La privacidad como integridad contextual y su aplicación a las redes sociales

Pribatutasuna testuinguru-integritate gisa eta honen aplikazioa sare sozialetan

Privacy as contextual integrity and its application to social networks sites

Amaya Noain Sánchez[1]

zer

Vol. 20 - Núm. 39
ISSN: 1137-1102
e-ISSN: 1989-631X
DOI: 10.1387/zer.15531
pp. 163-175
2015

Recibido el 16 de septiembre de 2014, aceptado el 10 de noviembre de 2015.

Resumen
El objetivo del siguiente texto es presentar la teoría de la integridad contextual enunciada en 1997 por Helen Nissenbaum como marco teórico para la protección de la información privada en escenarios de vigilancia pública. Nissenbaum enlaza la salvaguarda de la privacidad en la era de la información al mantenimiento de las normas informativas que rigen cada contexto, proporcionando un punto de partida alternativo para la protección de los datos privados de los usuarios de las redes sociales.

Palabras clave: Esfera privada, privacidad, redes sociales, integridad contextual, privacidad en público.

Laburpena
Lan honen helburua 1997. urtean Helen Nissenbaum-ek hedatutako testuinguru-integritatearen teoria marko teoriko gisa aurkeztea da, zaingo publikoko eremutan informazio pribatua babesteko. Nissenbaum-ek informazio-aroko pribatutasunaren babesa testuinguru bakoitzak eskatzen dituen informazio arauen mantentzearekin lotzen ditu, sare sozialen erabiltzaileen datu pribatuen babesa lortzeko abiapuntu alternatibo bat emanez.

Gako-hitzak: Esparru pribatua, pribatutasuna, sare sozialak, testuinguruaren integrazioa, pribatutasuna esparru publikoan

[1] Universidad Complutense de Madrid, amayanoain@ucm.es

Abstract
The following article is aimed to introduce Helen Nissenbaum's contextual integrity, a theoretical approach formulated in 1997 as a benchmark for preserving privacy in the context of public surveillance. The author links the privacy protection in the digital age to the respect of the informational norms of a particular context, providing, therefore, an alternative starting point to preserve user's private data when intereacting on Social Networks Sites.

Keywords: Privacy realm, privacy, social network sites, contextual integrity, privacy in public.

0. Introducción

Tradicionalmente, el espacio público era aquel constituido por los asuntos que incumbían a la colectividad e incluían una interacción cara a cara en lugares compartidos, oponiéndose así a lo privado, que quedaba confinado al ámbito reservado del individuo, a su esfera protegida. Dicha consideración se antoja ineficiente por cuanto esta dicotomía rara vez se presenta de manera aséptica y no contempla las intromisiones en la vida privada producidas en el espacio público. Más aún en la actualidad, donde lo público es aquello que queda expuesto a la mirada a través de los medios de comunicación y lo privado lo que queda oculto de los *mass media* (Thompson 1998: 166). En esta redefinición de estadios en la que ambos ya no están determinados por la naturaleza de sus temáticas sino por la visibilidad que confieren a los acontecimientos en los medios de comunicación, el espacio público se torna en espacio mediático, disociado de la presencia física y estructurando muchos de sus contenidos con asuntos pertenecientes a la esfera reservada del individuo (García Jiménez, 2008: 105). En este escenario, uno de los mayores desafíos que nos plantean las nuevas tecnologías es delimitar un concepto de privacidad[2] que implique qué debe quedar protegido y qué se considera intromisión.

1. El problema de la privaciad en público

Desde las primeras concepciones de privacidad defendidas por filósofos del derecho como John Stuart Mill hasta la actual visión normativa, la protección de la intimidad y vida privada del individuo se ha centrado, exclusivamente, en la distinción entre espacios privados y públicos, perdiéndose en delimitaciones conceptuales acerca de lo que incumbe a cada esfera y revelándose, a la postre, ineficiente en escenarios reales donde esta distinción no es meridiana. Desde esta perspectiva, la mayoría de aproximaciones observan la problemática a través de las lentes de las intromisiones, ya sean producidas en la esfera privada o, por el contrario, por la desaparición del ágora pública a favor de lo personal (Sennet, 1977). Como consecuencia, equiparan erróneamente privacidad con esfera privada, lo que provoca que la protección de las informaciones privadas fuera del ecosistema reservado del individuo no sean consideradas legítimas de ser protegidas. En este sentido, Helen Nissenbaum denuncia que la mayoría de las teorías normativas y filosóficas fracasan al no identificar correctamente el problema que supone la aparición de datos privados en escenarios públicos, subestimándolo e, incluso, obviándolo en su totalidad[3].

El despliegue de información sobre la vida privada en espacios públicos no es algo nuevo de los entornos digitales. En numerosas ocasiones los datos privados son necesarios para completar acciones de la vida cotidiana, desde ir al médico o realizar gestiones bancarias, hasta mantener una conversación entre amigos, y, reflejo

[2] Usamos la voz "privacidad" al igual que "intimidad" y "vida privada" para traducir el término inglés *privacy*. La correspondencia semántica, no obstante, no es exacta en castellano. De dicha cuestión se ocupa Helena Béjar en *El ámbito íntimo: privacidad, individualismo y modernidad*. Madrid: Alianza.

[3] El estudio de la privacidad en público defendido por Nissebaum en 1997 como punto de partida para sustentar la teoría de la integridad contextual, fue anticipado por Allen en 1988 y retomado posteriormente por Slobogin en 2002.

de ello, lo mismo sucede en los espacios virtuales. La diferencia recae en que estos representan, por sus características inherentes, una esfera social única y novedosa en la que grandes cantidades de información son susceptibles de ser almacenadas y agregadas (Giovanni y Pashley, 2005) y los datos proporcionados pueden ser fácilmente copiados, utilizados y sacados de contexto (Boyd, 2006).

Antes de los recientes avances en tecnologías de la información, el problema de la privacidad en público no había experimentado la extensión que tiene actualmente tiene. En el pasado, la mayoría de los individuos asumían que sus actividades y movimientos del día a día no eran ni vigilados, ni catalogados, por lo que enlazaban sus actividades cotidianas de manera anónima. En la sociedad actual, por contra, la tecnología es capaz de obtener, procesar, analizar y agregar cantidades ingentes de información sobre una persona concreta. Dichos avances significan que, virtualmente, "no hay límite en la cantidad de información que puede ser recogida, ni en el nivel de análisis de datos que puede ser realizado y que la información puede ser compartida con facilidad y digitalmente almacenada para siempre" (Zimmer, 2005: 108). La consecuencia es "el incremento en la magnitud, detalle, meticulosidad y capacidad de la habilidad para vigilar el día a día de los ciudadanos mientras realizan sus actividades públicas" (Nissenbaum, 2004: 576). Alguien que compra en el supermercado es anónimo, así como los productos que adquiere pero cuando esto se produce en la Web su poder de agregación de información hace que podamos identificar al usuario hasta límites insospechados, perfilándole para averiguar sus pasos como potencial consumidor.

Si la observación en lugares públicos se ha convertido en parte de la vida diaria de los ciudadanos en la actualidad, la dificultad recae en cómo conjugar esas prácticas de vigilancia pública y de agregación de información con la protección de datos privados en esos lugares. Sabemos que el aspecto normativo reconoce que la protección de la vida privada debe ser medida respecto a otros valores y en función del contexto, existiendo, por tanto, una competencia de intereses. Un simple ejemplo de tal juicio valorativo es nuestra disposición a desplegar información privada y permitir que nuestra maleta sea buscada en los aeropuertos: la seguridad se juzga en estas situaciones y es más importante que la reserva de nuestras informaciones privadas. Lo mismo sucede con la privacidad en público. Aunque la mayor parte de la información recolectada en esas situaciones de vigilancia es considerada inocua, es posible que para otros contextos deseemos mantenerla en privado. Sin embargo, la identificación de privacidad con esfera privada hace que, conceptualmente, "la idea de que la privacidad pueda ser violada de alguna manera en un espacio público sea considerada, a menudo, paradójica. Para la mayoría, el valor de la privacidad se aplica exclusiva y únicamente a la esfera de la privacidad del individuo" (Zimmer, 2005: 107). Empero, el rango de dimensiones de la privacidad es mucho más extenso y va desde la información, a las actividades, decisiones, pensamientos y comunicación, entre otros, por lo que una teoría global sobre protección de la vida privada debería tener en cuenta todas estas dimensiones lo que se antoja imposible. En este sentido, el planteamiento de Nissenbaum no pretende una simple enumeración de atribuciones a lo público y a lo privado, ni una descripción de todos estos aspectos donde los datos privados entran en juego, sino que aporta un nuevo marco teórico para la protección de la vida privada en lo que concierne a las informaciones sobre los individuos.

Para verificar la ineficiencia del modelo bipolar privado *versus* público, Nissenbaum parte del análisis de tres principios que han guiado las políticas de protección de la vida privada en la tradición jurídica anglosajona, tres formas de conceptuar la privacidad por oposiciones entre binomios: competencias gubernamentales para vigilancia y control de datos *versus* privacidad del individuo[4], designación de lugares públicos frente a lugares privados o espacios de no intromisión[5] y catalogación entre información sensible e información no sensible. Dichas oposiciones, aunque útiles desde perspectivas teóricas, conllevan carencias por cuanto la aplicación de estos principios no es siempre obvia y en numerosas ocasiones, la línea divisoria no es ni estática, ni universal.

Las dos primeras oposiciones –que definirían el área en la cual el individuo no es molestado ni sufre intromisión alguna por parte de los poderes estatales, siendo, además, este área de naturaleza física– desembocarían en una protección exclusiva de la esfera privada, equiparando privacidad con espacio privado. Sin embargo, como indicábamos brevemente, los términos "esfera privada" y "privacidad" no son sinónimos. La esencia de la esfera privada evocaría al espacio protegido donde uno puede ocultarse completamente del mundo exterior[6], mientras que la privacidad o informaciones privadas poseen una dimensión más amplia, y aunque su ecosistema natural es la esfera privada puede saltar al ágora pública convirtiéndose en una parte importante y necesaria de la interacción social.

El tercer binomio que distingue entre datos sensibles o no sensibles no queda exento de problemas. Nissenbaum recupera la perspectiva de teóricos y filósofos sobre privacidad que sostienen que el grado de sensibilidad de la información debe ser un factor determinante para discernir si se ha producido o no una intromisión en la vida privada. Estos estudios buscan redefinir la categoría de la llamada "información sensible" y explican por qué el grado de sensibilidad es clave a la hora de defender las informaciones privadas. La autora toma el término "información sensible" de la tradición jurídica[7] y, en concreto, de Raymond Wacks adoptando su definición apor-

[4] En este sentido el derecho a la privacidad del individuo está configurado como un método de mantener a los gobiernos fuera de las vidas privadas de los ciudadanos, un argumento para proteger la información íntima y sensible de la intrusión de los poderes públicos. Helena Béjar señala la concepción de la privacidad como libertad negativa, en referencia al área en la cual el individuo no es molestado, ni sufre intromisión alguna: "libertad de algo o alguien respecto a la intervención pública." El concepto, que nace del ideal de libertad enunciado por John Stuart Mill, parte de una idea más genérica: el individualismo, enunciado por Alexis de Tocqueville en *Democracia en América*. Helena Béjar en *El ámbito íntimo: privacidad, individualismo y modernidad*, (1988).

[5] Tal y como sostiene Béjar, tras este principio se esconde las idea ancestral de la sacralización de ciertos espacios o, más concretamente, lugares físicos considerados de no intromisión, excepto cuando hay poderosos argumentos que indiquen lo contrario. En la tradición anglosajona, esta zona privada protegida se recoge en la Tercera y Cuarta Enmiendas de la Carta de Derechos de los Estados Unidos, definiendo límites explícitos del acceso del gobierno a los hogares. Esta identificación de esfera privada con lugar físico proviene del ideario de Samuel y Brandeis: "la common law siempre ha reconocido que la casa de un hombre es su castillo" y es recogida por otros estudiosos como Michael R. Curry en *Discursive displacement end the seminal ambiguity of space and place* (2002).

[6] CAPURRO, Rafael: Conferencia sobre la protección de la vida privada en las redes sociales pronunciada en el *II Congreso Internacional de Ética de la Comunicación*. Sevilla, 3 de abril 2013.

[7] Para ello revisa los escritos de Charles Fried: *Privacy* (1968), Tom Gerety: *Redifining privacy* (1977) y William Parent: *Privacy morality and the law* (1983).

tada en *Personal Information: privacy and the law*. Distingue así entre "información /datos personales" en el sentido general de información sobre personas, mientras que se reserva los términos "sensible" o "confidencial" para las informaciones de carácter privado. Sin embargo, la estructura de la Web permite a menudo, que datos identificativos de carácter no sensible puedan llevarnos a obtener informaciones de carácter privado mediante triangulación de datos. En este sentido la autora admite que "el perfilado de usuarios en la red es problemático, incluso cuando la información proporcionada no es sensible y cuando esta tiene lugar en los espacios públicos de la Web" (Nissenbaum 2004: 116).

La disparidad de situaciones en las que se mezclan informaciones privadas en espacios públicos hace necesario cuestionar el marco ofrecido por estos tres principios como estándar universal para deliberar sobre la protección de la vida privada. Para ello, sustenta su planteamiento en dos parámetros. El primero es que la privacidad como integridad contextual, como marco conceptual, estaría condicionada por dimensiones temporales y de localización entre otras y, en este sentido admite la variabilidad que se puede dar en la categorización de informaciones sensibles o no sensibles a través de diferentes culturas, períodos históricos y lugares. El segundo es que no se enuncia en términos maniqueos del tipo "público" *versus* "privado", "sensible" "no sensible" o "gobierno" "privado", ya que dichas distinciones se tornan inútiles fuera de las aproximaciones teóricas.

2. La privacidad como integridad contextual

El planteamiento de la integridad contextual fue enunciado por Nissenbaum en 1997 y constituye un marco conceptual que enlaza la protección de la información privada a las normas específicas que imperan en cada contexto. Esta aproximación teórica parte de la creencia de que todas las actividades que realizan los individuos tienen lugar en una pluralidad de esferas distintas definidas, cada una de ellas, por una serie de normas que gobiernan varios aspectos tales como roles, expectativas, acciones o prácticas. Dentro de estos contextos las normas existen tanto implícita como explícitamente, conformando y limitando comportamientos y perspectivas. La idea central de la integridad contextual se fundamenta en la siguiente creencia:

> "No hay arenas de la vida no gobernadas por normas informacionales […] Prácticamente todo: las actividades que llevamos a cabo, los acontecimientos que suceden, las transacciones que realizamos… todo ocurre en un contexto no sólo en cuanto a lugar, sino que conllevan unas convenciones y expectaciones culturales" (Nissenbaum 2004: 119).

Por ello, afirma, más que definir una teoría general sobre la protección de la vida privada en cada uno de esos escenarios, debemos aceptar la existencia de dichos dominios, ampliamente enraizados en la experiencia común, y gobernados por normas específicas[8].

[8] Nissenbaum hace referencia en este punto a los trabajos de Jeroen van den Hoven: "Privacy and the

De igual manera que las normas de comportamiento o las prácticas cambian en función de cada contexto particular, las normas que gobiernan el flujo de información personal también varían, indicando hasta qué punto el individuo puede desplegar ciertos datos privados y cuándo nuestra vida privada es invadida si las normas de información son contravenidas. Así, más que aportar definiciones universales sobre qué es público *versus* privado o una teoría global sobre la privacidad en público este planteamiento actúa dentro de los límites normativos de un determinado contexto.

Las normas de información gobiernan qué tipo y qué cantidad información personal es relevante y apropiada para ser compartida con otros así como a cuantos interlocutores y escenarios debe fluir. Dado que el marco de protección de los datos privados es la integridad contextual, una trasgresión en las normas informacionales que regulan el contexto supondría una violación de la privacidad, teniendo en cuenta, no obstante, que esta violación en ocasiones puede estar justificada por una fuerza mayor cuando otro elemento serio o urgente está en juego. En este sentido, el derecho a la intimidad y vida privada "no es ni un derecho al secreto, ni al control de la información, sino un derecho al apropiado flujo de información personal" (Nissenbaum 2010: 127).

Existe un número ilimitado de posibles fuentes para las normas contextuales incluyendo la historia, la cultura, la ley o la convención, entre otros. Nissebaum establece dos clases normativas que regulan el flujo de la información privada en contextos públicos: las "normas de propiedad" y de "distribución o de flujo de información".

2.1. Normas de propiedad

Son las que circunscriben el tipo o naturaleza de información sobre los individuos que, en un contexto concreto, se considera es aceptable, esperado o, incluso, demandado sea revelado. Es decir, cuándo es apropiado revelar esa información en un escenario particular. Por ejemplo, en la consulta del médico se considera oportuno que el individuo aporte datos sobre su condición física pero no sobre su salario.

En función de la situación, estas normas se tornan más o menos abiertas tal y como sucede en una conversación entre amigos donde la información personal fluye libremente. No así, sin embargo, en una clase o en una entrevista de trabajo, lugares en los que el flujo de información privada adecuado es regulado más estrictamente. Dado que no hay lugares fuera del amparo de las normas informacionales, estar en el más público de los lugares no significa que debamos dejar fluir todos nuestros datos privados o que "todo valga" en términos de nuestra información personal. Incluso en un espacio público por antonomasia como sería la calle, sentiríamos que se están entrometiendo en nuestra vida privada si un desconocido nos pregunta por nuestros nombres.

Las leyes de la propiedad enunciadas por Nissenbaum parten de aproximaciones filosóficas como la de James Rachels, quien estableció cómo las distintas relaciones humanas se encuentran parcialmente definidas por distintos patrones que indicarían la cantidad de información que se comparte en cada contexto. En este sentido, la visión de Rachels reclama que una adecuada protección de la vida privada otorgando al ciudadano el poder de compartir información discriminadamente, capacitándole

varieties of informational wrongdoing", en *Readings in Cyber Ethics* (2001).

no sólo para determinar cómo de cercana es la relación con los otros sino la naturaleza de sus relaciones: "En cada caso, la clase de relación que cada individuo tiene con otro envuelve una concepción de cómo es apropiado comportarse con él y la clase y grado de conocimiento concerniente sobre cada uno que es apropiadazo para ellos" (Rachels, 1975: 328). En la misma línea Ferdinand Schoeman arguye que los individuos mantienen diferentes relaciones con distintas personas en función de los contextos, por lo que "obtener información de una situación e insertarla en otra puede constituir una violación" (Schoeman, 1984: 408).

2.2. Normas de distribución o flujo de la información

Las normas de distribución o de flujo se refieren al movimiento o transferencia de información de una parte a otra u otras. Siguiendo las normas de propiedad, el contexto de una conversación con un amigo cercano permite un mayor flujo y un tipo más amplio de información privada desplegada: el día a día de mi vida diaria, opiniones políticas, emociones, experiencias sexuales, etc. Si bien, las normas de distribución prevendrán a nuestro interlocutor de distribuir dicha información a una tercera persona. En dichos casos, las normas protegen la distribución abierta e indiscriminada de mi información privada si no se cumplen ciertos requisitos.

3. La integridad contextual en las redes sociales

Algunos autores como Michael Zimmer encuentran en el marco teórico aportado por la integridad contextual la solución a los problemas referidos a la protección de la vida privada en los entornos creados por la Web 2.0. Así, de la misma manera que sucede en las relaciones en el entorno físico, cada escenario virtual estaría determinado por una serie de normas informacionales destinadas a mantener la integridad del contexto:

> "Cuando compro en la droguería, no hay nada secreto inherente a este hecho: lo hago en público, el cajero comprueba lo que me llevo, quizás también la persona que está en la misma cola e incluso se puede grabar en un perfil de comprador. Pero eso no significa que el contenido de mi bolsa: unas vitaminas, algo para el pelo o para mi salud sexual sea divulgado a todo el mundo en la tienda, compartido con mis compañeros de trabajo, familia o incluso gente que no conozco." (Zimmer, 2007).

En este sentido, el correcto uso de las normas de propiedad y flujo de la información indicaría que esos datos no deben divulgarse más allá del entorno donde se ha producido el intercambio de información y, dado que estas informaciones juegan un papel necesario en este escenario y su introducción se encuentra justificada por las normas que regulan el contexto, no se habría producido una violación de la privacidad.

Zimmer argumenta que, al igual que en las interacciones en espacios físicos, los usuarios de la Web 2.0 mantienen formulaciones particulares sobre su privacidad

personal, por lo que la teoría de la integridad contextual proporcionaría un marco valioso para la protección de la vida privada en la Red a nivel global, solventado problemas como los derivados de las distintas concepciones culturales de privacidad o algunas carencias del derecho referidas a la protección de la información privada en escenarios públicos.

Sin embargo, incluso cuando consideramos la noción más contextual de la privacidad en los entornos digitales, el hecho es que los usuarios tienden a compartir una cantidad ingente de información privada en la Web.[9]

Siguiendo la lógica de la integridad contextual cuando nos preguntamos qué lleva a los usuarios a mostrar unas informaciones y ocultar otras, llegaríamos a la conclusión de que es la cantidad de datos privados que ellos consideran necesarios para hacer funcionar la red social, tanto en términos de propiedad –la información que necesitan para que otros usuarios los encuentren, para dotar de sentido una conversación entre amigos, etc.– como en términos de distribución –modificando las opciones de privacidad para que esa información sea sólo visible a amigos, amigos de sus amigos o al público en general–. Pero, a diferencia de una conversación mantenida con un amigo en otro espacio social y público como sería la calle, el escenario público virtual aparece hipermedidado, lo que, en la mayoría de los casos, se opondría a la ley de la distribución y rompería la integridad contextual que protege la vida privada.

Del mismo modo, en el entorno digital y, más aun, en las aplicaciones de la Web 2.0, no resulta tan sencillo identificar contextos, lo que provoca que el usuario no siempre sepa por qué leyes informacionales guiarse. A este respecto existe un amplio debate acerca de cómo el uso de las redes sociales ha cambiado la percepción de la privacidad de los individuos, así como las acciones que toman para protegerla (Gross y Acquisti, 2005; Lampe, Ellison y Steinfield, 2008; Boyd y Hargittai, 2010). En estos recintos del espacio público mediado los individuos emplazan a voluntad parte de su información privada, destinada a nutrir estas redes y que sean útiles, pero aun cuando sopesan pormenorizadamente los datos que introducen, deben sacrifican una parte que ellos consideran razonable de su vida privada. Aunque priman alimentar su círculo social frente a su vida privada, muchos usuarios, sabedores de la importancia de la protección de su información personal, comparten sólo lo necesario para mantener su privacidad social a la vez que alimentan sus diferentes lazos relacionales dentro del mismo espacio confinado. Esta estrategia les permite conectar con toda su red social sin ser ni demasiado públicos no demasiado privados.

Con todo ello y, aunque conscientes de que están sacrificando parte de su información reservada, el hecho de que en las redes sociales formen parte de un espacio público acotado y que en ellas se desarrollen relaciones típicas de la esfera privada hace que, a menudo, sean percibidas como un espacio semipúblico, lo que actúa en detrimento del nivel de alerta del usuario.

En no pocas ocasiones esta indefinición torna inútil la aplicación de las normas de la integridad contextual. Al igual que Nissenbaum, Zimmer argumenta que este marco teórico está diseñado para considerar cómo la introducción de una nueva

[9] Barnes alude a la "Paradoja de la privacidad" según la cual, a la vez que los usuarios muestran un alto nivel de preocupación por la protección de su vida privada en la Red, continúan introduciendo cuantiosos datos privados para nutrirlas. Barnes, "A privacy paradox: social networking in the United States" en *First Monday* (2006).

tecnología en un determinado escenario cambia las normas que gobiernan el flujo informacional, estableciendo qué datos son o no pertinentes en cada contexto para mantener la integridad contextual:

> "Si la introducción de una nueva tecnología o práctica en un determinado contexto se encuentra en conflicto con las normas de flujo de información establecidas, una bandera roja es desplegada, indicando que la integridad contextual ha sido violada" (Zimmer, 2007).

Sin embargo, en los contextos digitales y, más concretamente, en las redes sociales la violación de las normas que regulan el despliegue de información es más factible debido a dos características propias de la red: la capacidad de divulgación ampliada y la mencionada indefinición de los escenarios en los que se dan los intercambios de información. Esta indeterminación choca radicalmente con las bases de la integridad contextual. Desde la perspectiva propuesta por Nissenbaum, en la vida diaria la inserción de datos privados viene determinada por contextos sociales altamente granulados. Por el contrario, en estos espacios públicos mediados esta granularidad no se produce ni es explícita (Hull, Lipford, y Latulipe, 2010: 289), por lo que no es sencillo interpretar qué normas deben usarse en cada escenario. Es más, dado que el cerebro automatiza los contextos y por tanto las normas informacionales que atribuye a cada uno de ellos, si no ha interpretado bien el escenario puede usar normas contraproducentes que dejen su vida privada totalmente descubierta.

Igualmente, como dominio público mediado la Web posee una serie de características que poco tienen que ver con las interacciones en el mundo físico. Para algunos autores, otra de las violaciones serias de las normas de la distribución vendría condicionada, nuevamente, por esa naturaleza hipermediada de las redes sociales, lo que implica la existencia de unos desarrolladores detrás de las aplicaciones que son invisibles para el usuario, oscureciendo el hecho de que la información está abandonando los límites de la red social y no fluyendo sólo a nuestros amigos (Hull, Lipford, y Latulipe, 2010: 295). El ejemplo más llamativo lo encontramos en redes sociales como Facebook, en las que las aplicaciones creadas por terceras empresas violarían la ley de la distribución y, consecuentemente, las normas de propiedad por cuanto ese contexto no justificaría la utilización de los datos recolectados bajo otras condiciones[10]. De este modo rompen el poder de decisión que la teoría de integridad contextual otorga al usuario.

Finalmente, uno de los máximos atractivos de la teoría reside en la adaptabilidad a contextos específicos, partiendo del hecho de que la cantidad y tipo de normas informacionales son siempre internas a un determinado contexto, esto es son relativas y no universales. La cara negativa nos impele a plantearnos qué sucede cuando el usuario no se rige por el mismo marco contextual que el resto de agentes implicados en el intercambio de información, a saber: desarrolladores de aplicaciones, usuarios conocidos e, incluso, usuarios universales e indefinidos a los que ni tan siquiera se conoce.

[10] Hull, Lipford y Latulipe lo denominan "daños colaterales" de las redes sociales. "Contextual gaps: privacy uses in Facebook", en *Ethics and Information Technology* (2010).

4. Conclusiones

Más que una teoría universal sobre la privacidad en público, la integridad contextual actúa dentro de las fronteras normativas de un determinado contexto. Esta peculiaridad solventaría la problemática derivada de la protección de la vida privada concebida por oposición a lo público, así como la dificultad producida por las distintas nociones culturales de intimidad y vida privada. Refuta, asimismo, la idea de que no sólo por el hecho de que los usuarios emplacen información personal en los espacios públicos como la Web 2.0 pueden perder todas las expectaciones de privacidad.

Si bien, aunque serviría para solucionar la problemática búsqueda de una definición global de privacidad adaptada a la totalidad de la red, aun cuando los conceptos culturales de intimidad y vida privada que operan en la red son locales, en su vertiente negativa, añadiría un alto grado de subjetividad. Esto, por extensión, acabaría dificultando la protección de la intimidad y vida privada si el marco normativo que regula un determinado contexto no es claro, explícito, o conocido por todos los agentes de la comunicación. De este modo se abre una puerta a que lo que es considerado intromisiones en la intimidad y vida privada en una cultura o sociedad, no lo sea para otra y que, además, esta variabilidad o arbitrariedad provoque una justificación de la intromisión.

Probablemente, el escenario digital existente en la época en que se enunció por primera vez la integridad contextual hacía prever una cierta convención normativa en cuanto al correcto uso de las primeras aplicaciones masivas, tales como correos electrónicos o foros. No obstante, tras la aparición de las aplicaciones de la Web 2.0 y, concretamente, tras la popularización del uso de las redes sociales, esta convención no parece factible.

Sin embargo, proporciona un interesante punto de partida para el estudio de contextos públicos en los que la información sensible juega un papel importante y, por extensión, incluye la necesidad de discurrir sobre un concepto de protección de la vida privada adaptado, no sólo a las nuevas tecnologías, sino a contextos reales donde la dicotomía espacio público *versus* privado difícilmente se presenta de manera excluyente. No significa, por tanto, que este planteamiento teórico haya fracasado tras la aparición de la Web 2.0, sino que subraya la importancia y necesidad de que los usuarios obtengan información clara sobre la finalidad para la que se emplearán los datos una vez insertados en la Web, así como para identificar contextos y, por tanto, las normas que imperan en cada marco.

En estas condiciones, la aplicación de la integridad contextual puede observarse como un avance hacia la "privacidad de diseño", un nuevo estado en el que cada usuario sea capaz de decidir críticamente qué mostrar y qué ocultar en función de sus propios deseos y necesidades, guiándose por una protección de las propias informaciones más personalizada y adaptada. Esta aplicación enlazaría el uso de la integridad contextual a las ideas defendidas por numerosas investigaciones que vierten su interés en la importancia de la autodeterminación individuo.

Referencias bibliográficas

ALLEN, Anita L. (1988). *Uneasy access: privacy for women in a free society*. New Jersey: Rowman & Littlefield.

BARNES, Susan B. (2006). A privacy paradox: social networking in the United States. En: *First Monday*, vol. 11, nº 9. [http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312] (29 de mayo de 2013)

BÉJAR, Helena (1988). *El ámbito íntimo: privacidad, individualismo y modernidad*. Madrid: Alianza.

BOYD, Danah (2006). Friends, friendsters and myspace top 8: writing community into being on social networks sites. En: *First Monday*, vol. 1, nº 12. [http://www.firstmonday.org/issues/issue11_12/boyd/index.html]. (29 de mayo de 2013)

BOYD, Danah y HARGITTAI, Eszter (2010). Facebook privacy settings: who cares? En: *First Monday*, vol. 15, nº 8, [http: //firstmonday.org/article/view/3086/2589] (10 de junio de 2013)

CURRY, Michael.R. (2002). Discursive displacement and the seminal ambiguity of space and place. En: LIEVROUW, Leah A y LIVINGSTONE, Sonia (eds.) *The Handbook of New Media: Social Shaping and Consequences of ICT*. London: Sage Publications, pp. 502-517.

FRIED, Charles (1968). Privacy. En: *The Yale Journal,* vol. 77, pp. 475-493.

GARCÍA JIMÉNEZ, Leonarda (2008). Las ciencias de comunicación a la luz de las nuevas tecnologías: retos para una disciplina en la incertidumbre. En: *Global Media Journal México,* vol. 5, nº 10, pp.103-118.

GERETY, Tom (1977). Redefining privacy. En: *Harvard Civil Rights-Civil Liberties Law Review,* vol. 12, nº 2, pp. 233-296.

GIOVANNI, Tabreez y PASHLEY, Harriet (2005). Students awareness of the privacy implications when using Facebook. En: *Privacy poster fair at the school of Library and Information Science* [http: //lorrie.cranor.org/courses/fa05/tubzhlp.pdf] (20 de junio de 2013)

GROSS, Ralph y ACQUISITI, Alessandro (2005). Information revelation and privacy in online social networks. En: *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*. Nueva York: ACM Press, pp. 71-80.

HULL, Gordon; LIPFORD, Heather Richter y LLATULIPE, Celine (2010). Contextual gaps: privacy issues on Facebook. En: *Ethics and Information Technology,* vol. 13, nº 4, pp. 289-302.

LAMPE, Cliff; ELLISON, Nicole B. y STEINFIELD, Charles (2008). Changes in use and perception of Facebook. En: *CSCW'08*. San Diego: ACM Press, pp. 721-730.

MILL, John Stuart (1976). *On liberty*. Londres: J.M. Dent & Sons. 1º Edición, 1859.

NISSENBAUM, Helen (2011). A contextual approach to privacy on line. En: *Daedalus,* vol. 140, nº 4, pp. 32-48.

NISSENBAUM, Helen (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

NISSENBAUM, Helen (2004). Privacy as contextual integrity. En: *Washington Law Review,* vol. 79, nº 1, pp. 101-139.

NISSENBAUM, Helen (1998). Protecting privacy in an Information Age: The problem of privacy in public. En: *Law and Philosophy*, vol. 17, nº 5-6, pp. 559-596.
NISSENBAUM, Helen (1997). Toward an approach to privacy in public: the challenges of information technology. En: *Ethics and behaviour,* vol.7, nº3, pp.207-219.
PARENT, William (1983). Privacy morality and the law. En: *Philosophy & Public Affairs* , vol. 12, nº 4, pp. 269-288.
PROSSER, Walter L. (1960). Privacy. En: *California Law Review,* vol. 48, pp. 383-423.
RACHELS, James (1975). Why privacy is important. En: *Philosophy & Public Affairs,* vol. 4, nº 4, pp. 323-333.
SCHOEMAN, Ferdinand (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.
SENNET, Richard (1977). *The fall of public man*. Nueva York: Knopf.
SLOBOGIN, Christopher (2002). Public privacy: camera surveillance of public places and the right to anonymity. En: *Mississippi Law Journal*, nº 72, pp. 213-299.
THOMPSON, John B. (1998). *Los media y la modernidad: una teoría de los medios de comunicación*. Barcelona: Paidós.
TOCQUEVILLE, Alexis de (1981). *De la démocratie en Amérique*. París: Garnier Flammarion.
VAN DEN HOVEN, Jeroen (2001). Privacy and the varieties of informational wrongdoing. En: *Readings in Cyber Ethics,* pp. 430-435.
WACKS, Raymond (1989). *Personal information: Privacy and the law*. New York: Oxford University Press.
WARREN, Samuel y BRANDEIS, Louis (1890). The right to privacy. En: *Harvard Law Review*, vol. 4, nº 5, pp. 193-220. Traducción a cargo de PENDÁS, Benigno y BASELGA, Pilar (1995) *El derecho a la intimidad*. Madrid: Civitas.
ZIMMER, Michael (2007). Privacy and surveillance in Web 2.0: A study in contextual integrity and the emergence of Netaveillance. En: *Society for Social studies of Science*. [http://www.academia.edu/3943172/Privacy_and_Surveillance_in_Web_2.0_A_study_in_Contextual_Integrity_and_the_Emergence_of_Netaveillance] (19 de abril de 2013)
ZIMMER, Michael (2008). Privacy on planet Google: using the theory of contextual integrity to clarify the privacy threats of Google's quest for the perfect search engine. En: *Journal of Business & Technology*, vol. 3, pp.109-132.
ZIMMER, Michael (2005). Surveillance, privacy and the ethics of vehicle safety communication technologies. En: *Ethics and Information Technology*, vol.7, nº 4, pp. 201-221.