración para que siga siendo así.¹⁰

Para lograr una participación activa en los cambios de la plataforma era necesario ingresar al sitio de Gobernanza de Facebook, leer todos los documentos y proponer los cambios, lo cual requería mucho tiempo de

¹⁰ “Declaración de principios y responsabilidades”, *Blog de Facebook*, acceso el 23 de agosto de 2014. <https://www.facebook.com/legal/terms>

los usuarios. La propia arquitectura del mecanismo de participación se convirtió en una barrera para el aporte activo. Además los usuarios entendían poco sobre las consecuencias de sus acciones, ya que percibían los cambios de las políticas de privacidad como “ruido de fondo”. En particular, cuando el número de cambios iba en aumento, estaban menos dispuestos a prestar atención a este movimiento de la arquitectura del sitio. La apatía creció al ver que no era posible incidir en los términos legales de su contrato con la red ni en las políticas que regulaban su conducta dentro de Facebook. La confianza se erosionaba en este intercambio discursivo de mejorar las herramientas del usuario para controlar su información, cuando en la práctica se hacía exactamente lo contrario. Si una persona quería borrar, permanentemente, información de su perfil debería ser capaz de hacerlo, al igual que cuando deseaba salir de una red social, toda la información almacenada a lo largo del tiempo en su perfil debería poder ser eliminada completamente (ilustración 16).

Cuanto más la compañía ratificaba la entrega de los controles sobre su información a los usuarios, en realidad se los retiraba. Chris Kelly (2009), el director de privacidad de Facebook, publicó en el blog de la empresa:

Las herramientas de privacidad, que se diseñan a la medida para decidir qué información es compartida y con quién, son el corazón de la confianza. En los últimos cinco años, Facebook ha aprendido que la privacidad efectiva se sostiene en tres principios básicos:

Control. Cuando la gente puede fácilmente controlar la audiencia que recibirá su información y contenidos, comparte más y pueden conectarse mejor con las personas que les importan en sus vidas.

Simplicidad. Cuando las herramientas son simples, la gente está más motivada a usarlas y a entenderlas.

Conexión. Con herramientas efectivas las personas pueden balancear con éxito su deseo de controlar el acceso a la información con su deseo de conexión –para descubrir y ser descubierto por aquellos que les importan–.

Los usuarios en cambio pensaban que, cada vez, era más complejo utilizar los controles, y que los principios que Kelly proponía no

Ilustración 16. Notificaciones del sitio de Gobernanza de Facebook



funcionaban dentro de la configuración de privacidad de Facebook. Mientras más controles sobre privacidad se implementaban en Facebook, menos amigable se tornaba la plataforma y más complicado resultaba para los usuarios proteger su privacidad. No fue fácil “controlar” quién ve qué en el Facebook del año 2009 porque los controles eran manuales, estaban ubicados en distintas páginas, se cruzaban entre sí y no bastaba con escoger una opción sin haber revisado las otras páginas donde los controles se volvían cada vez más difíciles de entender. La configuración de privacidad no era simple ni era sencillo entender los impactos de cada herramienta sobre el uso de la información que se subía a la red social y cuán protegidos estaban los datos de los usuarios. Se apelaba al deseo de conexión de los usuarios para que se vuelvan más visibles sus contenidos y con ello llegar a más personas en la red, lo que no necesariamente funcionaba como un principio de protección de la privacidad.

Clausurar la controversia de los Términos de servicio del año 2009 implicó que los usuarios se organizaran de forma más activa y que se apoyaran en organizaciones dispuestas a iniciar demandas legales contra la compañía. Esta vez, Facebook tuvo que dar marcha atrás en la aplicación de los nuevos Términos de servicio; proponer un sistema de gobernanza de con la participación de los usuarios y diseñar una plataforma tecnológica (sitio web de gobernanza de Facebook); implementar nuevos controles de privacidad; y, finalmente, conseguir un certificado

de TRUSTe sobre su política de privacidad.¹¹ Todo ello para mantener el sistema de confianza que estaba en entredicho.

Los guiones cognitivos y los patrones de conducta que acompañaron el cambio tecnológico fueron muy visibles en este caso (Akrich 1992; Latour 2002). Facebook apeló a los comportamientos de los usuarios frente a otras tecnologías, para naturalizar sus prácticas de intercambio, sistematización y almacenamiento de los datos. El “ambiente inteligente” que construyó es lo que algunos teóricos han denominado “computación ubicua” (Weiser 1991) o “la internet de las cosas” (Hongladarom 2011; Ashton 2009). La computación ubicua es la habilidad de los artefactos para comunicarse a través de redes de datos, no solo entre computadores sino también con objetos ordinarios. En el caso de Facebook, esto se refleja en la capacidad que tienen las cosas de formar redes entre ellas; justamente este fenómeno de ambiente inteligente afecta la concepción del sujeto de un modo importante en relación con la noción de privacidad, porque tecnológicamente se decide qué se entiende por privacidad y cómo regularla (Hongladarom 2011). Una vez que el sujeto se convierte en parte de la red de información a través de los datos que produce, empieza a ser distribuido a través de la red.

Como lo anotaba Solove (2004, 2008), los *dossiers* digitales reemplazan a los sujetos en el ciberespacio, gracias a la agregación de información que producen; ello los distribuye en un sistema que configura quiénes son y que predice lo que harán. Las “biografías no autorizadas” son creadas por compañías que amasan la información personal y los récords públicos de los individuos hasta convertirlos en hechos significativos al momento de investigar a las personas (Solove 2004). La distribución del ser se acelera con flujos de información cada vez más intensos y los sujetos pierden la conciencia de cómo sus datos son registrados, compartidos, publicados, vistos y vendidos.

La computación ubicua debe crear sistemas de confianza para poder funcionar en términos sociales. Así, Facebook logra establecer la percepción de un entorno seguro, a través del uso de las identidades reales de las personas y de la circularidad de la información dentro de sus

¹¹ Elliot Schrage (2009) anunció en el blog de Facebook el 29 de octubre que ha mejorado la transparencia sobre la privacidad. Ahora la compañía cuenta con un Certificado de TRUSTe (TRUSTe certification seal) que aprueba la política de privacidad de Facebook.

redes de amigos. Este lugar del ciberespacio estimula la producción de información personal (estados de ánimo, actividades, lecturas, posturas políticas) que se publica a los amigos y conocidos dentro de una red que ha sido configurada por el propio sujeto.

El sistema de confianza funciona como un mecanismo que permite a los usuarios creer que están dentro de un entorno seguro, donde lo que representan, transmiten y producen va a ser utilizado expresamente como ellos lo intentan. El problema es que manejan sentidos de lo privado diferentes de los de Facebook. Como hemos visto, más del 50 % de los usuarios no había leído los términos de privacidad y no era consciente de los derechos que le había otorgado a Facebook sobre sus contenidos, de la forma en que era rastreada su actividad en línea, y en que habitaba la red social y el ciberespacio.

Los términos no transparentaban los procesos de monetización del Free Labor de los usuarios (Terranova 2000) y, a través de eufemismos, se transformaba opacidad en transparencia, la venta de datos en intercambio de información, la cesión de los derechos de propiedad intelectual sobre los contenidos con propiedad de la información. Esta opacidad permite que la distribución del ser se acelere con flujos de información cada vez más intensos.

Uno de los problemas que presenta la socialización en línea es la capacidad, sin precedentes, que sus usuarios adquieren para “abrirse a los demás”, ocasionando serios problemas a su privacidad.

Sitios de redes sociales como Facebook tienden a tener una misteriosa habilidad para extraer pensamientos e información privados de sus usuarios, de modo que los usuarios no sienten *prima facie* que sus vidas privadas están en riesgo. Al contrario, usualmente sienten que están revelando información privada por su propia voluntad, cuando en realidad, fuera de la pantalla difícilmente revelarían tanto, incluso a sus amigos más cercanos. Tal vez el grado de distancia que ofrece Facebook –la distancia sentida por los usuarios cuando se conectan al sitio web, cuando están solos con su computador y sus “amigos”, son solo *blips* de imágenes y textos en la pantalla– da a los usuarios un falso sentido de seguridad, de modo que sienten que hay muy poco peligro en revelar sus secretos más íntimos en el sitio web (Hongladarom 2011, 364).

Una función fundamental del diseño de la red social ha sido establecer la confianza del usuario. Una vez que los sujetos ingresan a los espacios virtuales y los domestican, los sistemas de confianza entran en acción y los miembros asumen que la red responderá a su confianza con honestidad y buenas intenciones. El funcionamiento del artefacto se estabiliza a través de estas funciones sociotécnicas en las cuales los sujetos, el código, los artefactos legales y las instituciones intervienen en procesos de adecuación de respuestas/soluciones tecnológicas (Thomas 2008).

Esta tercera controversia muestra que la privacidad en Facebook se iba estabilizando a partir de la reformulación del problema a través de mecanismos de control. Las nociones de control y confianza están en la base de las controversias analizadas y, en todas ellas, se presiona a los usuarios a entregar sus contenidos y la propiedad de los mismos a Facebook, por medio de estrategias tecnológicas como News Feed, Beacon y los Términos del servicio. Para resolver las controversias, Facebook entregó más controles de privacidad, eliminó sistemas, pero creó otros. News Feed se mantuvo gracias las herramientas de configuración de privacidad que entregaron a los usuarios; Beacon se convirtió en Facebook Connect y Open Graph y con ello mantuvo su intención de ingresar o extraer los datos de los usuarios de la red, rastreándolos por toda la internet y usando la información producida en sus recorridos; los Términos de Privacidad de 2009 se anularon, pero se crearon unas nuevas normas que al final mantienen la propiedad de Facebook sobre los contenidos, no protegidos, de sus usuarios, y su capacidad de monetizar su actividad en línea. Facebook entregó, a cambio, un sistema de gobernanza a fin de promover la participación de las personas, que fue utilizado como un laboratorio para analizar el comportamiento frente a la toma de decisiones en la red social.

Así, la privacidad dentro de Facebook se convierte en un problema que se reformula en cada controversia y en un proceso de construcción continua signado por prácticas cotidianas que realizan ajustes y modificaciones ante nuevas formas de funcionamiento (Bruun y Hukkinen 2008; Pinch y Bijker 2008; Thomas 2008).

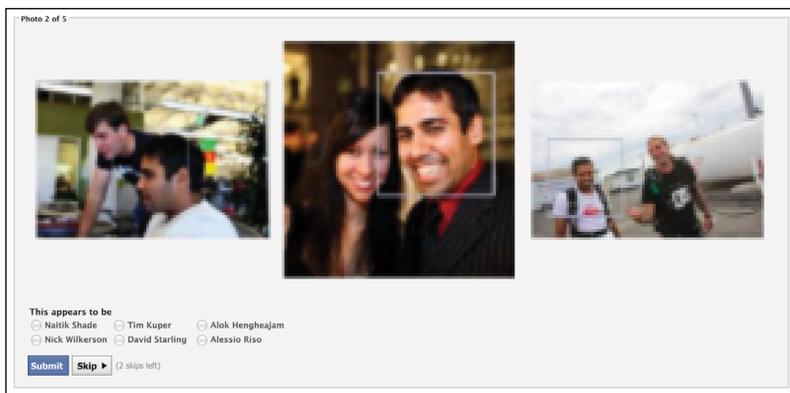
Demanda de la Comisaría de Privacidad de Canadá a Facebook: la cuarta controversia sobre la privacidad

El *contexto* de esta controversia es la demanda realizada por la Clínica de Interés Público y Política Canadiense de Internet (CIPPIC, por sus siglas en inglés) de la Universidad de Ottawa contra Facebook, el 30 de mayo de 2008. Contiene 24 alegatos sobre 11 temas. Entre ellos figuran los controles de privacidad, la recolección y uso de la información personal para fines publicitarios, revelación de la información personal de los usuarios a terceros para el desarrollo de aplicaciones, y la recolección y uso de información personal de los no-usuarios. Los puntos centrales que *reclamaba* la demanda tienen que ver con el “conocimiento y consentimiento” de los usuarios para la recolección, uso y difusión de su información personal; la “retención” de la información personal, en particular en el cierre de las cuentas de los usuarios de Facebook, y en la libre disposición de información personal de los no-usuarios; y, finalmente, las “garantías de seguridad” sobre aplicaciones de terceros y Facebook Mobile.

Tanto el Gobierno de Canadá, a través de su Comisaría de Privacidad y la CIPPIC como el mismo Facebook, desplegaron las redes de relaciones que avalaron sus posiciones. La Comisaría y la Clínica se apoyaron en dos equipos: ENISA (European Network and Information Security Agency) y el Grupo de Trabajo Internacional de Berlín sobre la Protección de Datos en Telecomunicaciones.¹² ENISA enfatizó los riesgos de las redes sociales y realizó una serie de recomendaciones para cada caso, con el objeto de desarrollar mejores prácticas y reducir la inseguridad de los usuarios. Las principales amenazas a la privacidad, según la Agencia, eran seis: a) agregación del *dossier* digital; b) recolección de datos secundarios; c) reconocimiento facial (ilustración 17); d) contenido basado en la recuperación de imagen; e) vinculación de imágenes de metadata, etiquetado y cruce de imágenes; y, f) dificultad para completar la eliminación de las cuentas. En esta controversia, varios de los puntos definidos en el Memorando fueron utilizados como sustento en la demanda canadiense a Facebook.

¹² De ENISA usaron su documento de trabajo “Asuntos de Seguridad y Recomendaciones para Redes Sociales en Línea”, publicado en octubre de 2007; del Grupo de Trabajo Internacional de Berlín, sobre la Protección de Datos en Telecomunicaciones, el “Memorando de Roma”, publicado en marzo de 2008.

Ilustración 17. Captcha de reconocimiento facial



Fuente: <https://bit.ly/3dSMfxz> (contenido fuera de línea).

El segundo grupo de trabajo, particularmente relevante, fue un cuerpo asesor independiente para la protección de datos y privacidad conformado por el directorio de la Comisión Europea, directorio de Derechos Fundamentales y Ciudadanía, Seguridad y Justicia.¹³ Definía a las redes sociales y sus responsabilidades, material que fue usado por la Comisaría como antecedente y elemento de referencia en la controversia:

Las redes sociales son servicios de sociedades de la información que comparten ciertas características:

- Los usuarios son invitados a proveer datos personales con el propósito de generar una descripción de sí mismos o “perfiles”.
- Los servicios de redes sociales proveen igualmente herramientas que permiten a los usuarios publicar su propio material (contenido generado por el usuario como fotografías, entradas diarias, música, video clips o vínculos a otros sitios).
- “La socialización en red” es posible gracias al uso de herramientas que proveen una lista de contactos para que cada usuario interactúe.

Los servicios de redes sociales generan gran parte de sus ingresos a través de la publicidad que funciona dentro de la web y que a la que acceden los usuarios. Los usuarios que publican grandes cantidades de

¹³ Creado bajo el art. 29 de la Directiva 95/46/EC.
<https://bit.ly/2GBPv4Z>

información sobre sus intereses en sus perfiles ofrecen un mercado refinado a los publicistas que buscan alcanzar públicos objetivo basados en información.

Es por ello importante que los servicios de redes sociales operen de tal forma que respeten los derechos y las libertades de los usuarios, quienes tienen legítimas expectativas de que los datos personales que publican sean procesados de acuerdo con la legislación de privacidad y de protección de datos nacionales y europeos.¹⁴

Según este grupo de trabajo, los proveedores de aplicaciones son controladores de datos de los servicios de redes sociales; en casos excepcionales son los mismos usuarios (cuando salen de los usos caseros de la información). De igual modo, el grupo consideró que un elemento importante de los controles de privacidad es el acceso a datos personales publicados en los perfiles, pues si no existen restricciones a esa información, los datos pueden ser utilizados por terceros y exponer información íntima en los buscadores.

Puesto que una minoría de usuarios realiza cambios en la configuración de sus perfiles, los servicios de redes sociales deben ofrecer herramientas de control de la privacidad amigables, de modo que permitan a los usuarios consentir específicamente el acceso a la información de sus perfiles para reducir el riesgo de que terceros procedan fuera de la ley. Los perfiles restringidos no deberían permitir el acceso de los buscadores a su información, incluidos los parámetros de edad o ubicación.¹⁵

Cada una de estas nociones es utilizada tanto en los alegatos de la CIPPIC como en las resoluciones de la Comisaría de Privacidad. En el mismo mes que la CIPPIC demandó a la red social, Facebook realizó tres alianzas estratégicas: firmó un convenio con 49 fiscales generales de los Estados Unidos con la promesa de convertirse en un entorno más seguro para usuarios menores de edad; meses más tarde aceptó participar en la “Fuerza de Trabajo para la Protección Técnica” liderada por el Centro Berkman para Internet y Sociedad de la Universidad de

¹⁴ Artículo 1, párrafo 2 de la Directiva 98/34/EC.

¹⁵ Grupo de Trabajo de Protección de Datos [Anexo 5].
http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Gráfico 10. Niveles de la controversia CIPPIC vs. Facebook



Harvard, creado como parte de la alianza entre MySpace y el Fiscal General de los Estados Unidos; y en febrero de 2009, junto con otras 17 redes sociales, firmó el pacto denominado “Principios para una sociabilidad en línea más segura para la Unión Europea”, con el propósito de proteger a jóvenes

La cuarta controversia fue particularmente importante porque visibilizaba otros actores que intervienen de forma indirecta, para fortalecer tanto las demandas de las organizaciones canadienses como las respuestas de Facebook a dichas demandas (gráfico 10). A continuación se muestra la red de relaciones que los actores de la controversia construyeron para negociar sus posiciones.

Este grupo de actores en beneficio de los usuarios conformó una red en un nuevo nivel: la acción de los Estados. La demanda de Canadá a Facebook planteó consecuencias legales que la red social debió afrontar, a escala mundial, y enseñó las redes de asociaciones multidominio tejidas alrededor de la protección de la privacidad en línea. Ya no se trataba de una controversia entre usuarios-red social, o entre usuarios-red social-compañías asociadas a Facebook-organizaciones protectoras de la privacidad. En este caso intervienen los Estados, la Comunidad Europea, instituciones intergubernamentales, fiscales generales, centros de protección de derechos e institutos de investigación vinculados a universidades.

En este contexto, la demanda de CIPPIC a Facebook fue respondida por la Comisaría de Privacidad a través del informe presentado por la comisaria asistente Elizabeth Denham el 16 de julio de 2009. En el

informe se distingue tres tipos de alegatos, los bien fundamentados y sobre los que Facebook adopta medidas correctivas, los bien fundamentados pero sobre los que Facebook decide no adoptar mejoras, y los mal argumentados por parte de CIPPIC. En cuatro temas se encontró que la demanda estaba bien argumentada y que Facebook contravenía el Acta de Protección de Información Personal y Documentos Electrónicos (PIPEDA, por sus siglas en inglés): a) fecha de nacimiento, b) configuración de privacidad, c) publicidad y d) monitoreo de actividad anómala. Sin embargo, estos temas estaban resueltos con las medidas correctivas que Facebook propuso en respuesta a las recomendaciones.

Fecha de nacimiento

CIPPIC *demandó* que es innecesario que los usuarios provean su fecha de nacimiento como condición para registrarse y que no se les explicaba adecuadamente por qué deben entregar estos datos y cómo serán utilizados. La *respuesta de Facebook* se basó en la prevención del uso de la red social por parte de menores de edad, la protección a los menores de contactos inapropiados, la protección a los menores de contenidos inapropiados y proveer de herramientas seguras a todos los usuarios de la red social.

Recomendaciones realizadas: mejorar su política de privacidad, con el fin de explicar los objetivos específicos de la recolección de la fecha de nacimiento; definir el significado de información de perfil y asegurar que cuando dicha información no es pública en el perfil no puede ser utilizada con fines publicitarios; indicar a los usuarios los propósitos de la recolección de esta información, incluidos los fines comerciales.

Facebook aceptó cambiar el lenguaje de su política de privacidad a “recolección de la información para usos publicitarios”; cambios que pasarían por un periodo de consulta a sus usuarios e introdujo esta frase en la recolección de la información: “Facebook requiere a todos los usuarios proveer su verdadera fecha de nacimiento para asegurar la autenticidad y proveer acceso a contenido apropiado a la edad. Usted será capaz de esconder esta información si lo desea y su uso será gobernado por la Política de Privacidad de Facebook” (Report of Findings 2009, 17).

Configuración de privacidad

CIPPIC *demandó* que Facebook estaba utilizando consentimiento *opt-out* para el uso y difusión de la información personal, sin cumplir con los requisitos de consentimiento de *opt-out*. Aseveró que Facebook no informaba lo suficiente a sus usuarios sobre cómo era utilizada su información personal, por ejemplo: que será compartida a través de la configuración preseleccionada, por tanto no existe consentimiento informado; que no realizar cambios a la configuración preseleccionada constituye consentimiento a esa configuración; que subir álbumes de fotos tiene una configuración pública de la información y que por tanto las fotos, y los comentarios de las fotos, pueden ser vistos por los amigos y por cualquier miembro de la red; que la configuración preseleccionada permite compartir información personal, incluso información sensible con cualquiera en la red.

La *respuesta de Facebook* fue que CIPPIC había caracterizado erróneamente los controles de configuración de la red, cuando en realidad estos incluían una arquitectura de amigos y una de red.

Al contrario de los reportes públicos, los datos del perfil de Facebook no son accesibles por cualquiera en internet, de hecho, no son accesibles para la mayoría de usuarios de Facebook. Los controles de configuración de privacidad de Facebook han jugado un rol central para darles control a los usuarios sobre quién tiene acceso a su información personal al dejarles escoger entre los amigos que ellos aceptan dentro de la red [...]. Además de los controles de privacidad que son parte fundamental de la arquitectura de Facebook, los usuarios tienen controles precisos y extensos para escoger quién ve qué entre sus amigos en la red, también tienen herramientas que les permiten limitar la información a la que pueden acceder los motores de búsqueda y otras entidades que están fuera de la red (Report of Findings 2009, 19).

Facebook indicó que entre un 20 % y un 30 % de los usuarios cambia su configuración de privacidad y que no sería práctico obligarlos a decidir sobre su configuración antes de empezar a utilizar la red porque esto sería una barrera para muchas personas. Igualmente, contestó que cada vez que un usuario sube un álbum de fotos le aparecerá en la pantalla

una pregunta: “¿Quién puede ver esto?”, lo que ayudará a controlar la privacidad del contenido aunque se mantenga intacta la configuración original que indica “todos”.

A los usuarios de Facebook no se les requiere, ni están obligados, a subir más información que su nombre, su correo electrónico, su fecha de nacimiento y su género. Cuando ellos realizan opciones *opt-in* para proveer información lo hacen con la intención de compartirla con otros. Han venido a Facebook explícitamente y han realizado opciones para subir información. En realidad, muchos usuarios han visto reportajes falsos en los medios de comunicación, que son repetidos en la demanda de CIPPIC, sobre los riesgos de que cualquiera pueda ver la información que ellos publican, y, a pesar de ello, han continuado subiendo información como una acción afirmativa (Report of Findings 2009, 22).

La comisaria asistente Denham indicó que Facebook provee a sus usuarios de extensos controles de privacidad, permitiéndoles controlar lo que ellos quieren compartir; que realizar configuraciones de privacidad al registro de la cuenta puede descorazonar a muchas personas a ser parte de la red por lo que la preselección de la configuración es aceptable; que las personas suben voluntariamente su información con el objetivo expreso de compartirla con otros y que la alternativa *opt-in* u *opt-out* no es relevante, cuando lo más importante es si la configuración original cumple con las expectativas razonables de los usuarios dentro de un modelo estructurado en el concepto de amigos. Recomendó que los perfiles de los usuarios sean inaccesibles para los motores de búsqueda; cambiar el control “todos”, preseleccionado en álbumes de fotos, a “Su red y amigos”; proveer un vínculo a los controles de privacidad en el momento del registro; notificar a los usuarios que ya se han registrado sobre las opciones de selección de los controles en la configuración de la privacidad.

Facebook respondió con una propuesta, Privacy Wizard, que permite a los usuarios seleccionar entre configuraciones de privacidad bajas, medianas y altas; quienes opten por protección alta no serán encontrados por los motores de búsqueda, con lo cual los usuarios tomarían decisiones mejor informadas. También ofreció entregar controles más granulares sobre cada pieza de información que decidan publicar

e implementar nuevos procesos de registro (que estaban a prueba al momento de su contestación a la comisaria asistente de Canadá) y de envío de información a los antiguos usuarios sobre los nuevos controles de privacidad.

Publicidad

CIPPIC *demandó* que Facebook no hizo un esfuerzo razonable para aclarar a los usuarios el uso de su información personal para publicidad; que se realizaba un uso inapropiado de *opt-out* en vez de *opt-in* en los *social ads* donde los usuarios pueden develar información personal sensible; que no permite a los usuarios realizar una opción *opt-out* de la publicidad de Facebook; y puesto que los usuarios no tienen esta última opción es innecesario que se les pida que acepten este tipo de publicidad como condición del servicio.

Ante esto la red social *respondió*:

Facebook busca ser transparente sobre el hecho de que la publicidad es una fuente importante de ingresos y en explicar a sus usuarios cómo su información personal será utilizada al autorizar a Facebook su uso para entregarles publicidad que sea relevante y personalizada [...]. La política de privacidad y, sobre todo la experiencia de los usuarios, no informan cómo funciona la publicidad en la red –la publicidad que le permite a Facebook proveer el servicio gratuitamente a sus usuarios se utiliza de forma objetiva de acuerdo con los atributos de los perfiles de las personas. Ello se hace sin permitirle al anunciador acceder a la información individual del perfil de los usuarios (Report of Findings 2009, 29).

Las *recomendaciones realizadas* fueron: que Facebook explique mejor el rol de la publicidad en el entorno de la red y las diferencias entre *Facebook ads* y *social ads*; informar a los usuarios sobre el uso de la información de su perfil para fines publicitarios y de la imposibilidad de salir de los *Facebook ads* y los *social ads*; colocar un recordatorio en una parte del menú del perfil, al igual que en otros sitios de la red indicando que la información personal que ellos suben a la red es recolectada, usada y difundida de acuerdo con la política de privacidad de Facebook, y un vínculo a la sección de la Política sobre la publicidad extendida. A la

primera recomendación, Facebook contestó mejorando la descripción de la publicidad dentro de la política de privacidad, pero objetó la segunda recomendación por considerarla disruptiva.

Monitoreo de actividad anómala

CIPPIC *demandó* que Facebook no informaba a sus usuarios que monitoreaba el sitio para detectar comportamientos anómalos, que fallaba en no mencionar esta práctica en su política de privacidad. Facebook *respondió* que los usuarios estaban informados de sus actividades de monitoreo y que, de hecho, Mini Feed y News Feed se basan en estas actividades.

[Facebook] utiliza ciertos algoritmos para proteger a los usuarios en el monitoreo de comportamientos anómalos y es bastante transparente sobre cómo esta actividad funciona, especialmente con aquellos afectados directamente en el sitio. Cuando los usuarios incurren en actividades anómalas se les envía notificaciones en tiempo real, por ejemplo, cuando envían demasiadas invitaciones a amigos —especialmente si estas invitaciones han sido reportadas por otros usuarios como conductas de acoso— ello puede conducir a la suspensión de la cuenta y a la imposibilidad de enviar más invitaciones de amigos. Utilizamos esta infraestructura ampliamente para prevenir abuso en el sitio y para mantener seguros a los usuarios de forma inmediata cuando se intenta tomar ventaja de los usuarios más jóvenes (Report of Findings 2009, 84).

La comisaria asistente recomendó que Facebook incluya en su política de privacidad una explicación sobre sus prácticas de monitoreo de actividad anómala en el sitio, a lo que Facebook respondió con la propuesta del siguiente texto a ser incluido en dicha política.

Para mejorar la seguridad del sitio, Facebook utiliza una variedad de sistemas tecnológicos para detectar y resolver actividad anómala que pueda ser llevada a cabo por los usuarios. Ello puede ocasionar que Facebook suspenda de forma temporal o permanente algunas de las funciones de algunos usuarios (Report of Findings 2009, 86).

Facebook sin embargo se niega a implementar cambios sobre los siguientes puntos de la demanda: a) aplicaciones de terceros, b) desactivación y eliminación de cuentas, c) cuentas de personas fallecidas, d) información personal de los no usuarios.

Aplicaciones de terceros

CIPPIC demandó que Facebook no informaba a los usuarios el propósito de develar información personal a los desarrolladores de aplicaciones; que les estaba entregando información personal más allá de la necesaria para los fines de la aplicación; que estaba requiriendo el consentimiento de los usuarios para revelar información personal más allá de la requerida para hacer funcionar la aplicación; que no notificaba a los usuarios sobre las implicaciones de retirar su consentimiento a compartir información personal con terceros; que permitía a los desarrolladores retener información personal de los usuarios luego de que se eliminara la aplicación y acceder a la información personal del usuario cuando sus amigos añadían aplicaciones sin la debida notificación; que no estaba salvaguardando, adecuadamente, la información personal y que no estaba monitoreando la cualidad y legitimidad de las aplicaciones de terceros o que no estaba tomando las medidas necesarias para prevenir vulnerabilidades inherentes a muchos de los programas de la plataforma de Facebook; que no estaba notificando, eficientemente, a los usuarios sobre cómo su información personal era develada a terceros y que estaba confundiendo a los usuarios con información, poco clara, sobre lo que significa compartir con terceros; que no estaba siendo responsable de la transferencia de la información personal que los terceros procesaban; que no estaba permitiendo a los usuarios no compartir su nombre, redes y listas de amigos cuando sus amigos utilizaban una aplicación.

En un estudio realizado por investigadores de la Universidad de Virginia, en octubre de 2007, sobre la información que necesitaban las 150 aplicaciones más utilizadas en Facebook se señalaba:

Encontramos que el 8,7 % no necesita ninguna información; el 82 % utiliza información pública (nombre, red, lista de amigos); y solo un 9,3 % requiere información privada (fecha de nacimiento, por ejemplo). Puesto

que a todas las aplicaciones se les ha dado acceso completo a la información privada, esto significa que el 90,7 % de las aplicaciones tuvieron más privilegios de los que necesitaban (Report of Findings 2009, 47).

Facebook *respondió* cuestionando la metodología de los investigadores. Indicó que el estudio tuvo una visión innecesariamente limitada en cuanto al uso prosocial y legítimo de la información y que evitó cualquier discusión sobre los límites significativos puestos en marcha para evitar el acceso a los datos de los usuarios, al igual que hizo caso omiso de los límites al uso y conservación de la información, así como de los mecanismos de aplicación que han vuelto exitosa la plataforma.

Los usuarios tienen una gran habilidad para escoger si interactuar o no con una aplicación particular de Facebook, y además tienen la habilidad de bloquear cualquier aplicación y de *opt-out* de todas las aplicaciones de Facebook de un modo muy sencillo (Report of Findings 2009, 43).

Sin embargo, la comisaria asistente de privacidad de Canadá sostuvo que Facebook no había desarrollado un sistema tecnológico que monitoree y controle el uso que hacían los desarrolladores de aplicaciones de la información de los usuarios. Si estos podían copiar la información personal de los usuarios en sus propios servidores

[...] no parece que exista ningún monitoreo efectivo del uso de la información por parte de Facebook. Esto lo admite Facebook en su política de privacidad cuando indica que “no puede controlar cómo [...] los desarrolladores de plataformas utilizan cualquier información personal que puedan obtener en conexión con la Plataforma de Aplicaciones” (Report of Findings 2009, 51).

Y en el mismo párrafo, Facebook colocó el peso en los usuarios para detectar y reportar problemas. “Su inhabilidad para monitorear el uso de los desarrolladores es una razón fundamental para que Facebook tome medidas preventivas” (Report of Findings 2009, 51). Por tanto, *recomendó*: limitar el acceso de los desarrolladores de aplicaciones a la información que no requieren de los usuarios para correr una aplicación específica; que los usuarios sean informados en cada instancia sobre la

información específica que la aplicación requiere; que los usuarios entreguen su consentimiento explícito para el acceso de los desarrolladores a información específica y; que prohíba la difusión de información personal de los usuarios que no están añadiendo una aplicación. Facebook se negó a implementar las recomendaciones.

Desactivación y eliminación de cuentas

CIPPIC *demandó* que Facebook distinguía entre desactivación de cuentas y eliminación de las mismas. La opción de desactivación producía confusión pues no deja claro que la cuenta no puede ser eliminada al ser desactivada. Por tanto, Facebook debería dejar que los usuarios decidan si quieren desactivar temporalmente sus cuentas o eliminarlas de forma permanente, con lo cual debería volverse explícito que Facebook guarda la información de los perfiles hasta una futura reactivación. Del mismo modo, la opción de desactivación debería contemplar un periodo de tiempo, escogido por el usuario, luego del cual toda la información de la cuenta debería ser eliminada de los récords de la red social. Finalmente, que la información de los usuarios, almacenada por Facebook durante la desactivación de la cuenta, debería ser guardada de forma segura.

Facebook *respondió* que en la sección “ayuda” se puede encontrar un vínculo a “Yo quiero eliminar mi cuenta de forma permanente”, donde se explica al usuario que una vez que escoge eliminar la cuenta, toda su información se volverá inaccesible para los otros miembros de la red, lo que significa que la persona desaparecerá del servicio de Facebook. Pero que si la persona decide reactivar la cuenta en algún momento, Facebook guarda toda su información para que la cuenta aparezca tal cual estaban antes de su desactivación.

Si es que usted piensa que no volverá a utilizar su cuenta de Facebook otra vez y desea que su cuenta sea eliminada, podemos hacerlo por usted, pero tenga en cuenta que no podrá reactivarla ni encontrar todo su contenido o la información que usted haya añadido. Si usted desea que su cuenta sea permanentemente eliminada sin opción a recuperación, por favor envíe su solicitud aquí (Report of Findings 2009, 59).

La comisaria asistente de privacidad de Canadá *recomendó* que Facebook incluyera una opción de eliminación de cuenta y una explicación de la diferencia entre desactivar y eliminar una cuenta en la configuración de cuenta del usuario. Facebook no aceptó la recomendación.

Cuentas de personas fallecidas

CIPPIC *demandó* que Facebook obligaba a sus usuarios a consentir, en las Condiciones del servicio, mantener activos los perfiles de personas fallecidas, algo que no cumple el objetivo primario de la red: ofrecer un entorno de sociabilidad en este mundo virtual. Facebook debería eliminar el perfil de una persona fallecida si sus familiares así lo requirieren. De igual modo, debería conseguir el consentimiento de los usuarios a mantener activos los perfiles de personas fallecidas como un homenaje en caso de que así lo desearan los herederos, y colocar en su política de privacidad lo que ya consta en sus términos de uso.

Facebook *respondió* que cuando se le notifica del fallecimiento de un miembro, normalmente mantiene activa la cuenta por un tiempo, para que los amigos puedan rendirle homenaje y que tengan acceso a los comentarios. Indicó que en su Centro de Ayuda hay un mecanismo para reportar fallecimientos y seguir el procedimiento. La comisaria asistente de privacidad de Canadá encontró que Facebook, al omitir una opción para que los usuarios decidan sobre el futuro uso de su información personal con el objeto de que se les rinda un homenaje, les exigía, por omisión, el consentimiento como una condición del servicio. Por tanto, *recomendó* que Facebook otorgue control al usuario para escoger con una opción *opt-out* si no desea que su cuenta permanezca abierta, incluso si es con fines de homenaje. Facebook no aceptó incorporar esta opción.

Información personal de no-usuarios

CIPPIC *demandó* a Facebook por no haber obtenido el consentimiento de quienes no son usuarios, para utilizar la información subida a la red por los usuarios, a través de sus comentarios en sus perfiles, el muro, News Feed, las etiquetas de fotos o videos donde aparecen con sus nombres o correos electrónicos cuando sus amigos los invitan a ser parte de

la red. CIPPIC consideró que Facebook debería prohibir a sus usuarios subir esa información, sin el consentimiento de esas personas, y que debería penalizarlos, de algún modo, cuando suban material no autorizado; si persistieran, debería incluso eliminar sus cuentas. De igual modo, Facebook debería contactar a quienes no son usuarios para que descubran la información personal que circula en la red y removerla del sitio.

Facebook *respondió* que [la Comisaría]

da mucha importancia a los no-usuarios y a la presencia de información vinculada a ellos en su sitio más que otros sitios en la web. Si un no-usuario desea bloquear futuras notificaciones, Facebook atiende su pedido y la información es retenida en la dirección del usuario que subió los datos, e incluso puede ser eliminada por Facebook si la información es inapropiada, sin que intervenga la acción de quien subió los datos en primer lugar (Report of Findings 2009, 77).

La comisaria asistente *recomendó* que Facebook considere implementar medidas sobre la falta de conocimiento de quienes no son usuarios y sobre su consentimiento cuando son etiquetados en fotografías. Exhortó también a que se considere implementar medidas para mejorar la falta de conocimiento de los no-usuarios sobre la recolección, uso y retención de sus correos electrónicos, y definir un tiempo razonable sobre la retención de los mismos.

No obstante, los puntos de la demanda que, según la comisaria asistente, no están bien argumentados por parte de la CIPPIC son: a) nuevos usos de la información, b) recolección de información en fuentes distintas a Facebook, c) Facebook Mobile y salvaguardias, d) engaño y desinformación.

Nuevos usos de la información

CIPPIC *demandó* que Facebook no estaba notificando a los usuarios sobre los nuevos usos de su información personal cuando la recolecta, utiliza y difunde, y que Facebook debería comunicarles y conseguir su consentimiento antes de utilizar y difundir información personal con nuevos propósitos. CIPPIC no logró identificar ninguna instancia en la

que Facebook hubiera introducido nuevos propósitos para el uso de la información, sin haber notificado a los usuarios y obtenido su consentimiento.

Recolección de información desde fuentes distintas a Facebook

CIPPIC *demandó* que Facebook había fallado al proveer a sus usuarios información específica relacionada con los propósitos y métodos de recolección de información personal de fuentes ajenas a Facebook, así como sobre el uso y divulgación de dicha información; por tanto, no había obtenido su consentimiento informado. En la investigación realizada por la comisaria asistente no se encontraron vestigios sobre el fundamento de la demanda dentro de las prácticas de Facebook.

Facebook Mobile y Salvaguardias

CIPPIC *demandó* que Facebook utilizaba *cookies* que no tenían fecha de expiración en su versión Mobile Facebook, lo que impedía salvaguardar apropiadamente la información personal de los usuarios, y que tenía fallos de seguridad en dos casos: cuando una persona ingresa a Facebook desde el teléfono móvil de otra persona y olvida salir de su cuenta, la otra persona puede ingresar a su cuenta de forma indefinida, incluso si cambia su clave; si un usuario entrega a una persona su contraseña de Facebook, ella puede ingresar a su cuenta desde un dispositivo móvil de forma indefinida, incluso si el usuario cambia su contraseña. Por tanto, solicitó el uso de *cookies* con fecha de expiración en los dispositivos móviles y que se desactiven cuando los usuarios cambien sus contraseñas.

En la investigación realizada por encargo de la comisaria asistente se descubrió que las *cookies* expiraban en un periodo de 14 días, luego de lo cual se solicitaba la autenticación del usuario al entrar al sitio, lo cual extendía el periodo de duración de las *cookies* otros 14 días. Igualmente se determinó que las prácticas de Facebook no diferían de las de otros servicios que permiten conexiones desde dispositivos móviles. Por tanto, la argumentación de la demanda no fue sólida.

Engaño y desinformación

CIPPIC *demandó* que Facebook desinformaba cuando señalaba que era puramente un sitio de sociabilidad en línea, puesto que en realidad desarrollaba otras actividades que no eran explicadas de forma clara, tales como publicidad y participación de terceros. También demandó que Facebook desinformaba sobre el nivel de control de los usuarios sobre su información. La comisaria asistente de privacidad de Canadá indicó que no existían evidencias de que Facebook desinformara o engañara a sus usuarios sobre el objeto de la recolección de la información o, que colectara información de sus usuarios engañándolos. Por tanto, consideró que esta demanda no estuvo bien fundamentada.

La demanda contra Facebook realizada en Canadá me permite analizar los argumentos legales puestos en juego cuando la privacidad está en riesgo. Por tanto, me ayuda a co-construir la noción de privacidad que los actores manejan para el ciberespacio, dentro de un proceso en el que participan administradores, organizaciones protectoras de la privacidad, gobiernos, centros de investigación universitarios, grupos de trabajo, asesores y fiscales generales. Nos muestra, igualmente, las versiones de privacidad que se estabilizan dentro del código y el valor de la regulación para normar comportamientos en el ciberespacio. La relación código-regulación (Lessig 2006; Vercelli y Thomas 2007) es muy visible en esta controversia y merece ser explicada no solo usando los textos que estabilizan las acciones de los códigos, sino también por la invisibilización de las acciones que deben realizar los sujetos para defender su privacidad dentro de la red.

El primer punto que reconoció la comisaria asistente de privacidad de Canadá fue que “no todos entienden la privacidad desde el mismo prisma”,¹⁶ las redes sociales son un fenómeno que ha mostrado el deseo que tienen las personas de publicar sus vidas en línea. Asimismo, el cambio de tecnologías y de normas sociales volvía imperativo el rol de la Comisaría para proteger la vida privada de la ciudadanía, utilizar la normativa legal para crear un entorno donde el oxímoron *privacidad en*

¹⁶ “News and announcements”, Blog de la OPC, http://www.priv.gc.ca/media/sp-d/2009/sp-d_20090716_e.asp

público no menoscabara las expectativas de privacidad de quienes habitan los entornos digitales, y se reconocieran las protecciones a la privacidad por parte de los servicios de redes sociales en línea. Las autoridades de Facebook dejaban la responsabilidad sobre develar información privada tan solo en los usuarios, especialmente cuando la mayoría no cuidaba suficientemente su propia privacidad. Los dueños de los sitios web deben estar obligados a instalar medidas de protección dentro de sus sitios, para asegurar que el espacio que los usuarios utilizan sea lo suficientemente protegido y seguro (Hongladarom 2011).

Para la funcionaria, el cambio de la sociabilidad desde el mundo fuera de la web a la pantalla conllevaba grandes cuestionamientos sobre lo que significa tener un “sentido de lo privado”. Por ello, consideró primordial sensibilizar a las personas para que balancearan los beneficios de la socialización en línea y el conocimiento de que lo que publican “nunca es del todo privado”. Facebook tan solo requiere de sus usuarios cuatro datos: nombre, correo electrónico, fecha de nacimiento y género; el resto es entregado voluntariamente por los miembros de la red en sus interacciones dentro del sitio. Las personas publican información privada por razones puramente personales en un contexto definido como privado al escoger quiénes acceden a qué información sobre sí mismas. Sin embargo, desde ese momento, Facebook monitoreaba las acciones de los usuarios y utilizaba su información para fines comerciales (Report of Findings 2009, 6-8).

Si bien el informe de la Comisaría de Privacidad de Canadá se basó en una demanda legal donde la información personal, el derecho a la autodeterminación del sujeto y las expectativas de privacidad fueron los principios fundamentales para proteger lo privado, es muy relevante que en el mismo se tome en cuenta las acciones de los sujetos, la producción de normas sociales dentro de Facebook y la estandarización de comportamientos (tabla 6).

Tabla 6. Acciones de los actores

	Acciones
Usuarios	<ul style="list-style-type: none"> - Consentir. - Conocer informadamente. - Producir contenidos voluntariamente. - Interactuar con otros y comentar. - Optar por configuraciones de cuenta y de privacidad. - Salir del circuito de publicidad social. - Reportar y denunciar abusos. - Detectar problemas y reclamar su solución.
Terceros (desarrolladores de aplicaciones)	<ul style="list-style-type: none"> - Recolectar información. - Almacenar información. - Desarrollar aplicaciones. - Negociar con Facebook la publicidad.
Facebook en el ámbito legal	<ul style="list-style-type: none"> - Diseñar políticas, normativa y códigos de ética. - Garantizar seguridad. - Informar adecuadamente a los usuarios. - Regular las acciones de los usuarios. - Reglamentar el uso de la información de los usuarios. - Reglamentar el uso de Facebook y de la información de los usuarios por terceros. - Invisibilizar, a través del lenguaje, usando eufemismos, algunas acciones de Facebook.
Facebook a nivel del código	<ul style="list-style-type: none"> - Configurar el espacio virtual. - Normar las acciones de los usuarios. - Limitar las posibilidades de interacción en la arquitectura del sitio. - Recolectar información. - Monitorear. - Rastrear. - Sistematizar la información de los usuarios, sus prácticas y sus intereses. - Construir <i>dossiers</i> digitales. - Volver viable el principio de transparencia radical.

El análisis de las acciones permite superar la construcción de la privacidad desde la información, pues al examinar aquellas que definen las relaciones entre Facebook y sus usuarios se explica la tecnologización de la regulación a través del proceso sociotécnico que se establece entre las capas social y tecnológica del artefacto: el código se vuelve más social y las acciones de los usuarios se estructuran según el diseño tecnológico de la red (Oudshoorn y Pinch 2005; Thomas 2008; Vercelli y Thomas 2007). La incorporación de las acciones al proceso de co-construcción es un elemento clave de esta controversia, porque revela los momentos de negociación de la privacidad entre los distintos actores.

La *negociación* de esta controversia se realizó a través de un proceso de co-construcción entre las relaciones que CIPPIC y Facebook establecieron con otras entidades y actores estatales, mediante los acuerdos a los que se llegaron en cuatro puntos: los cambios de Facebook sobre el texto informativo de los usos que se hará sobre la fecha de nacimiento de los usuarios; la incorporación del código a la configuración de privacidad; la inclusión del texto sobre la función de la publicidad en Facebook; y el monitoreo de actividad anómala.

- Fecha de nacimiento: se indicó que la recolección de la información tiene usos publicitarios y se introdujo la frase:

Facebook requiere a todos los usuarios proveer su verdadera fecha de nacimiento para asegurar la autenticidad y proveer acceso a contenido apropiado a la edad. Usted será capaz de esconder esta información si lo desea y su uso será gobernado por la Política de Privacidad de Facebook (Report of Findings 2009, 17).

- Configuración de privacidad: cambió la configuración predeterminada de “todos” a una optativa en los controles para álbumes de fotos e instaló el sistema Privacy Wizard para configurar niveles predeterminados de privacidad (bajo, mediano, alto), así, los motores de búsqueda no pueden publicar información sobre los perfiles con configuración de privacidad “alta”. Además, se incorporó nuevo código para ofrecer controles más granulares sobre los contenidos producidos.

- Publicidad: incluyó un nuevo texto para explicar mejor el rol de la publicidad dentro de la red.
- Monitoreo de actividad anómala: [Facebook incluyó el siguiente párrafo]

Para mejorar la seguridad del sitio Facebook utiliza una variedad de sistemas tecnológicos para detectar y resolver actividad anómala que pueda ser llevada a cabo por los usuarios. Ello puede ocasionar que Facebook suspenda de forma temporal o permanente algunas de las funciones de algunos usuarios del servicio de Facebook (Report of Findings 2009, 86).

En la demanda, Facebook aceptó incorporar un código para que los usuarios tuvieran controles más granulares sobre la información, pero no admitió consolidar los controles de privacidad en un solo lugar y con ello volver más amigable la configuración personal de los usuarios. Facebook insistió en que su principio de obligar a los usuarios a utilizar su identidad real los responsabiliza de sus acciones y con ello se minimizan los abusos dentro de la red social. Para Facebook, la confianza de los usuarios en el sitio permitía establecer el sistema de confianza y asegurar que sus intereses estaban protegidos, que no sufrirían daño alguno, directa o indirectamente en su interacción con la tecnología. Sin embargo, la necesidad de la protección de la privacidad debía extenderse a los datos mismos, ya que son, en un sentido real, parte del ser individual (Hongladarom 2011).

Everyone: la quinta controversia sobre la privacidad en Facebook

A fines del año 2009, Facebook cambió la configuración de los controles de privacidad de su artefacto. Expuso, así, en un lapso, la información de los usuarios cuando la nueva configuración entró en vigencia. A pesar del esfuerzo realizado para explicar a los usuarios cómo agrupar a los amigos y asignarles distintos niveles de acceso a la información, el cambio del acceso a los datos (de “nadie” a “todos”)

provocó graves problemas. El 1 de diciembre, Zuckerberg escribió en el *Blog de Facebook*:

Hemos diseñado un plan para eliminar las redes regionales completamente y crear un modelo simple de control de la privacidad, donde ustedes pueden consentir que su contenido sea visto solo por sus amigos, amigos de sus amigos, o todos. Estamos añadiendo algo que muchos de ustedes han solicitado –la habilidad de controlar quién ve cada pieza individual de contenido que ustedes crean y publican–. Además estamos respondiendo al pedido de muchos, de simplificar la configuración de privacidad al combinar varios grupos de controles. Nosotros empezamos a discutir esto en julio [...] en las próximas semanas les pediremos que revisen su configuración de privacidad. Ustedes verán un mensaje que explicará los cambios y que los llevará a la página donde podrán actualizar su configuración. Cuando terminen, aparecerá otra página de confirmación para que se aseguren que han escogido la configuración adecuada para ustedes. [...] Hemos trabajado por desarrollar controles que pensamos son mejores para ustedes, pero entendemos que todos necesitamos ser diferentes. Les sugeriremos configuraciones basados en su actual nivel de privacidad, pero el mejor modo de que ustedes encuentren los controles adecuados es que entiendan todas las opciones y personalicen su configuración ustedes mismos. Les animamos a hacerlo y a considerar con quién comparten en línea.¹⁷

La nueva configuración de privacidad tuvo varias lecturas apenas fue implementada; si bien se reconoció que podía ayudar a los usuarios a controlar mejor quién veía su información, también se observaron otras motivaciones. Según Brad Stone (2009a, 2009b), articulista del *New York Times*, podía ser una movida calculada para arreglar algunos problemas vinculados a su inmenso crecimiento y competir con sus rivales Google y Twitter hasta convertirse en el más importante repositorio de información que la gente pudiera tener en tiempo real. Se cuestionó que Facebook estuviera guiando implícitamente a que las personas relajaran su configuración de privacidad, a través de la configuración predeterminada, puesto que muchos usuarios no cambiaban sus controles de

¹⁷ Información desaparecida de la web, <https://blog.facebook.com/blog.php?post=190423927130>

privacidad. En vez de diseñar configuraciones cada vez más abiertas se debería ofrecer configuraciones que protegieran mejor la información de los usuarios.

EPIC criticó los cambios en este sentido y advirtió que los usuarios publicaban cada vez más sobre sí mismos de forma inadvertida y más allá de sus intenciones. En este *contexto*, pocos días más tarde EPIC presentó una demanda legal en contra de Facebook, en conjunto con otras organizaciones,¹⁸ ante la Comisión Federal de Comercio. Allí se señaló:

Esta demanda se refiere a los cambios materiales realizados por Facebook en la configuración de privacidad, la red social más grande en los Estados Unidos, que de forma adversa está impactando a los usuarios del servicio de Facebook. Los cambios realizados por Facebook a la configuración de privacidad vuelven pública información personal que antes estaba restringida. Los cambios de los controles de privacidad de los usuarios también exponen información personal que antes era restringida a terceros. Estos cambios violan las expectativas de privacidad y disminuyen sus posibilidades de ejercerlas, además contradice las propias representaciones de Facebook. Estas prácticas de negocios son desiguales y son prácticas de comercio engañosas, sujetas a revisión por la Comisión Federal de Comercio bajo la sección 5 del Acta de la Comisión Federal de Comercio.¹⁹

EPIC defendía el derecho a la privacidad apelando a la noción de autodeterminación informacional y expectativas de privacidad. Así, enfatizaba que la recolección, uso y diseminación de información personal podía afectar las oportunidades de empleo, aseguramiento, crédito y la obtención de servicios médicos, debido al peligro que implicaba el mal uso de la información recopilada sobre los usuarios de Facebook. El momento en que la información se vuelve pública bajo la categoría de “todos”, la información de estos perfiles puede ser vista prácticamente por todo el mundo (motores de búsqueda, personas que no son miembros de la red) sin ningún límite.

¹⁸ American Library Association, The Center for Digital Democracy, Consumer Federation of America, Fool Proof Financial Education, Patient Privacy Rights, Privacy Activism, Privacy Rights Now Coalition, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation.

¹⁹ Demanda del 17 de diciembre de 2009.

Para EPIC las políticas de privacidad poco claras eran el mayor problema para los consumidores, quienes no entendían qué significaba su “consentimiento”.²⁰ Se *reclamaba* que las políticas de privacidad se habían vuelto exenciones en vez de políticas y los usuarios las asociaban con protección de la privacidad. Las políticas de privacidad eran fluidas, cambiaban constantemente y, en la práctica, cuando las redes sociales deciden cambiar sus políticas de privacidad, cambian igualmente la configuración predeterminada.

Las acciones de Facebook lesionan a los usuarios en Estados Unidos al invadir su privacidad; ello permitiendo la exposición y uso de su información de acuerdo con propósitos distintos a aquellos consentidos o invocados por los usuarios; ocasionando que crean falsamente que tienen total control sobre el uso de su información, y disminuyendo su habilidad de confiar en ellos mismos y en las protecciones prometidas por la compañía.

Una prueba de que para Facebook la privacidad no era prioritaria fue la declaración de Mark Zuckerberg, en enero de 2010, cuando indicó que la privacidad ya no era una “norma social”. En una entrevista con Michael Arrington, fundador de TechCrunch, Zuckerberg declaró:

Cuando empecé en Harvard, la pregunta que mucha gente me hacía es ¿por qué quisiera yo subir información a internet? ¿Por qué me interesaría tener un sitio web? Y luego de 5 o 6 años el blog y todos estos servicios donde la gente comparte todo tipo de información ha tomado tanta fuerza. La gente se ha vuelto muy cómoda no solo compartiendo información de distintos tipos, sino que se ha vuelto más abierta a los otros. Esta norma social es algo que ha evolucionado con el tiempo. Nuestro rol es innovar y actualizar el sistema para que refleje lo que son las normas sociales actualmente. Muchas compañías estarían atrapadas por las convenciones y por los legados de lo que han construido; al hacer un cambio en la privacidad –un cambio para 350 millones de usuarios no es el tipo de cosa que muchas compañías quieren hacer–. Pero nosotros consideramos

²⁰ Los grupos de privacidad que acompañaron a EPIC en su demanda contra Facebook consideraban que los controles de privacidad de la red social estaban “diseñados para confundir a los usuarios y para frustrar sus intenciones de limitar la exhibición de la información personal que, en principio, han escogido compartir con su familia y amigos” (I. Paul 2010, en línea).

que es algo muy importante el mantener una mente de principiantes, lo que haríamos si recién estuviéramos empezando una compañía ahora, y hemos decidido que esta sería la norma social ahora y fuimos por ella (citado por M. Kirkpatrick 2010, en línea).

Ante la demanda de EPIC reaccionaron varios actores: usuarios, bloggers, senadores, articulistas, académicos, expertos en privacidad y los voceros de Facebook. Tan solo cuatro días después de que Facebook realizara los cambios de configuración a “todos”, se organizaron más de 500 grupos en contra dentro de la red social. Más de 1050 miembros se volvieron fans del grupo *En contra de la nueva configuración de privacidad de Facebook*. Este grupo demandaba “que Facebook deje de forzar a las personas a revelar cosas que no se sienten cómodas revelando”.²¹ En el grupo *Facebook! Arregla la configuración de privacidad* más de 950 usuarios reclamaban que

Facebook ha cambiado su política de privacidad y ahora nuestras listas de amigos, páginas, fotos de perfil y otros tipos de información son públicas para personas que no sabemos por qué los buscan en Facebook. Estupendo para acosadores, anunciantes, empleadores, autoridades, etc. Muy malas noticias para el resto de nosotros. Dile a Facebook que nuestra información personal es privada y que queremos controlarla.²²

Más de 74 000 usuarios formaron el grupo llamado *Petición: Facebook para de invadir mi privacidad* y protestaron porque, una vez más, Facebook la había vulnerado al imponer una nueva configuración de privacidad a más de 365 millones de usuarios:

los nuevos controles nos dan MENOS privacidad que antes, por lo que nos preguntamos ¿cómo exactamente esto nos hace sentir más seguros? [...] Tal vez la parte más frustrante es que los cambios que Facebook ha hecho se supone que son hechos para nuestro bien, sin que realmente se nos haya advertido o preguntado sobre ellos.

²¹ “En contra de la nueva configuración de privacidad de Facebook”, *Blog de Facebook*, acceso el 15 de abril de 2011, <http://www.facebook.com/group.php?gid=209833062912>

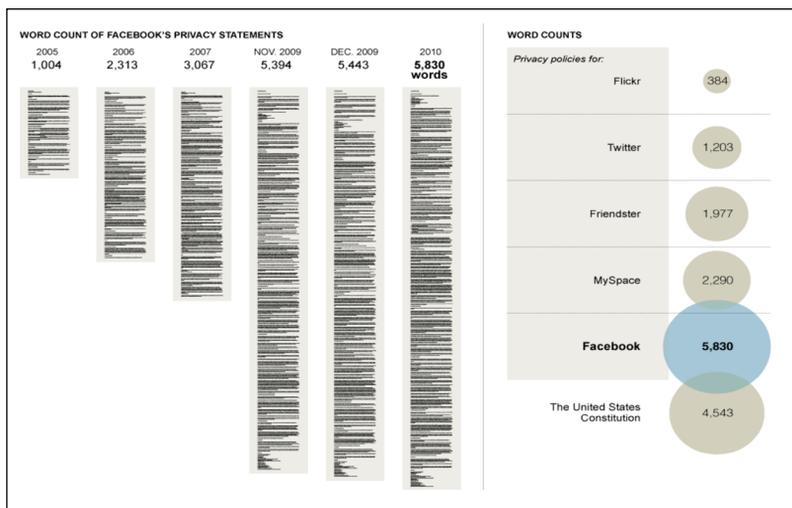
²² “Facebook! Arregla la configuración de privacidad”, *Blog de Facebook*, acceso el 15 de abril de 2011, <https://www.facebook.com/groups/192282128398/>

Entre los dos mil comentarios realizados por los usuarios en el *Blog de Facebook*, donde se discutían los cambios de la configuración de privacidad, varios miembros escribieron: “Vine aquí a comunicarme con gente con quien tengo una conexión personal, no para que mi información personal sea provista a terceros, de forma inescrupulosa, y sea pública para potenciales acosadores o ladrones de identidad”; “Me gustaban los antiguos controles de privacidad. Me hacían sentir más seguro, como que tenía mayor control”.

Para comprender la complejidad del uso de los controles de Facebook, Guilbert Gates publicó un artículo en mayo de 2010 en el *New York Times*. Allí muestra que Facebook ofrece 50 configuraciones y 170 opciones de privacidad; además presenta el aumento del número de palabras en sus declaraciones de privacidad y lo compara con el de otras redes sociales, e incluso con la constitución norteamericana (gráfico 11).

Sin embargo, no todos los usuarios pensaban que la privacidad estuviera en riesgo y consideraron que la demanda de EPIC no tenía sentido.

Gráfico 11. Número de palabras utilizadas en las declaraciones de privacidad en Facebook



Fuente: Gates 2010, en línea.

[Facebook está] tratando de promover que los usuarios compartan más información [...]. Al contrario que EPIC no creo que esto sea una cosa mala, mientras lo hagan correctamente. Si EPIC se saliera con la suya, eso impondría a todos el mandato “No debes compartir a menos que hayas chequeado esta casilla y hayas realizado todos los cambios en los controles detalladamente” [...]. Yo pienso que esto es injustificado porque la mayoría de usuarios no está preocupados de la información que comparte, y para aquellos que sí lo están esta solución es una forma de empoderarlos (Szoka 2009, en línea).

Académicos y expertos en privacidad también se pronunciaron en esta controversia. En opinión de Ed Felten, profesor de la Universidad de Princeton, la política de Facebook era un engaño; intentaba que las personas perdieran el control sobre la información, y aunque al inicio, las declaraciones de Zuckerberg sugerían que la nueva configuración era proprivacidad, en realidad hacía más pública la información de los usuarios. Para Joseph Bonneau, experto en seguridad de la Universidad de Cambridge, que la lista de amigos, una de las piezas más sensibles de información que poseen los usuarios, fuese pública representaba un gran riesgo, debido a las prácticas de uso de la información, estafa, engaño y cruce de redes. Según Graham Cluley, experto en seguridad, al volver pública la información a través de “todos”, lo que realmente sucedía era un “todos para siempre”, pues incluso si las personas cambiaban su configuración de privacidad más tarde ya habían perdido el control sobre lo que otras pueden hacer con su información fuera de Facebook; “hay un gran riesgo en que la gente siga las recomendaciones de Facebook sin considerar cuidadosamente sus posibles consecuencias”.²³

Jared Newman (2009), articulista de *PC Word*, entre otros, consideraba que el trasfondo de la configuración de privacidad preseleccionada de Facebook era compartir todo el perfil para volver más fácil que los encuentros, identificaciones y aprendizajes entre amigos; en realidad debería ser leído “haga más fácil que todo el mundo pueda encontrar su identidad y sobre usted”. Pete Cashmore, el fundador de Mashable, un sitio de medios sociales productor de noticias, sostuvo en CNN que “la

²³ Demanda EPIC 2009, 19-21, https://epic.org/privacy/facebook/EPIC_FB_FTC_Complaint_Letter.pdf

privacidad ha muerto y los medios sociales son los responsables”, pues han exponenciado la información personal, para que esté disponible en internet (Evangelista 2009, en línea).

Para Irene North (2010) del *Daily Censored*, Facebook se había convertido en el Gran Hermano: la gente entrega voluntariamente información personal que permite monitorear a sus amigos y familia; mientras Facebook hace *lobby* para proteger al país de espías, permite que todos vean dónde están sus usuarios a través de los servicios de GPS, quiénes son sus amigos por medio de las etiquetas en las fotos. “Facebook ha desarrollado las herramientas para permitir que cualquier agencia, en el país, sepa todo lo que hacen sin tener que conseguir ninguna orden de allanamiento para ello, [...] ha logrado entregar a sus usuarios una ilusión de privacidad en un lugar público”.

Los senadores Charles E. Schumer, Michel F. Bennet, Mark Begich y Al Franken²⁴ escribieron una carta a Zuckerberg en la cual indicaron su preocupación sobre tres puntos: la expansión de información pública revelada por los nuevos controles de privacidad, el almacenamiento de datos por parte de terceros y la personalización instantánea. En todos los casos, estaba en riesgo la información personal tanto de los usuarios como de sus contactos, y confiaban en que Facebook creara comunidades abiertas y transparentes que aseguraran políticas de protección de la información biográfica sensible de sus miembros.²⁵ El senador Schumer incluso solicitó al director de la Comisión Federal de Comercio que examinara las prácticas de exposición de la información de quienes usan redes sociales, que corrigiera los excesos de apertura para que terceros accedieran a esta información y que dictara guías para las compañías sobre cómo proteger la información privada y prohibir el acceso sin el permiso del usuario.

En mayo de 2010, Zuckerberg publicó un artículo, en el *Washington Post*, en el que se puede vislumbrar los términos de la negociación de esta controversia. Cuando los usuarios protestan, Facebook escucha y

²⁴ EPIC envió una carta a estos cuatro senadores días después (5 de mayo de 2010) de que ellos enviaran un comunicado a Mark Zuckerberg (27 de abril de 2010), en el cual EPIC daba a conocer la demanda contra Facebook ante la Comisión Federal de Comercio, y la resistencia de la Comisión a tomar una resolución en este caso.

²⁵ Demanda EPIC 2009, Anexo 6.

responde a los reclamos de sus miembros; no obstante, los usuarios sostienen que los controles de privacidad que Facebook ofrece son muy complicados y que las personas necesitan controles más fáciles. Si bien la política de Facebook ha sido ofrecer control granular de la información ahora buscará el modo de volverlo más sencillo.²⁶ Zuckerberg puntualizó los principios que rigen a Facebook:

Usted tiene el control sobre la información que comparte. No compartimos su información personal con personas o servicios que usted no quiera. No le entregamos acceso a su información personal a los anunciantes de publicidad. Nunca venderemos su información a nadie. Siempre mantendremos Facebook como un servicio gratuito para todos.²⁷

Tres meses más tarde, Facebook implementó una característica llamada “lugares”, que permite a los usuarios visibilizar dónde están a través de una opción *opt-in*.

¿Algunas vez fuiste a un show y te enteraste más tarde que tus amigos también asistieron? Con “lugares” puedes descubrir si tú y tus amigos se encuentran en el mismo lugar en el mismo tiempo. Tienes la opción de compartir tu ubicación y permitir que tus amigos sepan dónde estás y también ver si tus amigos se encuentran cerca (Eyal 2010, en línea).

Con este proyecto Facebook inició todo un proceso de visualización de los movimientos de los usuarios fuera de internet. Open Graph saltó fuera de la pantalla para rastrear a las personas en sus recorridos por el mundo físico. Ya se había probado, en abril de 2010, un sistema de visualización presencial durante el encuentro f8 (ilustración 18).

Con “lugares”, no solo se implementó este nuevo sistema de seguimiento de los recorridos de las personas en tiempo real; también se generó el código para que los usuarios compartieran más información con los desarrolladores de aplicaciones, como dirección, número de teléfono móvil y la autenticación social (ilustración 19).

²⁶ La popularidad de Facebook contrastaba con su Índice de Aceptación de Consumidores (ACSI), que la ubicaba en el número 64 de ese ranking, por debajo incluso del Servicio de Rentas Internas de los Estados Unidos (IRS) y equiparaba sus niveles de satisfacción con los de las aerolíneas o las empresas de televisión por cable. <https://bit.ly/3fRuAYG> (contenido fuera de línea).

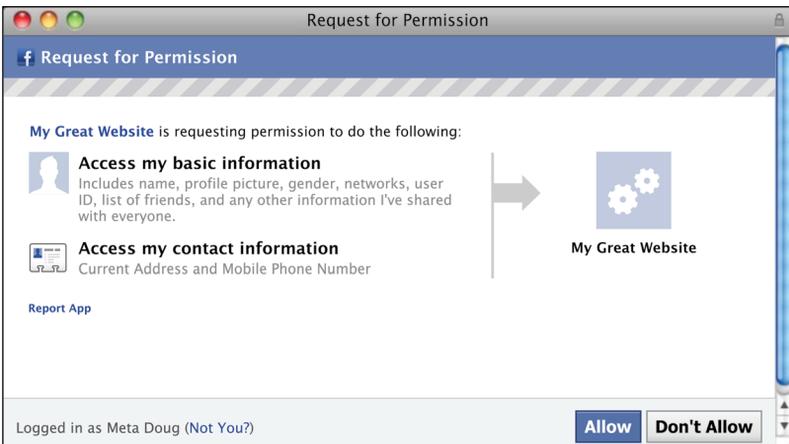
²⁷ *Washington Post*, 24 de mayo de 2010, (contenido fuera de línea), <https://wapo.st/33Hmgpm>

Ilustración 18. Visualización presencial en el f8, abril de 2010



Fuente: http://allfacebook.com/facebook-tests-location-through-rfid-at-f8_b13794.

Ilustración 19. Autorización para entregar número de teléfono celular y dirección a los desarrolladores de aplicaciones



Fuente: Bowen 2011, en línea .

Desde el f8, Zuckerberg enfatizó los nuevos modos en que Facebook entraba en contacto más directo con la vida de las personas; así, un usuarios conectado podría saber qué leen, en qué parte de la ciudad se encuentran

o a qué espectáculo asisten sus amigos. A estos nuevos límites a los que se empujó la privacidad de los usuarios le siguieron textos tranquilizadores como el Chris Cox,²⁸ quien escribió el siguiente mensaje a los usuarios: “Su perfil debería sentirse como su hogar en la web, ustedes nunca deberían sentir que en él aparecen cosas que no quieren y nunca deberían preguntarse quiénes pueden ver lo que está ahí” (2011, en línea).

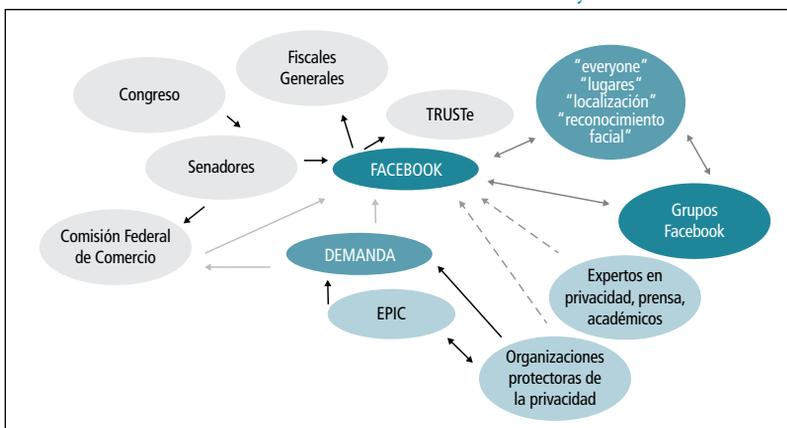
En esta controversia entró en disputa el nuevo sistema de controles de privacidad que, por configuración predeterminada, volvió pública la información de los usuarios no solo a todos los miembros de la red, sino a los desarrolladores de aplicaciones y a los motores de búsqueda. Así, la información que antes estaba protegida tanto por el sistema como por la opción del usuario en la personalización de su privacidad, quedaba expuesta al escrutinio de todos. El segundo punto de la controversia fue la promesa de Facebook de no compartir la información de los usuarios con terceros, y lo hizo. El tercer punto es haber confirmado que Verified Apps funcionaba perfectamente, pero los desarrolladores de aplicaciones estaban recolectando de forma permanente más de un 90 % de información de los usuarios innecesaria para que la aplicación funcionara. Finalmente, Facebook ofreció que las fotos y los videos de las cuentas cerradas no estarían disponibles para ser compartidos y solo permitió el acceso a estos contenidos.²⁹

En la *negociación* de esta controversia intervinieron actores diversos: organizaciones, artefactos, código, demandas, al igual que sujetos que declararon a favor y en contra de Facebook. Participaron las organizaciones de protección de la privacidad lideradas por EPIC, senadores de los Estados Unidos, el fiscal general, el Congreso norteamericano, a través de las demandas de sus senadores a Facebook y a la Comisión Federal de Comercio. También expertos y académicos se expresaron en los medios sobre las nuevas aplicaciones y los Términos de Privacidad que Facebook fue implementando en los dos años que duró la controversia junto con los grupos de usuarios que protestaron (gráfico 12). Todos los actores mantienen una alta flexibilidad interpretativa (Bijker 1995) que, disputa la propia función del artefacto hasta estabilizar una gramática (Thomas 2008) de la privacidad en Facebook.

²⁸ Fue uno de los programadores de código para los controles de privacidad de News Feed.

²⁹ Demanda de EPIC a Facebook ante la Comisión Federal de Comercio, <https://bit.ly/2RB5BOC>

Gráfico 12. Actores de la controversia Everyone



Para Facebook la privacidad había dejado de ser una norma social por que el cambio tecnológico había condicionado el sentido de la relación entre los sujetos y su forma de habitar el ciberespacio. En los primeros años de Facebook los sujetos se preguntaban para qué necesitaban escribir sobre sí mismos en sitios web personales. Poco a poco las personas fueron deseando contar quiénes eran, cómo se sentían, qué hacían y con quién, de forma pública y ante una audiencia escogida por ellas. La arquitectura del artefacto fue promoviendo la internalización de una privacidad reducida, que difícilmente puede reclamar amplias expectativas de privacidad (Alpert 2006). La evolución del código no fue neutra y estuvo acompañada de un proceso intenso de co-construcción entre los programadores, Zuckerberg, usuarios, sistemas legales, gobiernos, activistas y medios. El cambio tecnológico de Facebook se inspiró en un modelo de negocios donde el Free Labor (Terranova 2000) ha sido un elemento fundamental para su éxito; igualmente, en una noción de transparencia radical (Zuckerberg 2010), en un sistema de confianza que permita que los usuarios se sientan seguros y protegidos en el entorno virtual de la red, y en considerar a la norma social un elemento fundamental para moldear comportamientos condicionados por la capa tecnológica del artefacto (Solove 2006, 2008).

Para entender cómo es posible que la tecnología de Facebook lograra estas transformaciones es necesario tomar en cuenta no solo las

características del artefacto sociotécnico, sino también el sistema social y económico en el que se inserta. Esta controversia resulta relevante para explicar el fenómeno de la privacidad en la red social en sus inicios, porque revela un sistema de regulación que funcionaba afuera de la red, en las instituciones gubernamentales y las capacidades de actores externos a Facebook para regular la evolución del código dentro del ciberespacio.

Los usuarios pueden tener expectativas de privacidad (Poulet y Rouvroy 2009) dentro de Facebook porque están protegidas, legal y socialmente, fuera de la web. Dichas expectativas están reforzadas por normas sociales (Solove 2008) que evolucionan con los sujetos y sus contextos. El contexto de Facebook es un ciberespacio regulado, cuidadosamente, por la arquitectura del código, son los programadores quienes diseñan su naturaleza y las formas en que la privacidad será o no protegida (Lessig 2006). La naturalización de expectativas cada vez más limitadas con respecto a la privacidad tiene que ver con la función que cumplió el diseño de la red para condicionar el cambio de la norma social.

Cuando Zuckerberg declaró que “la privacidad ya no era una norma”, lo que realmente mostró es que su proyecto de transparencia radical era exitoso, y que su diseño de un lugar firmemente regulado por la tecnología estaba logrando controlar las formas de socialización de los sujetos, sin que este moldeamiento social fuera percibido, necesariamente, como peligroso. Aunque las protestas contra Facebook sobre su falta de protección a la privacidad de los usuarios no han sido pocas y han sido protagonizadas por gobiernos, políticos e instituciones protectoras de la privacidad, en la resolución de esta controversia, no lograron frenar la estrategia de Facebook: dar dos pasos agresivos adelante y retroceder con un pequeño paso atrás (Hoofnagle y Zimmer 2010).

Casi dos años más tarde de que EPIC y sus organizaciones aliadas presentaran su demanda contra Facebook ante la Comisión Federal de Comercio, esta finalmente resolvió:

Prohibir que Facebook describa de forma engañosa las condiciones de privacidad y de seguridad de la información personal de los consumidores; se le requiere que obtenga de los usuarios su consentimiento expreso antes

de realizar cambios que afectan sus preferencias de privacidad; se le requiere que prevenga a cualquiera de obtener el acceso al material de los usuarios luego de pasados 30 días de que el usuario haya borrado su cuenta; se le requiere que establezca y mantenga un programa de privacidad comprensivo, diseñado para prevenir los riesgos a la privacidad asociados a cualquier desarrollo y manejo de nuevos, o de los ya existentes, programas y servicios, y que proteja la privacidad y confidencialidad de la información de los consumidores; y se le requiere que dentro de 180 días, y cada dos años luego de esa fecha y por los próximos 20 años, obtenga auditorías independientes de terceros que certifiquen que el programa de privacidad cumple con los requisitos que la FTC le ordena, y que asegure que la privacidad de la información de los consumidores está protegida.³⁰

Los aspectos que Facebook debía mejorar o cambiar, según EPIC, eran:

- Facebook incorpora, luego de esta controversia, una opción *opt-out* de las aplicaciones. Para EPIC esta opción nuclear debería ser una opción granular, de modo que las personas puedan optar por quedarse con algunas aplicaciones y no renunciar a todas.
- Personalización instantánea debería estar apagada en la configuración predeterminada y no ser una opción *opt-out* una vez que el usuario activa su cuenta.
- Los Social Plugins como *like* permiten que Facebook vea cómo los usuarios interactúan fuera de la red social en otros sitios de Internet, y aunque Facebook ha indicado que vuelve anónima esta información luego de 90 días, no debería retener ninguna información que identifique a los usuarios por ningún periodo de tiempo. Si su propósito es obtener información agregada, el anonimato no es una barrera para ello.
- Los usuarios deberían tener control total sobre su información, incluido su nombre, su correo electrónico, su fecha de nacimiento y su género.

³⁰ Comisión Federal de Comercio, “Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises”, 29 de noviembre de 2011, <http://ftc.gov/opa/2011/11/privacysettlement.shtm>

- Facebook tiene la opción de utilizar el protocolo de seguridad HTTPS para proteger la información que los usuarios suben a la plataforma. Actualmente esta información se sube sin encriptar, lo que pone en riesgo que otros intercepten los datos, por ende se solicita que Facebook implemente una opción para que los usuarios puedan utilizar HTTPS.
- Que Facebook permita la portabilidad de los datos generados por los usuarios dentro de la red social si en algún momento ellos quieren cambiarse de servicio de socialización en línea.³¹

Mientras tanto, en el campo legal la privacidad en Facebook se tradujo en la necesidad de mejorar el código, en transparentar las intenciones del uso de la información por parte de la compañía y en conseguir un consentimiento más informado por parte de los usuarios para que la red compartiera sus datos personales. La flexibilidad interpretativa de Facebook se mantuvo, aunque la privacidad asociada a la información fue el marco que se estabilizó en esta controversia (tabla 7).

En esta controversia es el valor del código lo que se estabiliza; así, desde que las bases de datos clausuraron la relación entre privacidad e información, en las redes sociales se dio el siguiente salto para moldear a los sujetos, no solo a partir de los datos que sobre ellos se sistematizan en las capas tecnológicas de las compañías y los gobiernos, sino a través de sus prácticas, sus acciones y los contenidos por ellos generados. En este contexto, la privacidad es una co-construcción entre el marco legal, la regulación del código y las normas sociales. El hallazgo de esta controversia es que la norma social puede ser moldeada por el código cuando se diseña de forma estratégica y consistente en los espacios virtuales.

Para Zuckerberg, el concepto de Social Graph ha sido fundamental para establecer las conexiones entre lo que la gente produce, pero la noción de flujo social es igual de importante para conseguir que compartan su información. Y no se equivocó el fundador de Facebook, cuando vaticinó “con el tiempo la privacidad será menos apreciada y se

³¹ Comisión Federal de Comercio, “Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises”, Anexo 7.

Tabla 7. Flexibilidad interpretativa en la controversia Everyone

Actores	Nociones de privacidad
Facebook	<p>Los usuarios tienen el control sobre su información y la red no entrega el acceso a esta si ellos no quieren.</p> <p>El perfil debe sentirse como el hogar, en el cual no debe pasar nada que el usuario no desee.</p>
Comisión Federal de Comercio	<p>Puesto que la demanda se centra en el cambio de la configuración de la privacidad en los perfiles de los usuarios, la privacidad está estrechamente vinculada a la información, al código y al cambio tecnológico.</p> <p>Las innovaciones de Facebook no se pueden realizar a expensas de la privacidad y los usuarios.</p>
EPIC y sus aliados	<p>La privacidad se centra en el control de la información y en el consentimiento informado de los usuarios.</p> <p>Los cambios realizados vuelven la información más pública y dejan de proteger aquello que antes se consideraba privado.</p> <p>Los usuarios asocian políticas de privacidad a protección de privacidad.</p> <p>Lo privado se relaciona con aquello que queda fuera del alcance de los demás; es una experiencia que la gente tiene (Solove, Rotenberg y Schwartz 2006).</p>
Senadores	<p>Entregar a los usuarios el control de cada pieza de información que producen y facilitarles herramientas más sencillas para que puedan ejercer su autodeterminación informacional.</p> <p>Privacidad es propiedad de la información, por ello proponen que Facebook entregue a los usuarios la posibilidad de emigrar a otras redes sociales todo aquello que han producido en la red.</p>
Usuarios	<p>La privacidad resulta de las prácticas con las cuales los usuarios se sienten cómodos, por eso reclaman que Facebook no los fuerce a revelar información incómoda. “Nuestra información es privada y queremos controlarla”. Facebook ha vulnerado la información de las personas y no se entiende cómo estos controles pueden hacerlos sentir más seguros; la red es el lugar para conectarse con la familia y los amigos, pero ahora parece un sitio donde la gente está en riesgo ante acosadores y ladrones de identidad.</p> <p>Facebook es un servicio gratuito que la gente “paga” al ver la publicidad y al convertir sus vidas en contenido que puede ser monetizado por Facebook. Mientras más intercambios de información los usuarios producen, más dinero gana la compañía. Los usuarios piden negociar un balance entre lo que no quieren volver público y los usos que la compañía hace de su información.</p>

Tabla 7. (Continuación)

Actores	Nociones de privacidad
Prensa y blogueros	La privacidad ha muerto y los medios de comunicación social son los responsables. Las personas publican más y con ello Facebook las guía a relajar sus controles de privacidad, los cuales son diseñados de forma confusa con el fin de desalentar a los usuarios de proteger su información.
	Facebook se ha convertido en el Gran Hermano y ha tenido éxito en ofrecer la ilusión de privacidad en un lugar público a los usuarios, quienes deberían comprender que “público” no es público en Facebook, sino en el ecosistema de la red; se debería educar a los usuarios sobre el significado de lo público.
	No se puede hablar de privacidad en el proyecto Facebook, que es convertir a la red social en el mayor repositorio en tiempo real y con información creada por las propias personas.

la sacrificará con tal de lograr tener información adicional. Facebook se ha convertido en el experimento más grande de exhibición personal” (Kirkpatrick 2010, 314).

Ensamblajes sociotécnicos

Como hemos visto hasta ahora, la SCOT no reconoce la separación entre lo social y lo tecnológico (Bijker 1995), más bien se centra en explicar las configuraciones sociotécnicas. Dichas configuraciones son aclaradas por los ensamblajes sociotécnicos, a través del análisis de las relaciones de poder que se producen a una escala más larga entre los actores sociales y tecnológicos vinculados tanto al artefacto como a los grupos sociales relevantes.

Así, Bijker reconoce tres posibles configuraciones. En la primera no existen grupos sociales dominantes y, por tanto, no se presenta un marco tecnológico dominante, la flexibilidad interpretativa es muy alta y las innovaciones pueden ser radicales. En la segunda, un grupo social es dominante e impone un marco tecnológico, con lo que logra dominar tanto la definición del problema como la solución de la que es parte el

artefacto; en este caso las innovaciones tienden a ser convencionales y los cambios mayores vienen de la mano de actores con baja inclusión en el marco tecnológico. Finalmente, en la tercera configuración, dos o más grupos sociales dominantes cruzan sus marcos tecnológicos y solo un criterio externo puede resolver el problema.

Tanto los marcos tecnológicos como los ensamblajes sociotécnicos revelan la forma en que el poder se ejerce y se distribuye para modificar el estado de cosas dentro de las relaciones. He analizado cómo los marcos tecnológicos de la privacidad en los inicios de Facebook ayudan a comprender las relaciones entre los grupos sociales relevantes y los artefactos, en los procesos de desestabilización y clausura (los artefactos mientras se constituyen). Revelan, igualmente, los paradigmas desde los cuales los actores configuran el artefacto. Así los marcos tecnológicos actúan influenciando el desarrollo tecnológico y mostrando los procesos opacos de disputa y de estabilización de la tecnología.

Los ensamblajes sociotécnicos en cambio nos son útiles para explicar la agencia de los actores humanos y no humanos y cómo los primeros son capaces de ejercer el poder al alinear las agencias de los otros (Bijker 1995; Thomas 2008). Este ejercicio, según Bijker (1995), puede darse de dos modos: por medio de un poder semiótico, cuando se logra disminuir la flexibilidad interpretativa a través de la estabilización y la clausura, con lo cual la capacidad de significar un artefacto representa poder; y a través del poder micropolítico ejercido en las prácticas que transforman y moldean la acción de los grupos sociales relevantes, tiene que ver con el modo en que los marcos tecnológicos restringen o impulsan el cambio. Abordar el poder como una capacidad habilita el estudio de las interacciones más allá del diseño de estrategias conscientes. “Poder semiótico y micropolítica del poder están inextricablemente vinculados: las micropolíticas dan como resultado específicas estructuras semióticas, en tanto que el poder semiótico influencia las estructuras micropolíticas” (Thomas 2008, 237).

Conclusiones

Mi propósito con esta obra ha sido rastrear cómo se han construido las nociones de privacidad desde que se desarrollaron en Occidente para comprender las versiones de la privacidad que se producen como consecuencia de habitar las redes. La privacidad es entonces un concepto controversial y en constante evolución, y es también una práctica que se co-construye entre las capas sociales y tecnológicas de Facebook.

Desde un enfoque sociotécnico, se han utilizado las controversias de la privacidad para abrir su caja negra, así se han rastreado códigos, normas legales, usuarios, empresas, políticos, compañías, activistas y gobiernos. El trabajo ha sido organizado en cuatro niveles para explicar: (i) la relación de la privacidad con el cambio tecnológico; (ii) la clausura del concepto de privacidad dentro del derecho como noción relacionada con la información y con el control de los datos personales; (iii) la agencia del código para diseñar espacios virtuales estandarizados,¹ transformar los comportamientos y condicionar normas sociales; y (iv) el valor del artefacto sociotécnico, parte sociedad, parte tecnología, para naturalizar la exhibición del sujeto y promover la renuncia a su sentido de privacidad.

¹ Estandarizados en cuanto a la arquitectura del sitio y como dispositivos condicionantes de la transformación del sentido de privacidad, de trance, o de disolución del límite entre lo público y lo privado en el momento de participar. Estos espacios públicos no estandarizan los valores, las ideas o las creencias de los usuarios; muchos de ellos se han organizado para reclamar de Facebook aquello que no consideraban justo y transparente.

¿Cómo se han construido las diferentes nociones de privacidad en Occidente y cuál es su relación con el cambio tecnológico?

En el siglo XIX, el concepto de privacidad en Occidente es un producto de la modernidad y del surgimiento del sujeto individual relacionado con la crisis de la vida pública y la secularización de la sociedad. La personalidad se convierte en una categoría social en la que el individuo se transforma en una idea que funciona para proteger el nascente individualismo (Sennett 1977). La intimidad y la personalidad se vinculan permanentemente dentro de esta nueva concepción del sujeto que tiene como contexto la privatización del espacio y de la vida pública. Se crea así una división entre el ámbito público y la esfera íntima de las personas, con lo cual se asienta una noción individualista del sujeto, quien reclama el derecho a no participar en la vida colectiva y a cerrar la puerta de lo social (Emerson 1970), al igual que a distinguir lo individual de lo colectivo (Hixson 1987). En este contexto surgen dos tradiciones sobre la concepción de privacidad que se derivan de sistemas culturales específicos: el europeo y el norteamericano.

Como se analiza en la primera sección, las trayectorias de la privacidad han evolucionado a través de las relaciones entre los sujetos, sus instituciones y sus estructuras tecnológicas, produciendo equivalencias de valores que sustentan las doctrinas sobre la privacidad en el tiempo. Con el pensamiento liberal se creó una versión de la privacidad fundamentada en el estereotipo del propietario, y en la libertad, mientras que la vertiente europea protegió el honor, la dignidad, la imagen y la personalidad.

La privacidad se concibió entonces como un valor que logra estabilizarse hasta que surgió un cambio del paradigma tecnológico. Así, el derecho a ser dejado en paz apareció con la creación de una tecnología que le permitió a la prensa amarillista utilizar las fotos que se tomaban desde la invención de la cámara portátil de Kodak. En este contexto, la autonomía en la toma de decisiones es la doctrina que se vincula al deseo de las personas de mantener sus asuntos fuera del alcance de los demás y presenta dos controversias importantes: la masificación del teléfono y de los métodos anticonceptivos. La autodeterminación va de la mano de la construcción autónoma de la personalidad y del uso de la información

de los sujetos, en particular, cuando las bases de datos empiezan a registrar información sensible y ello afecta su sentido de lo privado y de su reputación. Esta versión de la privacidad es el antecedente de una forma de concebir lo privado que se mantiene de forma muy potente en la actualidad: la privacidad como control de la información. Finalmente, los sistemas de monitoreo y autenticación refuerzan la doctrina americana de razonables expectativas de privacidad y con ello se relaciona el cambio tecnológico con la privacidad de forma cada vez más irreversible.

La agencia del artefacto Facebook en la construcción de un espacio público estandarizado a partir de la influencia de las capas informáticas sobre las capas sociales

Puesto que la sociedad está tecnológicamente estructurada y la tecnología es socialmente construida (Thomas 2008), el estudio de Facebook no distingue *a priori* qué es social ni qué es tecnológico (Bijker 1995). En la sección 2 se examinan las trayectorias de la privacidad dentro de varios contextos: las dinámicas de co-construcción de lo privado entre el código y la norma social dentro de Facebook; la política del artefacto desde el desarrollo del modelo de monetización de la producción cultural del usuario y el principio de transparencia radical; al igual que las capacidades del código para naturalizar la exhibición de los sujetos a través de metáforas como el perfil, la biografía y el intercambio con los *amigos*, la co-construcción de la norma social entre las acciones de los usuarios y la función de la arquitectura de la red social.

Asimismo, se estudia la capacidad de tecnologizar la sociabilidad en línea que tiene el artefacto y los efectos de instalar un régimen de propiedad dentro de prácticas sociales de los miembros de la red, en relación con sus nociones de privacidad. Las dinámicas de co-construcción que se estudian abrieron la caja negra de Facebook y mostraron los intereses que vehiculizan los grupos sociales relevantes, a través de las negociaciones en las que intervienen para rediseñar la privacidad en Facebook. Las versiones del aparato que surgen del análisis permiten identificar los procesos de problema/solución que acontecieron en los ocho años de funcionamiento del artefacto sociotécnico. Entre los más importantes, el control de las conductas que ejerce Facebook para conducir las formas

de socialización dentro de las que se aplana el contexto social, impidiendo que los sujetos sean capaces de desarrollar personalidades situadas. Con ello, la intención de promover la identidad única formatea un tipo de identidad que lo comparte todo con todos, incapaz de establecer un sentido de intimidad en línea.

Este tipo de socialización sirve a un modelo económico del artefacto, el *Free Labor*. Este apoya una producción cada vez mayor de formas de representación del ser en línea, donde se vuelve más atractivo expresar los sentimientos, narrar el minuto a minuto, tener grandes listas de amigos, colgar imágenes, entregarse a los sistemas de monitoreo –incluso fuera de la *web*– para registrar qué partes del mundo se habitan, o exhibir la lista de libros y de películas preferidos. A través del código, la norma social y la regulación, Facebook logra imponer su régimen de propiedad dentro de la red social.

Las controversias que los actores han desarrollado en el proceso de co-construcción de la privacidad en la red social y el cambio de la norma social en la interacción entre la capa tecnológica y la capa social de Facebook para redefinir lo privado.

Las controversias generadas sobre la privacidad en Facebook han permitido entender cómo este concepto va transformándose en el ciberespacio en función de las prácticas de los usuarios y de la fuerza social de la norma. Mientras tanto, Mark Zuckerberg empuja al límite el sentido de protección de los usuarios y apela tanto al control de su propia información como al sistema de confianza que se establece con el entorno. Utiliza la arquitectura de Facebook para modelar la conducta de los miembros de la red usando más código y más regulación.

En la sección 3 se muestran los procesos sociotécnicos de co-construcción de la privacidad en Facebook a raíz de los momentos de negociación que se producen frente al cambio tecnológico del artefacto. Esta arqueología de las redes sociales a través de la trayectoria de Facebook permite entender cómo se estructura el marco tecnológico de la privacidad. Es aquí donde los grupos sociales relevantes se amplían y entra en acción la fuerza de la regulación y de los gobiernos. También he explicado cómo la privacidad va mucho más allá de los datos, pues en

un ejercicio de co-construcción, las normas sociales y las capas tecnológicas del artefacto llegan a estandarizar formas de representación y de comportamiento.

La sección 4 está dedicada a exponer las cinco controversias de la privacidad que revelan la alta flexibilidad interpretativa que mantienen los actores frente al artefacto y las formas de privacidad que han terminado estabilizándose. Es aquí donde se evidencia la constante interacción entre código y regulación para moldear la privacidad de dos maneras: privacidad-información y privacidad-control. Recordemos, por ejemplo, que mientras *News Feed* es percibido por los usuarios como una violación de sus expectativas de privacidad o como un instrumento de acoso, Facebook lo difunde como un mecanismo para mantenerse en contacto entre amigos. Cuando surge *Beacon*, los miembros reclaman su capacidad invasiva y poder para convertir el espacio de la red en un Gran Hermano, donde se vuelve público todo aquello que pasa en internet fuera de Facebook. Si bien la empresa reconoce el desequilibrio de la nueva característica y la elimina, también crea una nueva arquitectura que hace lo mismo que *Beacon* de una forma más sutil: *Facebook Connect* y *Open Graph*.

El año 2009 se cambian los términos del servicio y se vuelve público el tratamiento que Facebook da a los datos de los usuarios, en particular la licencia PI, a través de la cual los miembros cedían los derechos de propiedad intelectual sobre los contenidos generados por ellos y que no estaban protegidos con controles de privacidad. Además se vuelven visibles los eufemismos de la terminología legal que confundían a los usuarios, por ejemplo, *compartir con terceros* realmente quiere decir vender a terceros los contenidos y ganar ingresos con la información producida por los usuarios. Cuando los usuarios pensaron que controlaban su información, Facebook les dijo que habían perdido los derechos sobre la información que producían sin protecciones de privacidad.

En este sentido, la demanda del gobierno de Canadá contra Facebook puso a nuevos actores en juego dentro del proceso sociotécnico de co-construcción. Dentro de esta controversia las organizaciones protectoras de la privacidad adquirieron una agencia muy importante, una vez que tuvieron el respaldo gubernamental. De igual modo, Facebook establece relaciones con entidades gubernamentales, fiscales generales,

centros de investigación y se adhiere a convenios de privacidad con organismos como la Comisión Europea.

Finalmente, la controversia sobre el cambio de la configuración predeterminada de *amigos a pública* generó una de las protestas más importantes en la red social; se elevaron reclamos que delinearon la privacidad más allá de su noción de información. Se definió la privacidad como aquello que queda fuera del alcance de los demás, como una experiencia personal de los sujetos respecto de las prácticas con las que los usuarios se sienten cómodos. Facebook planteó la privacidad desde el punto de vista de habitar lugares seguros: “El perfil de los usuarios debe sentirse como el hogar, en él no debe pasar nada que el usuario no desee” (Cox 2001). Sin embargo, al mismo tiempo se clausuró la versión de la privacidad en directa relación con la información y el control: “Nuestra información es privada y queremos controlarla”.²

Los hallazgos

Al iniciar la investigación en la que se basa este libro, partí de la premisa de que la tecnología es determinante en la configuración de la privacidad en el ciberespacio. Lo que no supuse es que, desde las primeras controversias sobre privacidad en el siglo XIX, la tecnología fuera igualmente un elemento fundamental dentro del debate sobre la intimidad que iba a mantenerse durante todo el siglo XX. La agencia histórica de la tecnología en la configuración de la privacidad a lo largo de la historia moderna es uno de los primeros y más importantes hallazgos. Ello vuelve todavía más adecuado el análisis sociotécnico escogido para este estudio.

El segundo hallazgo que identifiqué es la agencia reguladora de la arquitectura dentro de la red. Me arriesgué a afirmar que el diseño tecnológico negocia unas prácticas de naturalización de la exhibición del sujeto y de un renunciamiento de la privacidad como norma social, y lo que descubrí fue no solo su capacidad modeladora de comportamientos, sino sus procesos de co-construcción con la normativa legal. En cuatro de las cinco controversias sobre la privacidad en Facebook, la negociación terminó produciendo “más código”: News Feed provocó un

² «Facebook! Arregla la configuración de privacidad». En <https://bit.ly/3m2OLpE>

nuevo set de controles y el surgimiento del concepto del Social Graph. Beacon produjo la creación de Facebook Connect y del Open Graph. El cambio de los Términos de privacidad del año 2009 se tradujo en nuevos controles en dicho ámbito y en una herramienta tecnológica nueva: (i) el sitio *web* de gobernanza de Facebook y nuevo texto legal: la Declaración de derechos y responsabilidades. El cambio de la configuración predeterminada a *Everyone* produjo nuevos sets de controles y el cambio en la arquitectura de privacidad a través de un doble modelo: granular para cada uno de los contenidos y nuclear para los tipos de configuración de privacidad que ofrecía Privacy Wizard.

Al concebirse Facebook como un negocio innovador y de alcance global basado en la socialización de las personas, no era posible imaginar la capacidad de la propia empresa de conceptualizar el producto que estaba diseñando, en una clara dinámica de co-construcción entre las características sociales de la red, su innovación tecnológica, el modelo de negocios y sus pretensiones globalizadoras. Zuckerberg y sus escritores de código diseñaron una red social cerrada, que partía de un sistema de confianza consolidado a través de un principio clave: la privacidad. Facebook es una de las primeras redes sociales que pidió a los usuarios utilizar sus identidades reales y comprobó sus identidades a través de un sistema de circularidad de la privacidad. De esta estructura inicial se pasó a *teorizar* sobre las capacidades de relación que se producen entre los miembros a través de sus prácticas de intercambios y así apareció el *Social Graph* y los límites de la red dentro de internet.

El próximo salto fue pasar de un sistema de red a uno de plataforma y, con ello, generar capacidades para seguir las huellas de los usuarios dentro de todo el ciberespacio; en este marco el *Open Graph* fue concebido y con ello se reforzó la capacidad de aplicar el principio de transparencia radical que Zuckerberg venía madurando desde que la red se volvió un fenómeno mundial. Las mismas prácticas de intercambio fueron pensadas como una *economía del don*, solo que, dentro de la versión del creador de Facebook, el usuario no recibe una recompensa monetaria al trabajo que desarrolla gratuitamente para la compañía, como tampoco conserva la propiedad intelectual de los productos culturales que genera dentro del artefacto. Partiendo de una ética hacker, promotora de valores democráticos, de horizontalidad, de libertad y de

producción de conocimiento sin fines de lucro, Zuckerberg transforma su red social en una empresa jerárquica en la que toma decisiones unilaterales y cambia las reglas del juego de forma vertical, así se instaura un régimen de propiedad en un entorno de socialización que se convirtió en el más grande repositorio de *dossiers* digitales y de estilos de vida en el mundo actual. En este nuevo Facebook, la privacidad es una norma social que se mantiene como un camino de paso a la transparencia total del sujeto.

Otro de los hallazgos que deseo enfatizar es el modelo de negocios de Facebook y sus intenciones de estandarizar globalmente un régimen de propiedad sobre la producción de bienes culturales generados por los usuarios, utilizándolos como mano de obra gratuita. Es revelador el uso del Free Labor como mecanismo de consolidación de la empresa, no solo porque explica qué significa el usuario para la Facebook, sino también porque muestra qué es lo que está detrás del proyecto de conectividad que impulsa esta empresa. En cuanto a la intimidad, este modelo ha logrado transformar una noción de privacidad, inicialmente considerada un elemento fundamental en la construcción de la red, en una noción de transparencia radical donde la privacidad ya no tiene cabida, todo ello en función de las ganancias que la red obtiene al apoyar este cambio.

El andamiaje conceptual

La metáfora de “tejido sin costuras” de Bijker (1995) ha sido el punto de partida para el diseño conceptual de la investigación que respalda esta obra. He tomado prestado algunos de los conceptos sustantivos de la construcción social de la tecnología, con los cuales estructuré el andamiaje que ha permitido confrontar la privacidad en Facebook. Es así como he logrado explicar la evolución de la privacidad en relación con el cambio tecnológico, y con ello, adentrarnos en la aventura de descubrir los procesos de co-construcción entre sujetos y artefactos. He utilizado las teorías tanto en niveles descriptivos como explicativos. En términos descriptivos, los conceptos de grupos sociales relevantes, flexibilidad interpretativa y artefacto funcionaron para mostrar las versiones de la privacidad que se construían en los intersticios entre los códigos y las

normas. En términos explicativos, fueron las nociones de análisis socio-técnico, marco tecnológico, función, controversia, clausura y ensambles sociotécnicos los que iluminaron el camino para estudiar las trayectorias de la privacidad antes de llegar a Facebook y dentro de la red social.

Cada grupo social mostró sus formas de interpretar el mundo y los intereses que les llevaban a negociar un sentido de la privacidad en el ciberespacio. Esta posibilidad de analizar, a partir de los actores, la propia construcción del artefacto sociotécnico y sus capacidades de imponer modelos de comportamiento, me posibilitó mapear resoluciones de problemas diferenciados y seguir los sentidos que el artefacto fue adquiriendo al ser interpretado por ellos. Así, Facebook se convirtió en tantos artefactos como visiones de él se presentaron (Thomas 2008), gracias a la flexibilidad interpretativa de los grupos sociales relevantes. La noción de marco tecnológico me adentró en los paradigmas que funcionan dentro de cada grupo. Con ello, pude analizar las teorías, las estrategias, las doctrinas, los intereses, las prácticas y el conocimiento tácito que forman parte del artefacto (Bijker 1995; Pinch y Bijker 2008; Thomas 2008).

El análisis sociotécnico ofreció un doble nivel explicativo y pude mostrar el momento en que los artefactos tecnológicos se volvieron parte constitutiva de las relaciones políticas, sociales, culturales y económicas, además del instante en que estas se materializaron en artefactos tecnológicos. Al tomar como concepto central la controversia, organicé la investigación en momentos de análisis que fueron desvelando los marcos tecnológicos de los grupos sociales relevantes y, con ello, entendiendo los recorridos de estabilización y clausura de la privacidad dentro de Facebook. Finalmente, los ensambles sociotécnicos me permitieron estudiar las relaciones de poder que se han ejercido para transformar las normas de privacidad dentro de Facebook y la capacidad de los grupos dominantes de lograr sus objetivos, clausurando el sentido del artefacto.

Sin embargo, también experimenté algunos límites del abordaje constructivista (Thomas 2008, 241). El primero fue la dificultad de registrar los cambios que operan en la significación de los artefactos por parte de los grupos sociales relevantes. Hemos visto, por ejemplo, que Facebook en un inicio operó con la premisa del valor de la privacidad para construir un sistema de confianza en la red social; pero, cuando este sistema estuvo lo suficientemente regulado por el código y por la

transformación de la norma social, se aplicó la noción de transparencia radical, un nuevo sentido del artefacto que negó la primera significación. Con esto, los procesos de clausura y estabilización se representan como procesos monolíticos, cuando en realidad es muy difícil registrar y explicar los cambios de la función del artefacto que se dan en el transcurso del tiempo. Por esta razón, la teoría resulta limitada para estudiar el cambio tecnológico de forma diacrónica.

A pesar de su intención dinámica, el abordaje constructivista resulta estático: representa un momento estable de un sistema de interacciones. La temporalidad histórica de los marcos tecnológicos y los ensamblajes sociotécnicos solo es representable mediante una sucesión de modelizaciones, tantas como estabilizaciones son detectadas. Pero a diferencia de otros abordajes, sí permite identificar y analizar momentos de desestabilización y cambio en la orientación general de las interacciones, y de alteración en las dinámicas de cambio tecnológico (Thomas 2008, 242).

Justamente, estas modelizaciones son las que he realizado, al identificar los momentos de cambio a través de las controversias sobre la privacidad. Con ellas he representado también las transformaciones de los paradigmas de los grupos sociales relevantes, los marcos tecnológicos y los ensamblajes sociotécnicos que han entrado en acción.

Sin los aportes de la sociología jurídica no hubiese podido explicar la trayectoria sinuosa de la privacidad dentro del mundo del derecho. Han resultado básicas para mi propósito las doctrinas sobre el valor de la norma dentro de los estudios de presentación del ser y de las normas de civilidad (Post 1995), las razonables expectativas de privacidad (Solove 2002, 2004; Schwartz 2000; Pouillet y Rouvroy 2009), la autodeterminación informacional (Westin 1984; Acquisti y Gross 2006; Barnes 2006; Dwyer, Hiltz y Passerini 2007). Al entender estas doctrinas he logrado explicar los paradigmas de los grupos sociales relevantes y los intereses que los llevan a negociar una noción de privacidad en particular.

De igual manera, los estudios sobre redes sociales (boyd 2004, 2006; Haythornthwaite 2005) se han alimentado de los conceptos sobre simulación y conservación de la ilusión (Turkle 2009; Giffin 1984), fundamentales para explicar los modos en que los sujetos han habitado

Facebook en sus procesos de co-construcción de la privacidad. Sin los aportes de Lawrence Lessig, hubiese sido muy difícil explicar la capacidad de dominación y control de la tecnología dentro de la red social y las negociaciones entre código y norma social. Finalmente, la economía digital ingresó en mi investigación a través del concepto de Free Labor que ofrece Terranova (2000) y, con esto, entregó un camino para argumentar la economía política de Facebook y su modelo de negocios en relación con la privacidad.

Para seguir investigando

Originalmente la investigación en la cual se basa este libro estuvo orientada a un estudio más centrado en los usos de Facebook y en la construcción de la privacidad desde las prácticas de los usuarios. Había diseñado otros énfasis que luego dejé atrás una vez que tomé el camino del análisis sociotécnico. Entre los intereses originales estaba investigar las relaciones entre el sujeto y la pantalla, desde los estudios sobre virtualidad y cibercultura; el análisis semiológico de la arquitectura de la red social; el goce dentro de los mundos virtuales y la negociación de la privacidad frente a la posibilidad de gratificación inmediata; y, finalmente, el valor del rito como mecanismo de construcción de privacidad.

En los últimos cinco años, habitar las redes implica también hacer frente a otros problemas individuales y colectivos. Ya no solo la privacidad está en juego en Facebook, los algoritmos se utilizan para analizar datos de los usuarios para predecir sus intenciones de consumo y sus preferencias políticas. La filtración de un documento confidencial de Facebook en 2018³ mostró la importancia de las predicciones realizadas por esta red sobre el comportamiento de sus miembros. Este documento cita la experticia sin parangón que ha desarrollado la empresa para predecir los futuros comportamientos de sus usuarios utilizando machine learning con sus datos privados. Estas predicciones se utilizan para intervenir y modificar los gustos de sus miembros, por ejemplo, un servicio denominado Loyalty Prediction es reconocido por su habilidad

³ “Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document” (2018. Biddel, Sam. Intercept, April 13 <https://bit.ly/35kclCT>).

para analizar qué usuarios podrían realizar cambios en sus consumos, con lo que se alerta a las marcas que pagan el servicio para que intervengan enseguida con anuncios y mensajes más agresivos para estabilizar la lealtad del usuario a la marca y garantizar el comportamiento futuro de sus clientes.⁴ En esta misma línea los algoritmos basados en psicometría utilizados por Cambridge Analytica y Facebook probaron que era posible influenciar campañas electorales a través del uso de código.

Quedan abiertas entonces muchas opciones para estudiar la privacidad desde las ciencias sociales y su relación con el cambio tecnológico, en una era marcada por el vértigo de la velocidad y por las posibilidades de representación y de conexión de los sujetos.

⁴ La plataforma de inteligencia artificial llamada FB Learner Flow analiza millones de datos todos los días, entrena a sus modelos algorítmicos y genera predicciones en tiempo real para ser vendida a las empresas (“Introducing FB Flow: Facebook’s AI Backbone” Jeffrey Dum, Facebook Code, May 9, 2016 <https://bit.ly/3bDVXE1>).

Referencias

- Acquisti, Alessandro, y Ralph Gross. 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook". En *Privacy Enhancing Technologies: 8th International Symposium PET 2006*, editado por George Danezis y Philippe Golle, vol. 4258, 36-58. Heidelberg: Springer.
- Acquisti, Alessandro y Jens Grossklags. 2007. "What can behavioral economics teach us about privacy?" En *Digital Privacy: Theory, Technologies, and Practices*, editado por Alessandro Acquisti, et al., 363-77. Abington: Auerbach Publications.
- Akrich, Madeleine. 1992. "The De-scription of Technical Objects". En *Shaping Technology/Building Society: Studies in Sociotechnical Change*, editado por Wiebe E. Bijker y John Law, 205-24. Cambridge: MIT Press.
- Alpert, Julia. 2006. "A call from the panopticon to the judicial chamber 'Expect Privacy'". *Journal of International Commercial Law and Technology* 1 (2): 62-71.
- Arendt, Hannah. (1958) 2005. *La condición humana*. Barcelona: Paidós.
- Argersinger, Peter H., y Jo Ann E. Argersinger. 1984. "The machine breakers: Farmworkers and social change in the rural Midwest of the 1870s". *Agricultural History* 58 (3): 393-410.
- Ashton, Kevin. 2009. "That 'Internet of Things' Thing. In the real world, things matter more than ideas". *RFID Journal*, 22 de junio. <http://www.rfidjournal.com/article/view/4986>
- Ballester, María. 1998. *La intimidación como fundamento de la inviolabilidad de domicilio*. Palma: Universitat de les Illes Balears.

- Barante, Amable-Guillaume-Prosper Brugière, baron de. 1863. *La vie politique de M. Royer-Collard, ses discours et ses écrits*. París: Didier.
- Barbrook, Richard. (1999) 2005. "The High- Tech Gift Economy". *First Monday* 3 (12). <https://doi.org/10.5210/fm.v3i12.631>
- Barnes, Susan B. 2006. "A privacy paradox: Social networking in the United States". *First Monday* 11 (9): 1-11. doi:10.5210/fm.v11i9.1394.
- Bauer, Martin W. 1995. *Resistance to New Technologies: Nuclear Power, Information Technology, and Biotechnology*. Nueva York: Cambridge University Press.
- Beaussire, Émile Jacques Armand. 1888. *Les principes du droit*. París: F. Alcan.
- Bijker, Wiebe E. 1993. "Do not Despair: There is Life after Constructivism". *Science, Technology and Human Values* 18: 113-38.
- 1995. *Of bicycles, bakelites, and bulbs: toward a theory of sociotechnical change*. Cambridge: MIT Press.
- Bijker, Wiebe, Thomas Hughes y Trevor Pinch. 1987. *The social construction of technological systems: new directions in the sociology and history of technology*. Cambridge: MIT Press.
- Bloustein, Edward J. 1964. "Privacy as an aspect of human dignity: An answer to Dean Prosser". *New York University Law Review* 39: 962-1007.
- Bogost, Ian. 2010. *The expressive power of videogames*. Cambridge: MIT Press.
- boyd, dahah. 2004. "Friendster and publicly articulated social networks". En *Proceedings of ACM Conference on Human Factors in Computing Systems*, editado por ACM's Special Interest Group on Computer-Human Interaction, 1279-82. Nueva York: ACM Press.
- 2006. "Friends, Friendsters, and MySpace Top 8: Writing community into being on social networks sites". *First Monday* 11 (12). <http://firstmonday.org/article/view/1418/1336>
- 2007. "Socializing digitally". *Vodafone Receiver Magazine* 18, junio. <http://www.danah.org/papers/VodafoneReceiver.pdf>
- 2008a. "Facebook's privacy trainwreck. Exposure, invasion and social convergence". *Convergence: The International Journal of Research into New Media Technologies* 14 (1): 13-20. <http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf>

- boyd, dahah. 2008b. "Non of This is Real. Identity and Participation in Friendster". En *Structures of Participation in Digital Culture*, editado por Joe Karaganis, 132-157. Nueva York: Social Science Research Council.
- boyd, dana, y Nicolle Ellison. 2007. "Social Network Sites: Definition, History, and Scholarship". *Journal of Computer-Mediated Communication* 13 (1): 210-230.
- Bruun, Henrik, y Janne Hukkinen. 2008. "Cruzando fronteras: un diálogo en tres formas de comprender el cambio tecnológico". En *Actos, actores y artefactos. Sociología de la tecnología*, coordinado por Hernán Thomas y Alfonso Buch, 185-216. Bernal: Universidad Nacional de Quilmes.
- Callon, Michel, y Vololona Rabearisoa. 1999. "La Leçon d' Humanité de Gino". *Réseaux* 17 (95): 197-233.
- Cassidy, John. 2006. "Me Media. How hanging out on the Internet became big business". *The New Yorker*, 15 de mayo. <http://www.newyorker.com/magazine/2006/05/15/me-media>
- Clarke, Roger. 1988. "Information Technology and Dataveillance". *Communications of the ACM* 31 (5): 498-512. <http://www.rogerclarke.com/DV/CACM88.html>
- Cohen, Julie E. 2000. "Examined Lives: Informational Privacy and the Subject as Object". *Stanford Law Review*, 52: 1373-438.
- Collins, Harry M. 1981. "The place of the core-set in modern science: social contingency with methodological propriety in science". *History of Science* 19 (43): 6-19.
- Contamine-Raynaud, Monique. 1978. "Le secret de la vie privée". En *L'information en droit privé. Travaux de la conférence d'agrégation*, editado por Ivon Loussouarn y Paul Lagarde, 401-451. París: LGDJ.
- Cooley, Thomas M. 1895. *The Elements of Torts*. Chicago: Callaghan and Co.
- Cordova, Cristina. 2010. *The end of privacy as we know it?: The ethics of privacy on online social networks*. Stanford: Program in Ethics in Society, Stanford University. <http://es.scribd.com/doc/31183528>
- De Schutter, Oliver. 1999. "La vie privée entre droit de la personnalité et liberté". *Revue Trimestrielle des Droits de l'Homme*, 40: 827-63. <http://www.jurisquare.be/nl/journal/revtrimdrh/index.html>

- Denning, Brannon P. 2010. "Book Review: *Judgment Calls: Principle And Politics In Constitutional Law*. By Daniel A. Farber y Suzanna Sherry. Oxford, United Kingdom: Oxford University Press, 2009". *Texas Law Review* 89 (1). <https://ssrn.com/abstract=1288146>
- Dew, Charles B. 1994. *Bond of Iron: Master and Slave at Buffalo Forge*. Nueva York: W. W. Norton.
- Dewey, John. 1936. "Liberalism and Civil Liberties". *Social Frontier* II (febrero): 137-38.
- Donath, J., y dahah boyd. 2004. "Public displays of connection". *BT Technology Journal* 22 (4): 71-82.
- Dwyer, Catherine. 2011. "Privacy in the age of Google and Facebook". *IEEE Technology and Society Magazine* 30 (3): 58-63. doi:10.1109/MTS.2011.942309
- Dwyer, Catherine, Starr Roxanne Hiltz y Katia Passerini. 2007. "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace". *Proceedings of the Thirteenth Americas Conference on Information Systems*. Keystone, CO: AMCIS. <http://aisel.aisnet.org/amcis2007/339>.
- Emerson, Thomas I. 1970. *The System of Freedom of Expression*. Nueva York: Vintage Books.
- Festa, Paul. 2003. "Investors snub Friendster in patent crab". *CNet News*. 11 de noviembre. http://news.cnet.com/2100-1032_3-5106136.html
- Follari, Roberto. 2005. "Modificaciones epistemológicas actuales, oferta educativa y organización curricular". *Educação* 28 (2): 171-83.
- Fono, David, y Kate Raynes-Goldie. 2005. "Hyperfriendship and beyond: Friends and social norms on LiveJournal". En *Internet Research Annual Volume 4: Selected Papers from AoIR Conference*, editado por Mia Consalvo y Caroline Haythornthwaite, 91-103. Nueva York: Peter Lang.
- Fried, Charles. 1970. *An Anatomy of Values: Problems of Personal and Social Choice*. Cambridge: Harvard University Press.
- Fry, Benjamin Jotham. 2000. "Organic Information Design". Tesis doctoral, Massachusetts Institute of Technology, School of Architecture and Planning, Program in Media Arts and Sciences.

- Fuchs, Christian. 2011. "An Alternative View of Privacy on Facebook". *Open Access Information* 2 (1): 140-65.
- Gavison, Ruth. 1984. "Privacy and the Limits of Law". En *Philosophical Dimensions of Privacy. An Anthology*, editado por Ferdinand D. Schoeman, 346-402. Nueva York: Cambridge University Press.
- Geertz, Clifford. 1976. *The Religion of Java*. Chicago: Chicago University Press.
- Giffin, Holly. 1984. "The coordination of meaning in the creation of a shared make-believe reality". En *Symbolic play: The development of social understanding*, editado por Inge Bretherton, 73-100. Nueva York: Academic Press.
- Godkin, Edward Lawrence. 1890. "The Rights of the Citizens: IV. To His Own Reputation". *Scribner Magazine* 58 (julio): 67-82.
- Goffman, Erving. 1981. *La presentación de la persona en la vida cotidiana*. Buenos Aires: Editorial Amorrortu.
- Granovetter, Mark. 1983. *The Strength of Weak Ties: a Network Theory Revisited*. Nueva York: State University of New York.
- Grimmelmann, James. 2009. "Saving Facebook". *Iowa Law Review* 34: 1137-1206.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262822
- Haythornthwaite, Caroline. 2005. "Social networks and Internet connectivity effects". *Information, Communication y Society* 8 (2): 125-47.
- Hixson, Richard F. 1987. *Privacy in a Public Society: Human Rights in Conflict*. Nueva York: Oxford University Press.
- Hongladarom, Soraj. 2011. "Personal Identity and the self in the online and offline World". *Minds and Machines* 21 (4): 533-548.
<http://philpapers.org/rec/HONPIA-2>
- Jolicoeur, Pénélope. 2005. "Conséquences d'une redéfinition du concept de vie privée sur l'environnement informationnel propre aux étudiants fréquentant une institution d'enseignement supérieur". Tesis de maestría, Université de Montreal, Faculté de Droit.
<https://papyrus.bib.umontreal.ca/xmlui/handle/1866/2408>
- Kirkpatrick, David. 2010. *The Facebook Effect: the inside story of the company that is connecting the world*. s. l.: Virgin Books.

- Kline, Ronald. 2005. "Resisting Consumer Technology in Rural America: The Telephone and Electrification". En *How Users Matter. The Co-construction of Users and Technology*, editado por Nelly Oudshoorn y Trevor J. Pinch, 51-66. Cambridge: MIT Press.
- Konvitz, Milton R. 1966. "Privacy and the Law: A Philosophical Prelude". *Law and Contemporary Problems* 31: 272-80.
- Kraybill, Donald B. 1989. *The Riddle of Amish Culture*. Baltimore: Johns Hopkins University Press.
- Kreimer, Pablo. 1999. *De probetas, computadoras y ratones. La construcción de una mirada sociológica sobre la ciencia*. Buenos Aires: Universidad de Quilmes.
- Krieger, Leonard. 1957. *The German Idea of Freedom. History of a Political Tradition*. Boston: Beacon Press.
- Lampe, Cliff, Nicolle Ellison y Charles Steinfield. 2006. "A Face(book) in the crowd: Social searching vs. social browsing". En *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, editado por Pamela Hinds et al., 167-70. Nueva York: ACM.
- Lane, Frederick S. 2009. *American Privacy: The 400-Year History of our most contested right*. Boston: Beacon Press.
- Latour, Bruno. 2002. "What is Iconoclasm? Or Is there a world beyond the image wars?" En *Iconoclasm, Beyond the Image Wars in Science, Religion and Art*, editado por Peter Weible et al., 14-37. Cambridge: MIT Press.
- 2005. *Reemsamblar lo social. Una introducción a la teoría actor-red*. Buenos Aires: Manantial.
- Law, John. 1998. "After metanarrative: On knowing in tension". En *Into the Realm of Organisation: Essays for Robert Coper*, editado por Robert Chia, 88-108. Londres: Routledge.
- Law, John, y Annemarie Mol. 2001. "Situating Technoscience: An inquiry into spartialities". *Society and Space* 19: 609-21.
- Lessig, Lawrence. 2006. *Code 2.0*. Nueva York: SoHo Books.
- Levin, Avner, y Patricia Sánchez. 2009. "Two notions of privacy online". *Vanderbilt Journal of Entertainment y Technology Law* 11: 1001-51.
- Licklider, Joseph Carl Robnett, y Robert Taylor. (1968) 2001. "The computer as a communication device". *Kurzweil. Accelerating Intelligence*, 9 de noviembre
<http://www.kurzweilai.net/the-computer-as-a-communication-device>

- Locke, John. (1690) 1980. *Second Treatise of Government*. Indianapolis: Hackett Pub. Co.
- Maclaine, Polly, y Hernán Thomas. 2007. "How the Vineyard came to Matter: Grape Quality, the Meaning of Grapevines and Technological Change in Mendoza's Wine Production". *Universum* 1 (22): 217-234. <http://www.redalyc.org/articulo.oa?id=65027763014>
- Martin, Brian, y Evellen Richards. 1995. "Scientific Knowledge, Controversy, and Public Decision Making". En *Handbook of Science and Technology Studies*, editado por Sheila Jasanoff et al., 506-26. Londres / Thousand Oaks / Nueva Delhi: Sage Publications.
- Martin, Kristen E. 2010. *Case BRI-1006 (a) Facebook (A): Beacon and Privacy*. Virginia: Business Roundtable Institute for Corporate Ethics.
- Mason, Alpheus Thomas. 1946. *Brandeis. A Free Man's Life*. Nueva York: Viking Press.
- MacKinnon, Catharine A. 1989. *Towards a Feminist Theory of the State*. Cambridge: Harvard University Press.
- Meikle, Graham. 2010. "It's like Talking to a Wall". En *Facebook and Philosophy: what's on your mind?*, editado por Dylan E. Wittkower, 13-20. Chicago: Open Court.
- Meulders-Klein, Marie-Thérèse. 2005. "L'irrésistible ascension de la "vie privée" au sein des droits de l'homme". En *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, editado por Frédéric Sudre, 305-33. Bruselas: Nemesis, Bruylant.
- Mitchell, William J. 1996. *City of bits: Space, Place, and the Infobahn (On Architecture)*. Cambridge: MIT Press.
- Moore, Barrington. 1984. *Privacy: studies in social and cultural history*. Nueva York: M. E. Sharp Inc.
- Moser, Ingunn. 2000. "Against Normalization: Subverting norms of Ability and Disability". *Science as Culture* 9 (2): 201-239.
- Murphy, Robert R. 1984. "Social distance and the veil". En *Philosophical Dimensions of Privacy. An Anthology*, editado por Ferdinand David Schoeman, 34-55. Nueva York: Cambridge University Press.
- Nelkin, Dorthy. 1995. "Scientific Controversies. The Dynamics of Public Disputes in the United States". En *Handbook of Science and Technology Studies*, editado por Sheila Jasanoff et al., 444-56. Londres-Thousand Oaks / Nueva Delhi: Sage Publications.

- Nimmer, Melville B. 1954. "The Right of Publicity". *Law y Contemporary Problems* 19: 203-27.
- Nissenbaum, Helen Fay. 2010. *Privacy in Context. Technology Policy and the Integrity of Social Life*. California: Stanford Law Books.
- Nye, David E. 1994. *American Technological Sublime*. Londres: Fontana-Collins.
- O'Brien, David M. 1979. *Privacy, Law, and Public Policy*. Westport: Greenwood Press.
- Oudshoorn, Nelly, y Trevor Pinch. 2005. Introducción a *How Users Matter. The Co-construction of Users and Technology*, de Nelly Oudshoorn y Trevor Pinch, 1-26. Cambridge: MIT Press.
- Owen, Matt. 2012. "Facebook Timeline case study: The Hunger Games". *Econsultancy Digital Marketers United*, 1 de mayo. <http://Econsultancy.com/ec/blog/9740-facebook-timeline-case-study-the-hunger-games>
- Pacey, Arnold. 2001. *Meaning in technology*. Cambridge: MIT Press.
- Pérez Luño, Antonio Enrique. 1984. *Derechos humanos, Estado de derecho y Constitución*. Madrid: Tecnos.
- Pinch, Trevor. 1997. "La construcción social de la tecnología: una revisión". En *Innovación tecnológica y procesos culturales. Nuevas perspectivas teóricas*, editado por María Josefa Santos y Rodrigo Díaz, 20-38. México: Fondo de Cultura Económica.
- Pinch, Trevor, y Wiebe Bijker. 2008. "La construcción social de hechos y artefactos: o acerca de cómo la sociología de la sociología de la ciencia y la tecnología pueden beneficiarse mutuamente". En *Actos, actores y artefactos. Sociología de la tecnología*, editado por Hernán Thomas y Alfonso Buch, 19-62. Buenos Aires: Universidad Nacional de Quilmes Editorial.
- Post, Robert. 1995. "The Social Foundation of Privacy". En *Constitutional Domains: Democracy, Community, Management*, de Robert Post, 51-88. Cambridge: Harvard University Press.
- Pouillet, Yves, y Antoinette Rouvroy. 2009. "Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une reevaluation de l'importance de la vie privée pour la démocratie". En *État de droit et virtualité*, editado por Karim Benyekhlef y Pierre Trudel, 157-222. Montreal: Les Éditions Thémis.

- Quan-Haase, Anabel, y Alyson Young. 2010. "Uses and gratifications of social media: A comparison of Facebook and instant messaging". *Bulletin of Science, Technology and Society* 30 (5): 350-61.
- Quéau, Philippe. 1995. *Lo virtual. Virtudes y vértigos*. Barcelona: Paidós.
- Randall, Adrián J. 1986. "The Philosophy of Luddism: The Case of the West England Woolen Workers, ca. 1790-1809". *Technology and Culture* 27: 1-17.
- Regan, Priscilla M. 1995. *Legislating Privacy, Technology, Social Values and Public Policy*. Chapel Hill: University of North Caroline Press.
- Reiman, Jeffrey H. 1984. "Privacy, Intimacy and Personhood". En *Philosophical Dimensions of Privacy. An Anthology*, editado por Ferdinand D. Schoeman, 300-16. Nueva York: Cambridge University Press.
- Rheingold, Howard. 2008. "Virtual communities – exchanging ideas through computer bulletins boards". *Journal or Virtual Worlds Research* 1 (1). doi:<http://dx.doi.org/10.4101/jvwr.v1i1.293>
- Rule, James B. 2007. *Privacy in the Peril. How we are sacrificing a fundamental right in exchange for security and convenience*. Nueva York: Oxford University Press.
- Schoeman, Ferdinand David, ed. 1984. *Philosophical Dimensions of Privacy. An Anthology*. Nueva York: Cambridge University Press.
- Scholz, Trebor. 2010. "Introduction: Points of Control". *Social Research: An International Quarterly* 77(3): 931-40.
- Schwartz, Paul M. 1999. "Privacy and Democracy in Cyberspace". *Vanderbilt Law Review* 52: 1610-701.
- 2000. "Beyond Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practice". *Wisconsin Law Review*: 743-88. <https://escholarship.org/uc/item/1h80117d>
- Scott, James C. 1985. *Weapons of the Weak: Everyday Forms of Peasant Resistance*. New Haven: Yale University Press.
- Sennett, Richard. 1977. *The Fall of Public Man*. Nueva York / Londres: Knopf.
- Silverstone, Roger. 1992. *Consuming Technologies. Media and Information in Domestic Spaces*. Nueva York / Londres: Routledge.
- Simmel, Georg. 1950. *The sociology of Georg Simmel*. Glencoe: The Free Press.

- Sismondo, Sergio. 2010. *An Introduction to Science and Technology Studies*. Malden: Blacwell Publishing Ltd.
- Slobogin, Christopher, y Joseph E. Schumacher. 1993. "Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look". *Duke Law Review* 42 (4): 727-75.
<https://bit.ly/36EFpeC>
- Smith, Robert Ellis. 2004. *Ben Franklin's Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence: Privacy Journal.
- Solove, Daniel J. 2002. "Conceptualizing privacy". *California Law Review* 90 (4): 1088-1155.
- 2004. *The Digital Person. Technology and Privacy in the Information Age*. Nueva York: New York University Press.
- 2008. *Understanding Privacy*. Cambridge: Harvard University Press.
- Solove, Daniel J., Marc Rotenberg y Paul M. Schwartz. 2006. *Privacy, Information, and Technology*. Nueva York: Aspen Publishers.
- Starr, Paul. 1994. "Seductions of Sim: Smart Machine". *American Prospect* 17: 19-29.
- Steinfeld, Charles, Nicole B. Ellison y Cliff Lampe. 2007. "Social capital, self-esteem, and use of online social network sites; A longitudinal analysis". *Journal of Applied Developmental Psychology* 29(6): 434-45.
doi:10.1016/j.appdev.2008.07.002
- Strahilevitz, Lior J. 2005. "A social networks Theory of Privacy". *University of Chicago Law Review* 72 (3): 919-88.
- Stutzman, Fred. 2006. "Case Study: Facebook Feeds and Networked Political Action". *Unit Structures blog*. <https://bit.ly/3bFnPrp>
- Sudén, Jenny. 2003. *Material Virtualities: Approaching Online Textual Embodiment*. Nueva York: Peter Lang.
- Tavani, Herman T. 2008. "Informational Privacy: Concepts, Theories and Controversies". En *The Handbook of Information and Computer Ethics*, editado por Kenneth Einar Himma y Herman T. Tavani, 131-64. Nueva York: Hoboken.
- 2010. *Ethics and Technology. Controversies Questions and Strategies for Ethical Computing*. Nueva Jersey: Wiley.
- Terranova, Tiziana. 2000. "Free Labor. Producing culture for the digital economy". *Social Text* 18 (63): 33-57.

- Thaler, Richard, y Cass Sustein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven: Yale University Press.
- Thomas, Hernán E. 1999. “Dinâmicas de inovação na Argentina (1970-1995), Abertura comercial, crise sistêmica e rearticulação”. Tesis de doctorado, Universidad Estadual de Campinas.
- 2008. “Estructuras cerradas *versus* procesos dinámicos: trayectorias y estilos de innovación y cambio tecnológico”. En *Actos, actores y artefactos. Sociología de la tecnología*, editado por Hernán Thomas y Alfonso Buch, 217-62. Buenos Aires: Editorial Universidad Nacional de Quilmes.
- Thomas, Hernán E., Mariana Versino y Alberto Lalouf. 2007. “Trayectoria socio-técnica y estilos de innovación en países subdesarrollados: resignificación de tecnologías en una empresa nuclear y espacial argentina”. En *Globalización, acumulación de capacidades e Innovación: los desafíos para las empresas, localidades y países*, editado por Gabriela Dutrénit, Javier Jasso Villazul y Daniel Villavicencio, 384-414. México: Fondo de Cultura Económica y Organización de Estados Iberoamericanos.
- Trudel, Pierre. 2009. “État de droit et e-gouvernement”. En *État de droit et virtualité*, editado por Karim Benyekhlef y Pierre Trudel, 373-410. Montreal: Les Éditions Thémis.
- Turkle, Shirley. 2009. *Simulation and its discontents*. Cambridge: MIT Press.
- Turow, Joseph. 2003. “Americans and Online Privacy: The system is broken”, informe del *Annenberg Public Policy Center of the University of Pennsylvania*. http://repository.upenn.edu/asc_papers/401/
- Vercelli, Ariel, y Hernán Thomas. 2007. “La co-construcción de tecnologías y regulaciones: análisis socio-técnico de un artefacto anti-copia de Sony-BMG”. *Espacios* 28 (3): 5-30.
- 2008. “Repensando los bienes intelectuales comunes”. *Scientiae Studia* 28 (3): 427-442. <https://bit.ly/32aK7yc>
- Warren, Samuel D. y Louis D. Brandeis. 1890. “The right to privacy”. *Harvard Law Review* 4 (5): 193-220.
- Weiser, Mark. 1991. “The Computer for the 21st century”. *Scientific American* 265, 3: 94-104.

- Westin, Alan F. 1984. "The origins of modern claims to privacy". En *Philosophical Dimensions of Privacy. An Anthology*, editado por Ferdinand D. Schoeman, 56-74. Nueva York: Cambridge University Press.
- Westin, Alan F., y Louis Harris. 1990. *Consumers in the Information Age. Findings from the Survey*. Atlanta: Equifax Inc.
- 1998. *The Privacy Concerns and Consumer Choice. Findings from the Survey*. Atlanta: Equifax Inc.
- Whitley, Richard D. 1972. "Black boxism and the sociology of science: A discussion of the mayor development in the field". En *The Sociology of Science*, editado por Paul Halmos y Martin Albrow, 62-92. Keele: University of Keele.
- Winner, Langdon. 2008. *El reactor y la ballena. Una búsqueda de los límites de la era de alta tecnología*. Barcelona: Gedisa.
- Withman, James. 2004. "The Two Western Cultures of Privacy: Liberty vs. Dignity". *The Yale Law Journal* 113: 1151-1221.
http://digitalcommons.law.yale.edu/fss_papers/649
- Wittkower, Dylan E. 2010. "A Reply to Facebook Critics". En *Facebook and Philosophy: what's on your mind?*, editado por Dylan E. Wittkower, xxi-xxx. Chicago: Open Court.
- Zimmerman Umble, D. 1992. "The Amish and the telephone. Resistance and reconstruction". En *Consuming technologies. Media and Information in Domestic Spaces*, editado por Roger Silverstone y Eric Hirsch, 103-8. Londres / Nueva York: Routledge.
- Zittrain, Jonathan. 2006. "The Generative Internet". *Harvard Law Review* 119 (7): 1975-2040.

Notas de prensa

- BBC News. 2009. "Facebook 'Withdraws' data changes". *BBC News*, 18 febrero. Acceso el 27 de mayo de 2015.
<http://news.bbc.co.uk/2/hi/technology/7896309.stm?lss>
- Evangelista, Benny. 2009. "As Facebook Thrives, dos privacy have to fade?". *San Francisco Chronicle*, 30 de diciembre. Acceso el 27 de mayo de 2015. <https://bit.ly/3bFoucW>

- Gates, Guilbert. 2010. "Facebook Privacy: A Bewildering Tanble of Options". *New York Times*, 12 de mayo. Acceso el 27 de mayo de 2015. <https://nyti.ms/3jYDtKb>
- Hamblen, Matt. 2001. "McNealy Calls for Smart Cards to Help Security". *Computerworld*, 12 de octubre. Acceso el 27 de mayo de 2015. <https://bit.ly/326XuiO>
- Hoofnagle, Chris y Michael Zimmer. 2010. "How to win friends and manipulate people". *The Blog*, 25 de mayo. Acceso el 27 de mayo de 2015. <https://bit.ly/2ZfvLKL>
- Kirkpatrick, Marshall. 2010. "Facebook's Zuckerberg says the age of privacy is over". *The New York Times*, 10 de enero. Acceso el 27 de mayo de 2015. <https://nyti.ms/36DoOba>
- McCarthy, Caroline. 2007. "Facebook respond to MoveOn criticism of ad program". *CNET News*, 20 de noviembre. Acceso el 27 de mayo de 2015. <https://www.techmeme.com/071121/p89#a071121p89>
- McCullagh, Declan. 2010. "Why no one cares about privacy anymore". *CNET News*, 12 de marzo, acceso el 27 de mayo de 2015. <https://cnet.co/3npxeJa>
- Newman, Jared. 2009. "Facebook privacy changes: The good and the bad". *PC World*, 11 de diciembre. Acceso el 27 de mayo de 2015. <https://bit.ly/3jXQWsJ>
- North, Irene. 2010. "People concerned over more Facebook privacy changes". *The Daily Censored. Underreported News and Commentary*, 26 de abril. Acceso el 27 de mayo de 2015. (enlace fuera de línea) <https://bit.ly/3bHwTMy>
- Parr, Ben. 2008. "Social media and privacy: Where are we two years after Facebook News Feed?". *Mashable*, 8 de septiembre. Acceso el 25 de mayo de 2015. <https://bit.ly/3m2NBuA>
- Paul, Ian. 2010. "Facebook Privacy Complaint: A Complete Breakdown". *PCWorld*, 6 de mayo, <https://bit.ly/3ic6SqT>
- Pérez, Juan Carlos. 2007. "Facebook's Beacon more intrusive than previously thought". *PCWorld*, 30 de noviembre. Acceso el 27 de mayo de 2015. <https://www.pcworld.com/article/140182/article.html>

- Rotenberg, Marc. 2010. "Testimony and statement for the record of Marc Rotenberg in the Hearing On Line, Social Networking, and Crime Victimization". Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. Washington, 28 de julio. Acceso el 10 de enero de 2015.
- Schmidt, Tracy Samantha. 2006. "Inside the Blacklash Against Facebook, Time.com". *Time US*, 6 de septiembre. Acceso el 27 de mayo de 2015. <https://bit.ly/338I9O2> (contenido no disponible).
- Stone, Brad. 2009a. "Facebook Rolls Out New Privacy Settings". *New York Times*, 9 de diciembre. Acceso el 27 de mayo de 2015. <https://nyti.ms/2I2uql0>
- 2009b. "Privacy Group Files Complaint on Facebook Changes". *New York Times*, 17 de diciembre. Acceso el 27 de mayo de 2015. <https://nyti.ms/36Qy243>
- Szoka, Berin. 2009. "Facebook Privacy Controls Change & EPIC's FTC Complaint". *The Technology Liberation Front*, 17 de diciembre. <https://bit.ly/2A7nzCT>
- Terdiman, Daniel. 2009. "EPIC readying federal complaint over Facebook privacy policy". *News CNET*, 17 de febrero. Acceso el 27 de mayo de 2015. <https://cnet.co/36Hrwwb>
- Weiner, Nata. 2007. "Facebook Beacon: Two weeks later". *Blog The Idea Shower*, 30 de noviembre. Acceso el 27 de mayo de 2015. <https://bit.ly/3bMkrLu>

Información en Facebook

- Bowen, Jeff. 2011. "Noticias para desarrolladores". *Blog de Facebook*, 14 de enero. <https://bit.ly/3lX10UK>
- Cox, Chris. 2011. "Making it easier to share with who you want". *Blog de Facebook*. Acceso el 23 de agosto de 2014. <https://blog.facebook.com/blog.php?post=10150251867797131>
- Eyal, Michael. 2011. "Who, What, When, and Now ... Where". *Blog de Facebook*. Acceso el 15 de abril de 2011. <https://blog.facebook.com/blog.php?post=418175202130>

- Kelly, Chris. 2009. "Improving Sharing Through Control, Simplicity and Connection". *Blog de Facebook*. Acceso el 25 de abril de 2009.
<https://bit.ly/2R4tVIIt>
- McDonald, Paul. 2011. "Timeline. Now Available Worldwide". *Blog de Facebook*. Acceso el 15 de marzo de 2012.
- Schrage, Elliot. 2009. "Improving Transparency around Privacy". *Blog de Facebook*. Acceso el 30 de octubre de 2009.
<https://blog.facebook.com/blog.php?post=167389372130>
- Zuckerberg, Mark. 2006a. "An Open Letter from Mark Zuckerberg". *Blog de Facebook*. Acceso el 15 de marzo de 2009.
<http://blog.facebook.com/blog.php?q=Zuckerberg+2006>
- 2006b. "Calm down. Breathe. We hear you". *Blog de Facebook*. Acceso el 15 de marzo de 2009.
<http://blog.facebook.com/blog.php?q=Zuckerberg+2006>
- 2006c. "The next step...". *Blog de Facebook*. Acceso el 15 de marzo de 2009.
<http://blog.facebook.com/blog.php?q=Zuckerberg+2006>
- 2007a. "Thoughts on Beacon". *Blog de Facebook*. Acceso el 15 de marzo de 2009.
<https://blog.facebook.com/blog.php?post=7584397130>
- 2007b. "Announcement: Facebook Users Can Now Opt-Out of Beacon Feature". *Blog de Facebook*. Acceso el 15 de marzo de 2009.
<https://blog.facebook.com/blog.php?post=7584397130>
- 2009a. "On Facebook People Own and Control Their Information". *Blog de Facebook*. Acceso el 15 de diciembre de 2009.
<https://blog.facebook.com/blog.php?post=54434097130>
- 2009b. "Governing Facebook Service in an Open and Transparent Way". *Blog de Facebook*. Acceso el 15 de diciembre de 2009.
<https://blog.facebook.com/blog.php?post=56566967130>
- 2009c. "Update on Terms". *Blog de Facebook*. Acceso el 15 de diciembre de 2009.
<https://blog.facebook.com/blog.php?post=54746167130>

Documentos legales

- Acta de Privacidad de 1974 de Estados Unidos y sus Enmiendas (1974).
Carta de la Comisión Federal de Comercio de Estados Unidos a EPIC sobre su demanda contra Facebook.
- Carta enviada a Mark Zuckerberg por parte de EPIC, ACLU, CDT, Center for Digital Democracy, Consumer Action, Consumer Watchdog, Electronica Foundation y Privacy Rights Clearinghouse, 16 de junio de 2010.
- Comentarios de EPIC a la Comisión Federal de Comercio, Mesas redondas de privacidad, proyecto n.º P095416, 26 de enero de 2010.
- Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma en 1950, http://www.echr.coe.int/Documents/Convention_SPA.pdf
- Demanda a Facebook de la Clínica de Interés Público y de Política de Internet de Canadá (CIPPIC), que contiene 24 alegatos sobre 22 temas distintos, 30 de mayo de 2008.
- Demanda de EPIC a la Comisión Federal de Comercio “Complaint, Request for Investigation, Injunction, and Other Relief”. Washington, D. C., 17 de diciembre de 2009.
- EPIC. “Information Act”. Solicitud a la GSA sobre acuerdos entre la GSA y las compañías de redes sociales y las firmas de nubes de computación. 2009.
- Grupo de Trabajo de Protección de Datos de la Comunidad Europea. 2009. “Opinion 5/2009 on line social networking” adoptado el 12 de junio del 2009. Artículo 29.
- Memorándum de Roma. (2008). Del Grupo de Trabajo Internacional de Berlín sobre Recolección de Datos en Telecomunicaciones. Marzo. Security Issues and Recommendations for Online Social Networks. 2007. ENISA (European Network and Information Security Agency). Octubre 2007.
- PIPEDA (Personal Information Protection and Electronic Documents Act). *Government of Canada*. Acceso el 15 de julio de 2010. <http://laws-lois.justice.gc.ca>

Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc., 2009

Por Elizabeth Denham, Asistente de la Comisaria de Privacidad de Canadá.

Resolución de la Comisión Federal de Comercio. 29 de noviembre de 2011.

Respuesta a EPIC de la GSA sobre acuerdos entre la GSA y las compañías de redes sociales y las firmas de nubes de computación. 2009.

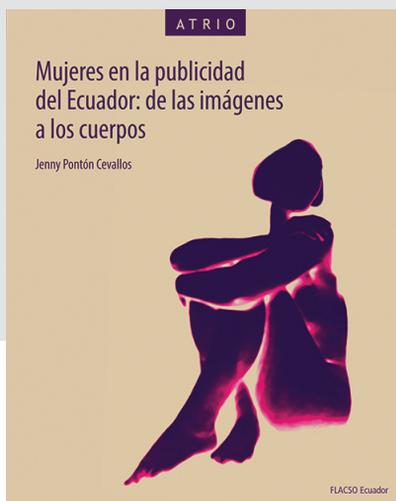
Segundo documento de la demanda de EPIC a la Comisión Federal de Comercio “Supplemental Materials in Support of Pending Complaint and Request for Injunction Request for Investigation and for Other Relief”.

Sobre la autora



María Belén Albornoz (Quito 1965), doctora en Ciencias Sociales por la Universidad Nacional de Cuyo (Argentina) con un posdoctorado por la Universidad de Aalborg (Dinamarca). Es profesora investigadora en el Departamento de Asuntos Públicos de FLACSO Ecuador y coordinadora de CTS LAB. Ha sido profesora visitante en Rensselaer Polytechnic Institute (EE.UU 2017) y ganó el *Fulbright Award* en 2017. Forma parte del consejo de la *Society for Social Studies of Science* (4S) y del directorio de la *Society for the Studies of New and Emerging Technologies* (S.NET), y es presidenta de la Sociedad de Estudios Sociales de Ciencia y Tecnología (CTS Ecuador). Investiga sobre modelos de transferencia tecnológica; políticas de ciencia, tecnología e innovación; big data; redes de política y trabajo justo en la *gig economy*. En 2017 publicó *Ingeniería, innovación y tecnología social* (Universidad Nacional de Quilmes); en 2015, *Políticas tecnológicas y tecnologías políticas. Dinámicas de inclusión, desarrollo e innovación en América Latina* (Universidad Nacional de Colombia).

Explora, en acceso abierto, otros títulos



Más libros de Editorial FLACSO Ecuador, aquí



Luego de que supimos que Cambridge Analytica y Facebook usaron algoritmos para influenciar en las campañas electorales, la relación entre política, privacidad y tecnología quedó al descubierto. Ahora no hay ninguna duda de que se pueden cuantificar los comportamientos sociales, conocer los estilos de vida de las personas e identificar grupos de votantes que puedan ser influenciados a través de Facebook.

Pero de todo aquello no conocíamos cuando Thefacebook apareció, cuando todavía no había llegado la era de la postverdad ni se consideraba un derecho humano a la propiedad y el control de los datos. No obstante, Belén Albornoz, la autora de este libro, demuestra que Thefacebook es parte del origen de las tecnologías invasivas y un primer momento en el cual la ciudadanía comenzó a percatarse de que su privacidad está en riesgo. Desde un abordaje sociotécnico explica cómo los artefactos y los códigos informáticos coproducen la privacidad en las redes sociales. Se detiene en el artefacto tecnológico de Facebook para mostrar su incidencia en el cambio de las normas sociales. Es así como esos artefactos se vuelven parte constitutiva de las relaciones sociales, culturales, económicas y políticas, al mismo tiempo que estas relaciones se materializan en otros artefactos y sistemas tecnológicos.

Este libro, en el cual la tecnología es uno de los actores en la construcción de la privacidad, nos permite entender desde cuándo los algoritmos empezaron a moldear nuestras vidas.