BIG SOCIAL DATA: LÍMITES DEL MODELO *NOTICE AND CHOICE* PARA LA PROTECCIÓN DE LA PRIVACIDAD

Big social data: Some limitations of *notice and choice* for privacy protection

Sara Suárez-Gonzalo

Sara Suárez-Gonzalo lleva a cabo su tesis doctoral en el *Departament de Comunicació* de la *Universitat Pompeu Fabra*. Se graduó en Publicidad y Relaciones Públicas por la *Universidade de Vigo* en 2014 y master en *Comunicación Social* por la *Universitat Pompeu Fabra* en 2015. Desde 2014 investiga el impacto del fenómeno *big data* en la privacidad de las personas, especialmente en las redes sociales.
http://orcid.org/0000-0001-6883-1984

Universitat Pompeu Fabra. Departament de Comunicació
Programa de doctorado
Roc Boronat, 138, 08018 Barcelona, España
sarapaz.suarez@upf.edu

Resumen

El fenómeno *big data* supone un desafío a la privacidad de los datos personales (Boyd, 2012). Este artículo es una contribución al debate sobre la validez del paradigma de autogestión de la privacidad reinante en el mundo occidental. Se señalan una serie de limitaciones del modelo en el que se basa dicho paradigma (el modelo *notice and choice*) con respecto a la lógica de procesamiento *big data*. También se analiza el modelo alternativo propuesto por Solove (2013) para explicar por qué no se aleja en lo esencial del modelo *notice and choice*. Por último, se expone la necesidad de construir un modelo cuya fundamendación conceptual sea coherente con la lógica *big data* y su impacto en la privacidad a nivel individual y colectivo.

Palabras clave

Big data; Datos masivos; Autogestión de la privacidad; *Notice and choice*; Libertad; Privacidad colectiva; Protección de datos personales; Ética; Solove; Paradoja de la privacidad; Redes sociales.

Abstract

Big data challenges personal data protection (Boyd, 2012). This paper is a contribution to the debate about the validity of the privacy self-management paradigm prevailing in western countries. I point out some limitations of the model *notice and choice* in which that paradigm is based in relation to the logic of big data processing. I also analyze the alternative model proposed by Solove (2013), to explain why it is not essentially different from *notice and choice* model. Finally, I expound on the necessity of developing a model which could be coherent with the logic of big data and its impact in privacy, both individual and collective.

Keywords

Big data; Privacy self-management; *Notice and choice*; Freedom; Liberty; Collective privacy; Personal data protection; Ethics; Solove; Privacy paradox; Social networks.

Suárez-Gonzalo, Sara (2017). "*Big social data*: límites del modelo *notice and choice* para la protección de la privacidad". *El profesional de la información*, v. 26, n. 2, pp. 283-292.

https://doi.org/10.3145/epi.2017.mar.15

Artículo recibido el 11-11-2016
Aceptación definitiva: 24-01-2017

1. Introducción

La "datificación" de lo cotidiano es una tendencia en alza (**Baruh**; **Popescu**, 2015, p. 3). A finales del siglo XX el volumen, la variedad y la velocidad de generación de datos comenzó a aumentar notablemente (**Laney**, 2001) y surgió el término *big data* (**Cox**; **Ellsworth**, 1997, p. 1). Hoy numerosas actividades del mundo digital y del presencial se registran en datos, que gracias al desarrollo tecnológico pueden recopilarse de forma rápida y barata (**Halavais**, 2015), siendo su usabilidad cada vez mejor (**Minelli**; **Chambers**; **Dhiraj**, 2013). Como consecuencia aumenta el número y la variedad de sectores interesados en los datos masivos (**Chen**; **Zhang**, 2014), al tiempo que crece la preocupación social por la privacidad, un concepto complejo que recogen como derecho fundamental numerosas constituciones (**Solove**, 2008). Sin embargo, varios estudios muestran que a menudo los comportamientos de las personas con respecto a la difusión de su información personal no reflejan esa preocupación (**Durán-Segura**; **Mejías-Peligro**, 2014; **Hargittai**; **Marwik**, 2016; **Hoy**; **Milne**, 2013; **Solove**, 2013; **Taddicken**, 2014; **Utz**; **Kramer**, 2009), dando lugar a la llamada "paradoja de la privacidad" (**Barnes**, 2006). **Barnes** atribuye esta incoherencia a las características personales de los individuos, pero **Turow**, **Hennessy** y **Draper** (2015) sugieren que se trata de una imposibilidad de los individuos para decidir acerca de su privacidad. Más allá de esto, la "paradoja del conocimiento" (**Baruh**; **Popescu**, 2015, p. 9) describe la posición de individuos muy informados y concienciados que, frente a la imposibilidad de proteger sus datos, rechazan la tecnología como una táctica de resistencia. Algunos tienden al *suicidio digital* (**Karppi**, 2011; **Dockray**, 2010).

El fenómeno *big data* supone un problema social para la protección de los datos personales y un desafío para la ordenación jurídica en materia de privacidad (**Jourová**, 2016). En el mundo occidental la legislación sobre privacidad de los datos personales sigue el modelo de la autogestión (*privacy self-managment*), que se basa en la notificación y la elección (*notice and choice*) (**Baruh**; **Popescu**, 2015; **Schwartz**, 2013; **Solove**, 2013). En la práctica, la información proporcionada a los individuos sobre el uso de sus datos es larga y compleja y no se produce una negociación (**Solove**, 2013). En la mayoría de los casos el consentimiento se rige por la máxima "lo tomas o lo dejas" (**Popescu**; **Baruh**, 2013). En el entorno académico emerge un debate sobre la conveniencia y las limitaciones de la autogestión (**Baruh**; **Popescu**, 2015; **Martin**, 2015; **Schwartz**, 2013; **Solove**, 2008; 2013), y este artículo es una contribución al mismo. El objetivo es identificar algunos de los factores que obstaculizan la protección de la privacidad de los datos personales mediante los mecanismos de la notificación y la elección en un mundo tecnológico profundamente interconectado.

2. Privacidad y lógica *big data*

2.1. La difusión de información personal

Los usuarios ceden una gran cantidad de información personal en las redes sociales, cimentando un rastro indisoluble (**Burkell** *et al.*, 2014; **Manovich**, 2012). Como explican **Boyd** y **Crawford** (2011), en ellas los usuarios cambian la forma tradicional de compartir información, y como consecuencia cada vez están más expuestos.

Estos datos masivos (conocidos en inglés como *big social data*, *social media data o social media big data*, **Tufekci**, 2014, **Halavais**, 2015, p. 586) despiertan un gran interés a las empresas y ya están siendo utilizados para incrementar la inteligencia de mercado (**He** *et al.*, 2015), en la predicción y gestión de situaciones de crisis y emergencia (**Castillo**, 2016; **Xiao**; **Huang**; **Wu**, 2015; **Pohl**; **Bouchachia**; **Hellwagner**, 2015), y también para mejorar tratamientos médicos (**Sarker** *et al.*, 2015; **Gouveia-Rodrigues** *et al.*, 2014), entre otras aplicaciones.

En ocasiones la difusión de información personal es consciente, en otras no. Las aplicaciones generan metadatos de forma automática que pueden revelar la localización, el tiempo o características del dispositivo desde el que se genera la información, tanto del individuo principal, como de aquellos con los que éste se comunica (*Privacy International*, s.f.). Asimismo, la información personal que genera y difunde una persona también la difunden otros. Es decir, la difusión de información personal no es sólo personal.

> "La difusión de información personal no es algo personal"

2.2. Procesamiento *big data*

Una característica de la recogida de datos masivos es que es indiscriminada. En los métodos tradicionales antes de recopilar se decide qué datos interesan, pero en la minería *big data* de entrada se obtiene un conjunto completo de información al que posteriormente se aplican filtros (**Baruh**; **Popescu**, 2015) y se cruzan las variables (**Solove**, 2013; **Baruh**; **Popescu**, 2015) con el objetivo de extraer información valiosa no explícita, una información que emerge combinando los datos. Esto permite estudiar fenómenos a gran escala (**Halavais**, 2015), vislumbrar atributos y patrones latentes en los datos (**Boyd**; **Crawford**, 2011) e inferir información que las personas no han difundido de forma explícita (**Tufekci**, 2015). En consecuencia, datos que de forma aislada parecen inocuos, procesados pueden revelar información sensible.

Facebook for business (2014) declara que el propósito del análisis de datos masivos no es vigilar la actividad individual, sino extraer información valiosa del conjunto de las expresiones colectivas. En este sentido, no sólo se recoge información detallada de los hábitos y preferencias de millones de personas (que permitiría vigilarlas individualmente si este fuera el objetivo), sino que sirve para estudiar los patrones de comportamiento y actuación de conjuntos más amplios de la sociedad. En publicidad esto permite adecuar productos y servicios, realizar campañas publicitarias más efectivas o predecir comportamientos o actitudes futuras de los consumidores (**Mayer-Schönberger**; **Cukier**, 2013; **Schroeck** *et al.*, 2012). El éxito de plataformas como *Amazon* o *Netflix* se debe en gran medida al uso de sistemas de recomendación automatizados basados en la similitud entre usuarios (**Capella**; **Yang**; **Lee**, 2015; **Fernández-Manzano**; **Neira**; **Clares-Gavilán**, 2016).

2.3. Automatismo y opacidad

Los procesos *big data* afectan directa o indirectamente a la vida de las personas (**Kroll** *et al.*, 2016), con aplicaciones tan importantes como la negociación de alta frecuencia de los mercados financieros (**Karppi**; **Crawford**, 2016, p. 2) o la persecución del crimen (**Bogomolov** *et al.*, 2014; **DeLorenzi**; **Shane**; **Amendola**, 2006). Hallinan y Striphas definen la cultura algorítmica como el uso de procesos computacionales para ordenar, clasificar y jerarquizar personas, lugares, objetos, y también los hábitos de pensamiento, conducta y expresión que emergen en relación con estos procesos (**Hallinan**; **Striphas**, 2016, p. 119). Al mismo tiempo que se hacen más complejos, explica **Pasquale** (2015), estos sistemas de procesamiento se vuelven cada vez más opacos debido al interés de los grandes poderes corporativos y gubernamentales, al amparo de los sistemas políticos y legales. Pasquale utiliza el término *agnotology* para referirse a la producción estructural de ignorancia, sus diversas causas y conformaciones, tanto si se deben a la negligencia, despiste, miopía, extinción, secretismo o la ocultación (**Pasquale**, 2015, p. 2). Este escenario despierta reclamos de transparencia, responsabilidad y control de los procesos de análisis de datos, a los que se suman muchos expertos por motivos diversos:

- **Capland** y **Boyd** (2016) defienden que los algoritmos están modificando la esfera pública;
- **Boyd**, **Levy** y **Marwik** (2014) señalan sus posibles efectos discriminatorios;
- **Pasquale** (2015) y **Kroll** *et al.* (2016) apuntan que carecen de la objetividad y la neutralidad de la que presumen.

Al mismo tiempo se extiende la convicción de que la mera transparencia no es suficiente para hacer frente a esta situación. Varios autores, entre ellos **Pasquale** (2015) o **Boyd** (2016), defienden que, por sí sola, la transparencia puede conducir simplemente a más complejidad y que, por ello, existe una necesidad de establecer procesos de control y atribución de responsabilidades.

> La violación de la privacidad adquiere una dimensión colectiva

2.4. Violación de la privacidad

La protección de la privacidad de los datos personales en este escenario es, cuanto menos, compleja:

- la difusión de datos personales no es algo personal ni controlable por la persona a la que pertenecen;
- los mecanismos a los que se someten dichos datos no son comprensibles ni transparentes y carecen de responsabilidad directa y de control externo.

Así, la violación de la privacidad puede ser imprevisible, puede producirse a largo término y no sólo se ocasiona a nivel individual, sino que adquiere una dimensión colectiva y afecta al conjunto de la sociedad.

3. Autogestión de la privacidad en el mundo occidental

Las leyes de protección de la privacidad de datos personales en el mundo occidental son similares (**Metcalf**; **Crawford**, 2016): comparten el paradigma de autogestión de la privacidad (**Schwartz**, 2013), que se basa en el modelo *notice and choice* (**Solove**, 2013; **Baruh**; **Popescu**, 2015).

Seguidamente se explican algunas características principales de la legislación europea y la estadounidense en la materia con el fin de mostrar que comparten unas características esenciales e ilustrar la plasmación jurídica del modelo *notice and choice*. Es importante destacar que el presente artículo se centra en este modelo como el ente abstracto que reúne las características esenciales del paradigma de protección de la privacidad de datos personales predominante en el mundo occidental.

Las leyes de protección de datos personales de Europa y Estados Unidos tienen su origen en las *Fair information practices* de 1973, una serie de principios básicos compartidos entre Estados Unidos y Europa occidental para las organizaciones del sector público y privado que procesaran información personal (**Schwartz**, 2013; **Solove**, 2013). Como indica **Schwartz** (2013), existen diferencias entre los reglamentos europeo y estadounidense que se han acentuado con la entrada en vigor en abril de 2016 del *Reglamento 2016/679 del Parlamento Europeo y del Consejo* (*Unión Europea*, 2016), más rígido en la protección de datos personales con respecto a la ya derogada *Directiva* de 1995 (*Unión Europea*, 1995). **Jourová** (2016) señala que esta reforma del *Reglamento* se centra en tres aspectos principales:

- resguardar el derecho fundamental a la protección de datos independientemente de cómo se desenvuelvan en el futuro la tecnología y el entorno digital;
- aumentar la confianza en el entorno digital;
- incrementar la actividad económica.

Como diferencias principales, la legislación europea establece reglas generales y unificadas para todos los estados miembros de la Unión. A mayores, una legislación sectorial se encarga de especificar las normas para casos concretos. Por el contrario la estadounidense es sectorial y establece diferentes estatutos para el ámbito público y el privado (**Schwartz**, 2013, p. 1974).

La regulación europea establece unos límites más estrictos que la estadounidense para la recopilación y el uso de datos, da protección adicional a aquellos de carácter sensible y defiende más derechos de los individuos. Asimismo, da más importancia a la notificación mediante un principio de transparencia que obliga al responsable del tratamiento de los datos a proporcionar información al afectado de que se están recogiendo, consultando o tratando datos que le conciernen, de una manera fácilmente accesible y con un lenguaje claro y sencillo. Se considera que el consentimiento es informado si el individuo conoce al menos la identidad del responsable del tratamiento de los datos y los fines para los que se recogen dichos datos. Esta regulación establece

medidas de control del consentimiento, interviene el flujo transfronterizo de datos e instaura agencias nacionales de control interno. Por su parte, la legislación estadounidense concede más importancia al consentimiento de las partes afectadas y menos a la notificación. En su caso, la *Federal Trade Commission* es el órgano más similar a una agencia nacional de control (**Schwartz**, 2013).

3.1. *Notice and choice*: condiciones básicas

Las diferencias fundamentales entre la regulación europea y la estadounidense se concentran en la forma de implementación de las normativas y en la centralidad de la notificación o el consentimiento. El reglamento europeo es más estricto con la notificación y el consentimiento y es más garantista que el estadounidense. En todo caso, su esencia es compartida: la notificación y la elección son las condiciones básicas para el funcionamiento del modelo *notice and choice* y la decisión individual la manera de proteger la privacidad.

Debido a que la regulación europea es la más exigente, se exponen como ejemplo los criterios que se extraen de su lectura al respecto de la notificación y el consentimiento:

- el consentimiento debe ser libre, informado, específico para cada caso concreto y revocable y debe reflejarse en un acto afirmativo claro e inequívoco;
- la notificación sirve de base para que el afectado dé su consentimiento de manera informada y por lo tanto debe ser previa a la recopilación o tratamiento de los datos, y cumplir las condiciones de ser adecuada e inequívoca.

> La legislación occidental en materia de datos personales sigue el paradigma de la autogestión

4. Crítica al modelo *notice and choice*

4.1. Limitaciones: lógica *big data*

Se extrae de lo anteriormente expuesto que para el funcionamiento del modelo *notice and choice* es esencial determinar de forma clara qué es un dato personal o qué datos pueden revelar información personal. Es necesario, al menos, para determinar:

- a qué individuos se proporciona la información y el derecho a consentir;
- cuándo puede surgir un problema de privacidad o un conflicto de intereses derivado del tratamiento de datos;
- sobre qué cuestiones se debe informar y consentir.

Sin embargo, lo argumentado en el apartado **2.2. Procesamiento *big data*** se traduce en una dificultad para determinar qué constituye un dato personal hoy en día, lo cual dificulta el cumplimiento de los criterios de funcionamiento del modelo *notice and choice*. En base al ejemplo europeo: la información al individuo difícilmente puede ser inequívoca y adecuada, si se proporciona previamente a la recopilación y al tratamiento de los datos. Por consiguiente difícilmente podríamos considerar que el consentimiento sea informado y que se pueda proporcionar o revocar de forma específica para cada caso.

En este artículo se considera que el cumplimiento de dichos criterios pasaría por:

- definir con claridad qué es un dato personal;
- proporcionar información completa y adecuada al individuo;
- permitir la decisión informada y significativa acerca de cualquier aspecto relativo a todas las posibles formas de tratamiento de dichos datos, en cualquier fase del proceso.

> La lógica *big data* supone una dificultad para determinar qué es un dato personal

Para que la decisión sea informada el individuo debería tener conocimiento, al menos, sobre las siguientes cuestiones:

- qué datos de los recogidos pueden concernirle, independientemente de quién los haya difundido, de cómo se hayan generado y de cómo serán procesados;
- cuáles son los objetivos, el diseño y el funcionamiento del sistema de análisis;
- qué información sensible puede revelar el conjunto de los datos analizados en cada una de las fases de análisis y, por lo tanto, de forma prolongada en el tiempo.

El cumplimiento de estos criterios complicaría en gran medida el proceso y supondría un esfuerzo desproporcionado para el individuo, no sólo por el tiempo de dedicación que requeriría, sino también por los conocimientos específicos necesarios para comprender información compleja. La información debe ser un derecho del individuo, y no una obligación para proteger los datos personales. A esto se suma la ineludible barrera que supone la intencionada opacidad de los sistemas de procesamiento de datos.

Teniendo en cuenta las limitaciones señaladas para que el consentimiento individual sea efectivamente informado y por lo tanto específico y revocable, queda por considerar el cumplimiento de un último criterio: ¿es libre?

4.2. Limitaciones: fundamentación conceptual

Para el modelo *notice and choice* "libre" equivale a "voluntario". El consentimiento se considera libre siempre que no exista una interferencia externa que afecte de forma directa a la voluntad del individuo de dar su consentimiento. Por este motivo, autores como **Richardson** (2016) han señalado que los regímenes legales occidentales de protección de datos se fundamentan en el canon tradicional de la privacidad. Éste se construye en base al ideal liberal de la libertad, como no-interferencia: para que una decisión sea libre es necesario y suficiente que no exista una interferencia en el propio curso de acción (**Berlin**, 1988, p. 196; **Hobbes**, 2011, p. 187).

Bobbio (2009, p. 98) explica dicha interferencia en términos de prohibición u obligación: la libertad consiste en la ausencia de prohibición (obligar a no hacer algo), y en la ausencia de obligación (obligar a hacer algo).

El liberalismo entiende por interferencia únicamente la intervención directa en la voluntad del individuo (**Pettit**, 2004). En el caso español esto se ve de forma clara en la *Guía para el ciudadano* que explica que el consentimiento

del individuo, recogido por la *Ley orgánica 15/1999* (*España*, 1999), debe ser libre: "salvo que la ley lo disponga no podemos ser obligados a facilitar nuestros datos" (*Agencia Española de Protección de Datos*, 2011, p. 10).

Varios autores han notado que la concepción liberal de libertad se construye sobre una idea individualista de la sociedad, que se comprende y se analiza como una suma de individuos aislados, atomizados (**Bertomeu**; **Domènech**, 2005). El liberalismo entiende, con todo, que la vida en común hace obligada la imposición de ciertas barreras a dicha libertad, a fin de garantizar que la de uno no se inmiscuya en la de otro hasta el punto de dañarla, y así, asegurar otros valores como la seguridad o la propiedad (**Mill** en **Berlin**, 1988, p. 197). Esto ayuda a comprender por qué el modelo *notice and choice* asume que garantizar la libre gestión de la privacidad pasa, justamente, por dejar que cada uno la gestione individualmente. O lo que es lo mismo: por cargar el peso de la protección de la privacidad sobre los individuos y sus decisiones. Del mismo modo se explica por qué esta norma se rompe en aquellos casos justificados por razones de orden público, como la persecución del terrorismo.

> Los fundamentos conceptuales del paradigma actual están desvinculados de la lógica y los objetivos del procesamiento de datos masivos

Desde esta perspectiva individualista, la privacidad se entiende como un espacio donde poder disfrutar de lo propio sin ser interferido (**Richardson**, 2016). Lo privado se ha identificado tradicionalmente con lo oculto, lo secreto, aquello que el individuo desea preservar del conocimiento y la acción de los demás (**Solove**, 2008). Por ello se prohíbe el acceso y la utilización de los datos personales del individuo, excepto en caso de que éste lo consienta, o de que sea él mismo quien los revele en un espacio público. Una cuestión importante, que no se abordará aquí pero que cabe apuntar, es si las redes sociales deben o no ser consideradas espacios públicos.

4.3. Choque de perspectivas

Mientras la lógica de procesamiento *big data* aprovecha el carácter interconectado de los datos y de las personas a las que pertenecen (**Boyd**, 2012) –a fin de extraer la mayor cantidad de información posible, el modelo de protección de datos personales se construye en base a una visión individualista de la sociedad, y se focaliza en los datos como entes aislados. Esta desvinculación entre las dos perspectivas pone de manifiesto una debilidad de la fundamentación conceptual del modelo *notice and choice* para comprender y abordar las vulneraciones provocadas por el uso de datos masivos.

El problema para gestionar la privacidad surge de:

- la lógica de generación y procesamiento de los datos masivos;
- un desacoplamiento entre dicha lógica y aquella de la que parte el modelo de protección de datos personales.

En la medida en que el problema afecta al conjunto de la sociedad, y cuyo control trasciende al conocimiento, las capacidades y las habilidades de cada individuo, se considera aquí un problema de tipo estructural. Atendiendo a los criterios del modelo *notice and choice*, pese a las limitaciones que supone este problema estructural para el buen funcionamiento del paradigma de autogestión, la decisión individual se seguiría considerando libre. Desde la perspectiva del presente artículo se considera que, si bien estas limitaciones no suponen una forma de interferencia directa sobre la voluntad de los individuos, sí representan otra forma de interferencia que merma la posibilidad de los individuos para gestionar sus datos personales y para hacer frente al impacto de su procesamiento. Por consiguiente se entiende que, en estas circunstancias, el consentimiento no es libre.

Como se ha dicho antes, ésta es una crítica al modelo *notice and choice* y no necesariamente a todas las formas de su plasmación jurídica. No obstante, cabe matizar que el *Reglamento* europeo recoge una idea matizada de la libertad aquí descrita, pese a que sigue remitiendo a ella (véanse las consideraciones 42 y 43 del *Reglamento*).

5. Crítica al *modelo mixto*

Una propuesta alternativa al modelo *notice and choice* es la del profesor **Solove** (2013), a la que aquí nos referimos como *modelo mixto*. Su planteamiento parte de una crítica al modelo *notice and choice* y se explica brevemente a continuación con el fin de demostrar que no se aleja en lo esencial del modelo criticado.

5.1. Puntos de divergencia

Existen tres cuestiones principales por las que, desde la perspectiva del presente artículo, el *modelo mixto* no parece adecuado:

La privacidad como valor contextual

La principal crítica de Solove al modelo *notice and choice* parte de su concepción de la privacidad. Para **Solove** (2008) la privacidad no debe conceptualizarse mediante la identificación de elementos esenciales o constitutivos de lo que ésta representa. **Solove** (2013) la entiende como un valor contextual que sólo puede conceptualizarse en relación con los daños que provoca su vulneración. Estos daños, explica, sólo pueden ser valorados en cada caso particular, es decir, en relación con el fin para el que sirva la vulneración de aquello que se considera privado. Siguiendo esta línea, Solove argumenta que el daño provocado por la vulneración de lo privado puede verse compensado en relación con otros posibles beneficios a nivel individual o social.

Esta tesis se inscribe en una forma de relativismo moral, que entiende que no es posible determinar de forma abstracta un ideal de lo que es una buena o una mala gestión de la privacidad, sino que es algo que corresponde decidir únicamente a cada individuo. Cualquier interferencia externa en esta decisión individual puede ir en contra de los intereses particulares y de la voluntad del individuo y, por lo tanto, limita la libertad y la autonomía de las personas. En consecuencia Solove considera que la gestión de la privacidad debe ser individual. Así, el *modelo mixto* conserva la premi-

sa fundamental del modelo criticado: comprende la libertad como no-interferencia, y defiende la autogestión de la privacidad como la manera de garantizar que la decisión acerca de la privacidad sea libre.

Por otra parte, el fin para el que se recojan o traten los datos (ya sea en aras del beneficio individual o colectivo, público o privado) es importante, pero no suficiente para guiar los procesos de recopilación y tratamiento de datos, ni los mecanismos de autogestión de la privacidad de datos personales. La privacidad no debe ser un mero valor contextual, ni entrar en un juego de preferencias como moneda de cambio. Debe existir algún criterio común para determinar lo que es una buena o una mala gestión de la privacidad. Las diferencias culturales deben ser tenidas en cuenta a la hora de determinar dicho criterio, comprender en qué consiste la privacidad y articular los mecanismos necesarios para protegerla.

> Determinar para qué fines es lícito tratar datos masivos y para cuáles no, es importante, pero aún lo es más asegurar que los procesos sean justos, responsables y permitan a los ciudadanos el control sobre su información

Problemas cognitivos y estructurales

Solove identifica una serie de problemas cognitivos, relativos a la falta de habilidad de los individuos para tomar decisiones racionales e informadas. Señala que los individuos, además de estar desinformados, tienen una racionalidad limitada.

Por otra parte encuentra varios problemas estructurales:

- un problema de escala, referido a un número demasiado elevado de entidades que recopilan y utilizan datos, para que los individuos puedan gestionar toda la información que les proporcionan;
- un problema de agregación, que puede provocar usos derivados de los datos;
- un problema relativo a la complejidad para sopesar los daños provocados por la violación de la privacidad.

Este último lo presenta referido a tres cuestiones:

- muchos problemas de privacidad se producen a largo término o aparecen debido al uso derivado de los datos;
- los daños a la privacidad son a menudo pequeños y dispersos, pero unidos pueden ser perjudiciales y tener un impacto para los demás,
- el paradigma actual sólo da importancia a los daños ocasionados por usos no-consensuados de los datos (**Solove**, 2013).

Solove focaliza su análisis en la dificultad de los individuos para sopesar los costes y beneficios de la cesión de datos. Argumenta que es esta dificultad la que provoca que su decisión no sea significativa. Los problemas que Solove define como cognitivos, no son una cuestión diferente de aquellos estructurales, sino una consecuencia de ellos, que merman la capacidad de las personas para gestionar su privacidad.

En segundo lugar, una crítica a la falta de racionalidad humana no puede ser considerada una cuestión que afecte de forma especial al funcionamiento del modelo *notice and choice* en particular, sino una forma particular de comprender al ser humano.

Y por otra parte, toda ley presupone, en mayor o menor medida, una capacidad humana para decidir racionalmente, y no parece adecuado construir un paradigma legal basado en la capacidad racional de los individuos para sopesar los costes y los beneficios de unas acciones sobre las que no tienen control.

En el presente artículo se considera que las personas sí tienen una capacidad para decidir racionalmente, y que, en todo caso, el problema de protección de la privacidad no se debe a una falta de capacidades individuales, sino a una imposibilidad para actuar mediante los mecanismos disponibles.

El paternalismo libertario

Muchos, explica Solove, consideran que la solución a esta falta de capacidad de los individuos para decidir significativamente, de la que él habla, pasa por vías paternalistas, es decir, por la actuación ajena a la voluntad individual. Solove comprende que el paternalismo supone una interferencia directa en la voluntad del individuo y por lo tanto lo considera algo profundamente negativo. De aquí surge su "Dilema del consentimiento" (**Solove**, 2013, p. 1894). Su solución al dilema se recoge en lo que él llama el "paternalismo libertario": combinar la decisión individual con una serie de ayudas al afectado para decisiones complejas, y proporcionar un conjunto de normas básicas para cuestiones extremas, dirigida aquellos que utilicen los datos. Ambas vendrían determinadas de forma externa a la voluntad de los individuos. Además, propone que el modelo debería admitir la decisión selectiva en base a casos y el seguimiento continuado del uso de los datos, con la posible ayuda de una agencia gestora.

Tras analizar el *modelo mixto*, se extrae que la crítica a la falta de racionalidad de los individuos es, precisamente, lo que hace a Solove ver la necesidad de una solución paternalista. Si se entiende que la falta de capacidades de los individuos es una consecuencia de los problemas estructurales, el paternalismo no es necesario. Lo necesario es solventar dichos problemas. En este sentido parece anterior la necesidad de asegurar que los mecanismos de protección (la notificación y el consentimiento individual) sean adecuados en relación a aquello que se debe gestionar (los datos personales) y a cómo se debe gestionar (teniendo en cuenta la lógica *big data*). Si no es así, el individuo podría verse obligado a decidir bajo una falta de capacidades y de recursos, y en un sentido que no responda necesariamente a sus propias convicciones ni a sus intereses.

5.2. Una cuestión esencial

El mayor punto de divergencia del presente artículo con el *modelo mixto* es que en él no se abordan los problemas estructurales como la causa de la falta de capacidades de los individuos y que, al igual que en el modelo *notice and choice*, no se comprende que éstos suponen una barrera para la decisión libre.

Como resultado, se entiende que el modelo no sólo falla en la misma cuestión fundamental que el modelo *notice and choice* –comprender la libertad desde una perspectiva limitada-, sino que es todavía más inadecuado en su conceptualización de la privacidad (como un valor contextual relativo a daños) y en su propuesta de solución al problema (el "paternalismo libertario").

> La privacidad no debe ser un mero valor contextual, ni entrar en un juego de preferencias como moneda de cambio

6. Libertad para la privacidad

Hemos argumentado que el modelo *notice and choice* y el *modelo mixto* son insuficientes, y sus planteamientos inadecuados, para dar respuesta a la causa y al impacto de los problemas de privacidad derivados del fenómeno *big data*. Por ello parece necesario revisarlos. Desde el presente artículo se aduce que esto pasa por modificar el ideal de libertad individual que fundamenta el modelo de gestión de la privacidad de datos personales, al haber sido identificado como el principal problema de base en los dos modelos analizados. Entendemos que esto permitiría operativizar una concepción más amplia del valor de la privacidad como un valor integrador de la estructura social, que estaría en grado de generar mecanismos más adecuados.

6.1. Una concepción alternativa de libertad

El liberalismo, explica García-Manrique, ha defendido históricamente que "una cosa es ser libre de X y otra ser capaz de X" (**García-Manrique**, 2013, p. 155). Él, por el contrario, presenta la capacidad como una cuestión no separable de la libertad. Entiende la libertad como la capacidad del individuo para ejercer su autonomía, es decir, para elegir un plan de vida valioso y vivir de acuerdo con él (**García-Manrique**, 2013, p. 155). Esta idea de libertad responde a la concepción republicana y tiene como uno de sus máximos exponentes a Pettit, que concibe la libertad como no-dominación (**Pettit**, 1999, p. 77). La perspectiva republicana representa una alternativa al ideal liberal de la no-interferencia, que como se ha argumentado, recogen los modelos analizados en este artículo.

La concepción liberal entiende por interferencia únicamente un tipo de intervención directa en la voluntad del individuo para decidir su curso de acción (**Pettit**, 2004, p. 120).

La republicana reconoce tanto las interferencias directas como las indirectas y plantea que es imprescindible distinguir entre aquellas no-arbitrarias o legítimas y aquellas arbitrarias o ilegítimas (**Pettit**, 2004, p. 199). Determinar qué interferencias son legítimas es sin duda algo complejo, que presupone una cierta idea de lo que es una vida humana buena. No se profundizará en esta cuestión. Lo que aquí interesa destacar es, simplemente, que ésta atribución de legitimidad a las interferencias es justamente lo que hace a la concepción republicana más precisa que la liberal: mientras la visión liberal considera que las interferencias que van en contra de la libertad son aquellas que interfieren de forma directa en el curso de acción del individuo, la republicana entiende que las interferencias que van en contra de la libertad son aquellas arbitrarias, o no justificadas (sean directas o indirectas). Al contemplar estas interferencias indirectas la concepción republicana reconoce la posibilidad de que un sujeto merme la capacidad de otro para actuar, sin interferir de forma directa en sus acciones. Éste es otro punto diferencial de la concepción republicana que, mediante este reconocimiento, recoge la importancia del elemento de poder (y por consiguiente, de la desigualdad de poder) en la libertad. En este sentido, asume la necesidad de distribuir una serie de recursos fundamentales, que satisfagan ciertas necesidades básicas, y proporcionen a todos por igual la capacidad para ejercer la libertad.

7. Conclusiones

La manera de relacionarse y compartir información con los demás ha cambiado. Vivimos en un ecosistema de datos sociales masivos. La cantidad de información personal que existe se dispara, pero su generación y difusión no son algo exclusivamente personal, ni controlable por el individuo al que pertenece. Las técnicas y los métodos de recogida y procesamiento *big data* evolucionan con rapidez. Los objetivos del tratamiento de datos se centran en encontrar relaciones a gran escala, vislumbrar atributos y patrones latentes en los datos e inferir información que no ha sido proporcionada de forma explícita. Así, la analítica de datos masivos impide determinar de forma aislada y previa a dicho tratamiento qué datos deben ser considerados personales. Hoy, la privacidad de nuestros datos está interconectada. Su violación puede ser imprevisible y adquiere una dimensión colectiva. Preservar la privacidad en este escenario es complicado, es algo que trasciende las capacidades y los conocimientos de los individuos. Al mismo tiempo la complejidad y la opacidad intencionada de los sistemas de procesamiento de datos masivos aumentan la desigualdad de poder de los individuos frente a los grandes poderes corporativos y gubernamentales que se benefician de los datos.

> Los comportamientos de las personas con respecto a la difusión de su información personal no se corresponden con su preocupación por la privacidad

Paradójicamente, el paradigma de autogestión de la privacidad reinante en el mundo occidental carga al individuo el peso de proteger su privacidad, con la intención de asegurar que dicha gestión sea libre. Las limitaciones estructurales expuestas a lo largo de este artículo no representan una interferencia directa en la voluntad de los individuos, no les obligan a consentir o les prohíben desaprobar el uso de sus datos. Por ello, el ideal liberal que fundamenta el paradigma de la autogestión no las contempla como una barrera para la protección ni la libre gestión de la privacidad. El *modelo mixto* propuesto por Solove como alternativa al modelo *notice and choice* falla en esta misma cuestión fundamental.

El incremento de la cantidad de datos abre un gran abanico de oportunidades para el desarrollo social y es importante estudiar cuáles son y cómo se pueden explotar, pero ello requiere de una profunda reflexión sobre el valor de la privacidad en nuestros días y sobre la libertad de los individuos para preservarla. La privacidad es un derecho fundamental que debe garantizarse. Es un valor importante para el desarrollo justo y democrático de la sociedad y no sería beneficioso que se convierta en una moneda de cambio.

Sorprende que los ciudadanos continúen cediendo su información personal, aparentemente de forma despreocupada, pese a que su preocupación por la privacidad es creciente. Sin embargo, la falta de recursos y herramientas disponibles, la falta de transparencia, de control y de responsabilidad sobre de los procesos a los que se someten los datos y, en definitiva, la desigualdad de poder a la que se enfrentan los ciudadanos, podrían estar provocando que éstos se vean forzados a decidir en un sentido que no responda necesariamente a sus propias convicciones ni a sus intereses. Éstas son algunas de las cuestiones que necesitan respuesta si queremos acercarnos a una verdadera solución al problema.

> Es necesario asegurar la libertad de las personas para proteger su privacidad y, para ello, fomentar que todas tengan la capacidad y los recursos necesarios

Es necesario repensar los fundamentos conceptuales del paradigma actual, que están desvinculados de la lógica y los objetivos del procesamiento de datos masivos. Los mecanismos de protección de la privacidad deben abordar el impacto del uso de datos masivos, tanto en el nivel individual de la privacidad, como en el colectivo. Asimismo, los individuos deben tener libertad para proteger su privacidad y por ello se debe asegurar que todos tengan la capacidad de hacerlo. Pensar en los aspectos comunes que requieren el resguardo de la privacidad es posible y podría ser un buen punto de partida, entre otras cosas, para determinar qué capacidades se deben fomentar entre la ciudadanía, qué barreras se deben imponer, qué recursos se deben asegurar y qué mecanismos de actuación se deben proporcionar.

A fin de disipar posibles confusiones, lo que aquí se defiende no es el paso de una concepción individualista, que no reconoce el problema estructural que afecta a la protección de la privacidad, a su opuesto colectivista, donde el individuo y su decisión no tengan cabida. Este artículo es una defensa de la libertad para tomar decisiones valiosas para la propia vida, mediante los propios recursos y capacidades. Es una defensa de la libertad individual para proteger la privacidad de los datos personales (de todos) en la era de los *big data*.

8. Bibliografía

Agencia Española de Protección de Datos (2011). *El derecho fundamental a la protección de datos: Guía para el ciudadano.* *https://goo.gl/8IvsGx*

Barnes, Susan B. (2006). "A privacy paradox: Social networking in the United States". *First Monday*, v. 11, n. 9, pp. 1-10. *https://goo.gl/PBn0vx*

Baruh, Lemi; **Popescu, Mihaela** (2015). "Big data analytics and the limits of privacy self-management". *New media & society*, pp. 1-18. *https://doi.org/10.1177/1461444815614001*

Berlin, Isaiah (1988). "Dos conceptos de libertad". En: Berlin, Isaiah. *Cuatro ensayos sobre la libertad*. Madrid: Alianza Editorial. *http://terras.edu.ar/biblioteca/10/10FP_Berlin_Unidad_3.pdf*

Bertomeu, María-Julia; **Domènech, Antoni** (2005). "El republicanismo y la crisis del rawlsismo metodológico (Nota sobre método y sustancia normativa en el debate republicano)". *Isegoría*, n. 33, pp. 51-75. *https://goo.gl/yHd7JC*

Bobbio, Norberto (2009). *Igualdad y libertad.* Barcelona: Ediciones Paidós Ibérica SA. ISBN: 978 8475098623

Bogomolov, Andrei; **Lepri, Bruno**; **Staiano, Jacopo**; **Oliver, Nuria**; **Pianesi, Fabio**; **Pentland, Alex** (2014). "Once upon a crime: Towards crime prediction from demographics and mobile data". En: *Procs of the 16th intl conf on multimodal interaction*. *https://arxiv.org/pdf/1409.2983.pdf*

Boyd, Danah (2012). "Networked privacy". *Surveillance & society*, v. 10, n. 3/4, pp. 348-350. *http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/networked/networked*

Boyd, Danah (2016). "Transparency ≠ Accountability". *Points: Experimental collection from data & society*, 29 Nov. *https://points.datasociety.net/transparency-accountability-3c04e4804504#.fsmuihtp6*

Boyd, Danah; **Crawford, Kate** (2011). "Six provocations for big data". En: *A decade in internet time: Symposium on the dynamics of the internet and society*, Oxford Internet Institute. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431*

Boyd, Danah; **Levy, Karen**; **Marwik, Alice** (2014). *The networked nature of algorithmic discrimination*. Open Technology Institute; New América; Data & Discrimination. *http://www.danah.org/papers/2014/DataDiscrimination.pdf*

Burkell, Jacquelyn; **Fortier, Alexandre**; **Yeung-Cheryl-Wong, Lorraine**; **Simpson, Jennifer-Lynn** (2014). "Facebook: Public space, or private space?". *Information, communication & society*, v. 17, n. 8, pp. 974-985. *https://www.researchgate.net/publication/278401946_Facebook_Public_space_or_private_space* *https://doi.org/10.1080/1369118X.2013.870591*

Capella, Joseph N.; **Yang, Sijia**; **Lee, Sungkyoung** (2015). "Constructing recommendation systems for effective health messages using content, collaborative, and hybrid algorithms". *Annals of the American Academy of Political and Social Science*, v. 659, n. 1, pp. 290-306. *https://doi.org/10.1177/0002716215570573*

Caplan, Robyn; **Boyd, Danah** (2016). "Who controls the

public sphere in an era of algorithms? Mediation, automation, power". *Data & society*, February 26.
https://datasociety.net/events/who-controls-public-sphere

Castillo, Carlos (2016). *Big crisis data*. Cambridge University Press. ISBN: 978 1107135765

Chen, C. L. Philip; **Zhang, Chun-Yang** (2014). "Data-intensive applications, challenges, techniques and technologies: A survey on big data". *Information sciences*, v. 275, pp. 314-347.
https://goo.gl/ilnlQu
https://doi.org/10.1016/j.ins.2014.01.015

Cox, Michael; **Ellsworth, David** (1997). *Application controlled demand paging for out-of-core visualization*. Report NAS-97-010, July 1997. Moffet Field: NASA Ames Research Centre.
https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf

DeLorenzi, Daniel; **Shane, Jon M.**; **Amendola, Karen-L.** (2006). "The CompStat process: Managing performance on the pathway to leadership". *The police chief. The professional voice of law enforcement*, v. 73, n. 9.
http://www.nashville.gov/Portals/0/SiteContent/Finance/docs/OMB/Strategic%20Management/CompStat.pdf

Dockray, Sean (2010). The *Facebook* suicide bomb manifesto, *Wired*.
https://www.wired.com/2010/05/the-facebook-suicide-bomb-manifesto

Durán-Segura, Mercedes; **Mejías-Peligro, Juan-Francisco** (2014). "Conocimientos y comportamientos de los usuarios de la red social *Facebook* relacionados con la privacidad". Ámbitos. Revista internacional de comunicación. *Infoxicación*, n. 26.
http://institucional.us.es/ambitos/?p=1198

España (1999). "Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal". *BOE*, n. 298, 14 de diciembre.
https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Facebook for business (2014). "Learn more about the people that matter to your business with Facebook audience insights". *Facebook for business*, 8 May.
https://www.facebook.com/business/news/audience-insights

Fernández-Manzano, Eva-Patricia; **Neira, Elena**; **Clares-Gavilán, Judith** (2016). "Data management in audiovisual business: *Netflix* as a case study". *El profesional de la información*, v. 25, n. 4, pp. 568-576.
https://doi.org/10.3145/epi.2016.jul.06

García-Manrique, Ricardo (2013). *La libertad de todos. Una defensa de los derechos sociales*. Barcelona: El viejo topo. ISBN: 978 8415216513

Gouveia-Rodrigues, Ramón; **Marques-das-Dores, Rafael**; **Camilo-Junior, Celso G.**; **Couto-Rosa, Thierson** (2014). "SentiHealth-cancer: A sentiment analysis tool to help detecting mood of patients in online social networks". *International journal of medical informatics*, v. 85, n. 1, pp. 80-95.
https://doi.org/10.1016/j.ijmedinf.2015.09.007

Halavais, Alexander (2015). "Bigger sociological imaginations: Framing big social data theory and methods". *Information, communication & society*, v. 18, n. 5, pp. 583-594,
https://doi.org/10.1080/1369118X.2015.1008543

Hallinan, Blake; **Striphas, Ted** (2016). "Recommended for you: The Netflix Prize and the production of algorithmic culture". *New media & society*, v. 18, n. 1, pp. 117-137.
https://doi.org/10.1177/1461444814538646

Hargittai, Eszter; **Marwik, Alice** (2016). "What can I really do?" Explaining the privacy paradox with online apathy". *International journal of communication*, v. 10, pp. 3737-3757.
http://ijoc.org/index.php/ijoc/article/view/4655

He, Wu; **Shen, Jiancheng**; **Tian, Xin**; **Li, Yaohang**; **Akula, Vasudeva**; **Yan, Gongjun**; **Tao, Ran** (2015). "Gaining competitive intelligence from social media data. Evidence from two largest retail chains in the world". *Industrial management & data systems*, v. 115, n. 9, pp. 1622-1636.
https://doi.org/10.1108/IMDS0320150098

Hobbes, Thomas (2011). *Leviatán o la materia, forma y poder de un estado eclesiástico y civil*. Madrid: Alianza Editorial. ISBN: 978 8420682808

Hoy, Mariea-Grubbs; **Milne, George** (2013). "Gender differences in privacy-related measures for young adult Facebook users". *Journal of interactive advertising*, v. 10, n. 2, pp. 28-45.
https://goo.gl/OHn7Gl
https://doi.org/10.1080/15252019.2010.10722168

Jourová, Vêra (2016). "How will the EU's reform adapt data protection rules to new technological developments?". *European Commission, Justice and Costumers*.
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404

Karppi, Tero (2011). "Digital suicide and the biopolitics of leaving *Facebook*". *Transformations. Journal of media and culture*, n. 20, pp. 1-18.
http://www.transformationsjournal.org/issues/20/article_02.shtml

Karppi, Tero; **Crawford, Kate** (2016). "Social media, financial algorithms and the hack crash". *Theory, culture & society*, v. 33, n. 1, pp. 73-92.
https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2602857
https://doi.org/10.1177/0263276415583139

Kroll, Joshua A.; **Huey, Joanna**; **Barocas, Solon**; **Felten, Edward W.**; **Reidenberg, Joel R.**; **Robinson, David G.**; **Yu, Harlan** (2016). "Accountable algorithms". *University of Pennsylvania law review*, v. 165.
https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2765268

Laney, Doug (2001). "3D data management: Controlling data, volume, velocity and variety". *Application delivery strategies*. Meta Group Inc., Stamford.
https://goo.gl/CBdMXf

Manovich, Lev (2012). "Trending: the promises and the challenges of big social data". En: Gold, Matthew K. *Debates in the digital humanities*. Arizona: University of Minnesota

Press, pp. 460-475.
http://dhdebates.gc.cuny.edu/debates/text/15

Martin, Kirsten (2015). "Understanding privacy online: Development of a social contract approach to privacy". *Journal of business ethics*, v. 137, n. 3, pp. 551-569.
https://doi.org/10.1007%2Fs10551-015-2565-9

Mayer-Schönberger, Victor; **Cukier, Kenneth** (2013). *Big data. A revolution that will transform how we live, work and think*. Londres: John Murray. ISBN: 978 1848547926

Metcalf, Jacob; **Crawford, Kate** (2016). "Where are human subjects in big data research? The emerging ethics divide". *Big data and society*.
https://doi.org/10.1177/2053951716650211

Minelli, Michael; **Chambers, Michele**; **Dhiraj, Ambiga** (2013). *Big data, big analytics*: *Emerging business intelligence and analytic trends for today's businesses.* John Wiley & Sons. ISBN: 978 1118562260
https://doi.org/10.1002/9781118562260

Pasquale, Frank (2015). *The black box society. The secret algorithms that control money and information*. London: Harvard University Press. ISBN: 978 0674368279

Pettit, Philip (1999). *Republicanismo. Una teoría sobre la libertad y el gobierno*. Barcelona: Paidós. ISBN: 978 8449306891

Pettit, Philip (2004). "Liberalismo y republicanismo". En: Ovejero, Félix; Gargarella, Roberto; Martí, José-Luis (eds.). *Nuevas ideas republicanas: autogobierno y libertad*. Barcelona, Paidós, pp. 115-135. ISBN: 978 8449315107

Pohl, Daniela; **Bouchachia, Abdelhamid**; **Hellwagner, Hermann** (2015). "Social media for crisis management: Clustering approaches for sub-event detection". *Multimedia tools and applications*, v. 74, n. 11, pp. 3901-3932.
https://goo.gl/efb7FU
https://doi.org/10.1007/s11042-013-1804-2

Popescu, Mihaela; **Baruh, Lemi** (2013) "Captive but mobile: Privacy concerns and remedies for the mobile environment". *The information society*, v. 29, n. 5, pp. 272-286.
https://doi.org/10.1080/01972243.2013.825358

Privacy-International (s.f.). *Metadata*.
https://privacyinternational.org/node/573

Richardson, Janice (2016). *Law and the philosophy of privacy*. Londres: Routledge. ISBN: 978 0415572439

Sarker, Abeed; **Ginn, Rachel**; **Nikfarjam, Azadeh**; **O'Connor, Karen**; **Smith, Karen**; **Jayaram, Swetha**; **Upadhaya, Tejaswi**; **Gonzalez, Graciela** (2015). "Utilizing social media data for pharmacovigilance: A review". *Journal of biomedical informatics*, v. 54, pp. 202-212.
https://doi.org/10.1016/j.jbi.2015.02.004

Schroeck, Michael; **Shockley, Rebeca**; **Smart, Janet**; **Romero-Morales, Dolores**; **Tufano, Peter** (2012). *Analytics: The real-world use of big data. How innovative enterprises extract value from uncertain data*. IBM Institute for Business Value.
https://goo.gl/vUCcwL

Schwartz, Paul M. (2013). "The EU-US privacy collision: A turn to institutions and procedures". *Harvard law review*, v. 126, n. 7, pp. 1966-2009.
http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_schwartz.pdf

Solove, Daniel J. (2008). *Understanding privacy*. Cambridge: Harvard University Press. ISBN: 978 067402772

Solove, Daniel J. (2013). "Introduction: Privacy self-management and the consent dilemma". *Harvard law review*, v. 126, n. 7, pp. 1880-1903.
http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Taddicken, Monika (2014). "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure". *Journal of computer-mediated communication*, v. 19, n. 2, pp. 248-273.
https://doi.org/10.1111/jcc4.12052

Tufekci, Zeynep (2014). "Big questions for social media big data: Representativeness, validity and other methodological pitfalls". En: *Procs of the 8th Intl AAAI Conf on weblogs and social media*.
https://arxiv.org/abs/1403.7400

Turow, Joseph; **Hennessy, Michael**; **Draper, Nora** (2015) *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Annenberg School for Communication University of Pennsylvania.
https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Unión Europea (1995). "Directiva 95/46/CE del Parlamento Europeo y del Consejo, 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". *Diario oficial de la Unión Europea*, n. L 282 de 23 de noviembre, pp. 0031-0050.
http://www.wipo.int/wipolex/es/details.jsp?id=13580

Unión Europea (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)". *Diario oficial de la Unión Europea*, n. L119 de 4 de mayo.
https://goo.gl/cAVmfJ

Utz, Sonja; **Kramer, Nicole C.** (2009). "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms". *Cyberpsychology: Journal of psychosocial research on cyberspace*, v. 3, n. 2, pp. 1-10.
http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1

Xiao, Yu; **Huang, Qunying**; **Wu, Kai** (2015). "Understanding social media data for disaster management". *Natural hazards*, v. 79, n. 3, pp. 1663-1679.
https://doi.org/10.1007/s11069-015-1918-0