Integridad contextual como marco conceptual para la protección de la privacidad en medios digitales

Contextual integrity as a conceptual framework to protect privacy on digital media

Amaya Noain-Sánchez

Como citar este artículo:

Noain-Sánchez, Amaya (2024). "Integridad contextual como marco conceptual para la protección de la privacidad en medios digitales [Contextual integrity as a conceptual framework to protect privacy on digital media]". *Infonomy*, 2(5) e24058.
https://doi.org/10.3145/infonomy.24.058

Amaya Noain-Sánchez
https://orcid.org/0000-0002-2845-3285
https://directorioexit.info/ficha7079
Universidad Rey Juan Carlos
Facultad de Comunicación
Departamento Periodismo y Comunicación Corporativa
Camino del Molino, 5
28942 Fuenlabrada (Madrid), España
amaya.noain@urjc.es

Resumen

Este texto profundiza en el concepto de "integridad contextual", marco de referencia desarrollado por Helen Nissenbaum para proteger la privacidad de los usuarios en los sistemas sociotécnicos. Sus investigaciones primigenias sobre vigilancia y protección de informaciones privadas se han aplicado a problemáticas como la recolección de datos personales en redes sociales, por buscadores como *Google*, tecnologías de macrodatos o sistemas de reconocimiento facial. Nissenbaum parte de la premisa de que la protección de la privacidad está ligada a la comprensión de los flujos de información que gobiernan cada escenario digital. Propone así una aproximación flexible a la protección de algo tan cambiante como el concepto de privacidad, evitando perderse en definiciones y casuísticas concretas y, por tanto, propiciando un marco de referencia que puede ser aplicado a cada concepción cultural. Su aproximación ha influido en normativas relativas a la protección de datos, como el comunitario RGPD, o normas sobre la seguridad de la información.

Palabras clave
Integridad contextual; Comunicación digital; Medios digitales; Flujos de información; Normas informacionales; Protección de datos, Privacidad; Esfera pública mediada; *Reglamento general de protección de datos*; RGPD.

Abstract
This text delves into the concept of 'contextual integrity', a benchmark developed by Helen Nissenbaum aimed at protecting users' privacy when interacting with sociotechnical systems. Her work on privacy and surveillance has been applied to address a huge variety of issues related to the collection of personal data on digital media, be it on social networks, by search engines such as *Google*, big data technologies or facial recognition systems. Nissenbaum offers a comprehensive approach by starting from the premise that privacy protection is linked to the users' understanding of information flows governing each digital context. In doing so, she proposes a fluid approach to privacy protection, avoiding the task of defining any context provided by technology, thus creating a benchmark which can be applied to any cultural or changing conception of privacy. This benchmark has also influenced regulations on personal data, such as the GDPR, and on information security.

Keywords
Contextual integrity; Digital communication; Digital media; Informational flows; Informational norms; Data protection; Privacy; Mediated public sphere; *General Data Protection Regulation*; GDPR.

1. Introducción

Una de las aportaciones más notables para abordar la protección de las informaciones privadas en los espacios públicos mediados digitales, corresponde a la investigadora estadounidense Helen Nissenbaum. Su doctrina, la Integridad Contextual (IC), parte del estudio de la vigilancia masiva propiciada por el uso de la tecnología digital a finales de los años 90 y primera década del siglo XXI. Si bien la vigilancia en sí misma no constituye un fenómeno novedoso, ni achacable exclusivamente al paradigma digital, la autora intenta dar respuesta a los desafíos que la digitalización, por sus características inherentes, presenta para la protección de la esfera privada del individuo.

Durante su trabajo como investigadora en el *Department of Media, Culture, and Communication* de la *New York University*, Nissenbaum se centra en prácticas como la grabación con cámaras de circuito cerrado en espacios públicos, el uso de dispositivos digitales de control en el entorno laboral o los registros en bases de datos gubernamentales (**Solove**, 2002) para, posteriormente, analizar el uso de las informaciones personales recabadas por los gobiernos tras los atentados terroristas del 11S en Nueva York.

Estas investigaciones parten de una coyuntura concreta vinculada al desarrollo tecnológico de la época: en un primer momento y, aun cuando podemos hablar del año 1995 como el año de uso generalizado de internet (**Castells**, 2001), la

capacidad de usar la tecnología para vigilar a los ciudadanos está sólo en manos del poder gubernamental y de grandes corporaciones.

Nissenbaum plasma las conclusiones de estas primeras investigaciones en su artículo "Privacy as contextual integrity" de 2004. No obstante, el subsiguiente despegue de la tecnología (y filosofía) 2.0 y sus desarrollos posteriores consiguen democratizar no sólo el uso de las herramientas digitales y la programación de la red por parte de cualquier usuario, sino que propician la visibilidad de lo que antes se comunicaba en el anonimato. La digitalización de todas las esferas de actividad del ser humano se traduce en una capacidad de vigilancia y control desconocida hasta entonces, se sobredimensiona la recopilación, intercambio y triangulación de la información como nunca en la historia. Además, estas acciones pueden ser realizadas por cualquiera con acceso a la red.

En este texto, Nissenbaum enuncia la necesidad de un marco global, flexible, adaptable a cada cultura y cambiante en función de los usos sociales. Un marco que huya de las definiciones clásicas e inoperantes que distinguen entre espacio público *vs*. espacio privado, como compartimentos estancos que separan las áreas (físicas) de protección, frente a aquellas de visibilidad y en las que cualquier injerencia en lo privado es aceptable. Reniega, asimismo, del diferente nivel de protección que se da a las informaciones en función de si contienen datos "sensibles" o "no sensibles", pues la capacidad de triangular datos que ofrecen las herramientas digitales facilita que cualquier dato identificativo ayude a desentrañar informaciones personales (**Nissenbaum**, 2004).

> Independientemente de que estemos en un espacio público como en nuestro entorno laboral, habrá ciertos datos personales que podremos desplegar sin que por ello se desprenda que se ha cometido una violación de nuestro ámbito privado, mientras que no haremos visibles otras informaciones

Las investigaciones centradas en este nuevo paradigma de vigilancia con múltiples actores culminan en su libro de 2010, *Privacy in context: Technology, policy, and the integrity of social life*. Como respuesta a todas estas situaciones fragmentadas, Nissenbaum enuncia su doctrina, con la que propone un enfoque sistémico y adaptable a la realidad cambiante de las interacciones humanas y del sustrato digital, un ecosistema en el que el intercambio de flujos informativos es incesante e inaccesible a la percepción analógica humana.

2. ¿A qué nos referimos con "respeto a la integridad del contexto"?

Nissenbaum enmarca su argumentación en términos de los flujos de información que se despliegan en cada contexto comunicativo y que nos permiten desarrollar de manera eficiente dicha interacción. En este intercambio, parte de las informaciones desplegadas corresponderán a informaciones privadas y su uso posibilitará el desarrollo de la actividad comunicativa en tanto que son de-

mandadas por el contexto. Una suerte de "pertinencia" de ciertos contenidos, en función de las características del contexto comunicativo y la finalidad del intercambio (una idea, la de finalidad, que se ha recogido en normativas como el *Reglamento general de protección de datos*, RGPD).

En nuestro día a día, el despliegue de datos relativos a nuestra vida privada forma parte de nuestras interacciones sociales e incluso, podría tratarse de un requisito necesario para la eficacia comunicativa. Esto significa que, independientemente de que estemos en un espacio público como en nuestro entorno laboral, habrá ciertos datos personales que podremos desplegar sin que por ello se desprenda que se ha cometido una violación de nuestro ámbito privado, mientras que no haremos visibles otras informaciones.

¿Cuál es el parámetro para saber qué informaciones privadas pueden intercambiarse en la comunicación sin infringir nuestra intimidad? El contexto.

Por contexto o escenario que rodea al hecho comunicativo nos referimos a un momento concreto de la interacción. Es decir, está determinado por una serie de coordenadas (tiempo, espacio, etc.), actores implicados, expectativas, usos y costumbres, etc., que lo caracterizan. Estos escenarios emergen en todos aquellos "dominios sociales" (**Nissenbaum**, 2010) en los que puede darse la interacción: el supermercado, una reunión de trabajo, una charla con amigos… Son infinitos e inabarcables, pero nunca son iguales, por lo que hacer una definición de los datos que se considera apropiado desplegar en cada momento para satisfacer la interacción comunicativa sería inviable.

Por contexto o escenario que rodea al hecho comunicativo nos referimos a un momento concreto de la interacción. Es decir, está determinado por una serie de coordenadas (tiempo, espacio, etc.), actores implicados, expectativas, usos y costumbres, etc., que lo caracterizan. Estos escenarios emergen en todos aquellos "dominios sociales" en los que puede darse la interacción: el supermercado, una reunión de trabajo, una charla con amigos…

En cada cruce de coordenadas particular, los intercambios de información vienen delimitados por una serie de convenciones que cambian en función de los factores que configuran el escenario como, por ejemplo, los agentes implicados, los usos culturales correspondientes o las necesidades del sujeto, entre otros. Por ello, diferentes personas, pertenecientes a culturas diversas desplegarán, en un mismo escenario, cantidades distintas de datos privados, sin sentir por ello que su intimidad y vida privada ha sido vulnerada.

En suma, cuando citamos el respeto a la integridad del contexto nos referimos a:

El mantenimiento de la coherencia de los flujos informativos que conforman dicho escenario, así como a la pertinencia del despliegue de ciertos datos en el mismo, estando estos dos factores determinados por la coyuntura concreta, esto es, las coordenadas que dan forma a esa situación específica (**Noain-Sánchez**, 2016a).

2.1. Dominios sociales

Nissenbaum habla de cinco parámetros que nos ayudan a conocer la naturaleza de los contextos comunicativos. Estos son:

1) temática (*data subject*)
2) emisor de los datos (*sender of the data*)
3) canal (*recipient of the data*)
4) tipo de información (*information type*)
5) principio de la transmisión (*transmission principle*).

Las propiedades de un contexto concreto se mantendrán en la medida en que no exista ninguna mutación en los elementos que lo definen, ya que, si cambia una de las coordenadas o los agentes involucrados, haría aparición otro escenario distinto.

2.2. Interpretación del contexto: normas informacionales

Para adecuar el flujo comunicativo, es decir, saber qué datos es pertinente dar a conocer en cada contexto, los individuos interactuantes deben comprender cuál es la naturaleza del escenario concreto, "leer" todas esas pistas informacionales ("normas informacionales" en palabras de Nissenbaum) que nos permiten comprender las atribuciones y alcance de dicho escenario.

Las normas informacionales son aquellas informaciones percibidas por el sujeto de la acción comunicativa y que proporcionan comprensión sobre las características de cada escenario concreto. Estas normas dictaminan qué tipo y qué cantidad de datos es conveniente pertinente revelar en cada contexto concreto, así como con cuántos interlocutores queremos compartir estos datos y a qué otros escenarios deben fluir. Es decir, proporcionan información sobre los límites hasta los que es adecuado desplegar información y de ser infringidas, estaríamos frente a una vulneración de nuestra privacidad o uso ilegítimo de nuestros datos personales.

Existe un número ilimitado de posibles fuentes informacionales (la convención, la ley, la historia, la cultura, los usos y costumbres…). No obstante, Nissenbaum las agrupa en dos clases normativas generales:

1) **Normas de pertinencia o de propiedad de la información:** son las que nos informan sobre el tipo o la naturaleza del intercambio comunicativo. Al hacerlo, indican qué información sobre los individuos se considera aceptable, esperada o, incluso, demandada revelar en una determinada coyuntura o contexto (**Nissenbaum**, 2004). En otras palabras, definen en qué escenarios y bajo qué condiciones resulta apropiado compartir ciertos datos. Por ello, también podrían denominarse normas "de lógica del contexto" (**Noain-Sánchez**, 2016a).

2) **Normas de distribución o de flujo de información:** se refieren al movimiento o transferencia de datos de un escenario comunicativo a otro. El despliegue de datos debe estar justificado por la finalidad a la que estos se destinan y, por tanto, estas normas establecen los límites que evitan la distribución abierta e indiscriminada de la propia información.

2.3. ¿Cómo se aplican las normas informacionales?

Nissenbaum cruza los distintos dominios sociales en los que se puede dar un intercambio comunicativo (una visita al médico, el entorno laboral, etc.) con la capacidad de acceso e interpretación a ambas normas:

- Los cinco parámetros previamente indicados (temática, emisor, tipo de información, formato y principio de la información) nos indicarán el dominio social en el que interactuamos.
- Y las normas informacionales nos indicarán qué datos privados podemos desplegar para que la interacción comunicativa sea satisfactoria.

En un intercambio comunicativo presencial, por ejemplo, en una visita al médico, se considera oportuno que el individuo aporte datos sobre su condición física o los medicamentos que toma, pero no esperamos que el doctor le pregunte sobre su salario o el coche que conduce. Estas serían normas de pertinencia o de propiedad de la información.

Siguiendo el ejemplo anterior, asumimos que lo que le contamos a nuestro médico es confidencial, por lo que bajo ningún concepto esperamos que lo comunique a otros sin haber sido informados, ni haber dado nuestro consentimiento explícito. Así, si nuestro historial médico se hiciese público en Internet sin nuestro conocimiento ni consentimiento, las normas de distribución o flujo de información habrían sido claramente quebrantadas.

La integridad contextual se mantiene cuando ambas normas son respetadas. Por el contrario, se entiende que se habrá producido una vulneración si una sola de ellas es violada en un momento dado.

En resumen, la idea central de la IC se fundamenta en la siguiente creencia:

> No hay arenas de la vida no gobernadas por normas informativas [...] Prácticamente todo: las actividades que llevamos a cabo, los acon-

> En nuestras actividades cotidianas la gente está en casa con sus familias, van a trabajar, buscan consejo médico, visitan amigos, consultan psiquiatras, hablan con abogados, van al banco, a centros de oración, votan, compran y más. Cada uno de esos escenarios o contextos está definido por un conjunto distinto de normas que gobiernan sus varios aspectos como roles, expectaciones, acciones y prácticas

> tecimientos que suceden, las transacciones que realizamos… todo ocurre en un contexto no solo en cuanto a lugar, sino que conllevan unas convenciones y expectaciones culturales […] En nuestras actividades cotidianas la gente está en casa con sus familias, van a trabajar, buscan consejo médico, visitan amigos, consultan psiquiatras, hablan con abogados, van al banco, a centros de oración, votan, compran y más. Cada uno de esos escenarios o contextos está definido por un conjunto distinto de normas que gobiernan sus varios aspectos como roles, expectaciones, acciones y prácticas (**Nissenbaum**, 2004).

2.4. La IC en los escenarios digitales

Cuando la interacción se caracteriza por la copresencia en un espacio físico y con unas coordenadas temporales compartidas (comunicación no mediada) la información que percibimos del contexto es accesible, fácilmente comprensible y no presenta problemas de interpretación. En dichas interacciones, salvo que desconozcamos los usos culturales/sociales en los que estamos inmersos, somos capaces de comprender qué datos debemos desplegar, ya que estarían justificados por el propio contexto.

La comunicación mediada, caracterizada por la ausencia de unas coordenadas espacio-temporales compartidas, dificulta la comprensión de las normas informacionales que rigen y definen el escenario comunicativo. Esta complejidad llega a su punto álgido con la digitalización. En el universo digital las normas informacionales vendrían determinadas exclusivamente por la información que es capaz de percibir, comprender o, incluso, intuir el usuario al visualizar la interfaz. Esta es la única aproximación perceptible (analógica) y, por tanto, comprensible a la que puede acceder, pero no transmite fielmente el flujo de datos que subyace bajo la superficie. Los flujos informacionales no son transparentes, son inaccesibles o bien implican un grado de complejidad que dificultan la comprensión o posterior toma de decisiones (**Noain-Sánchez**, 2016a).

En el universo digital las normas informacionales vendrían determinadas exclusivamente por la información que es capaz de percibir, comprender o, incluso, intuir el usuario al visualizar la interfaz. Esta es la única aproximación perceptible y, por tanto, comprensible a la que puede acceder, pero no transmite fielmente el flujo de datos que subyace bajo la superficie

A esto hay que sumarle que la capacidad de vulneración de la privacidad es mayor: las tecnologías digitales proporcionan un sustrato en los que grandes cantidades de información son susceptibles de ser almacenadas y agregadas y los datos introducidos pueden ser fácilmente copiados, utilizados y sacados de contexto, algo, esto último, que contravendría las normas informacionales y quebrantaría claramente la integridad del contexto. Por ejemplo, si nos registramos en cualquier servicio de redes sociales y la plataforma usa estos datos para otra finalidad

distinta, sin nuestro conocimiento, estaría vulnerando las normas de distribución de la información. La ruptura de la integridad contextual conlleva, además, un doble riesgo:

1) el perfilado de los usuarios sin que ellos sean conscientes y, un paso más allá,
2) la identificación de los mismos (recordemos cómo aumenta la capacidad de triangulación de los datos).

2.5. Proporcionar información cuando el usuario no es capaz de entender las normas informacionales ¿Cómo lo hacemos?

Siguiendo la lógica de la IC, es crucial conocer las atribuciones de cada contexto para poder decidir qué información personal desplegar. Pero si los escenarios son confusos o sus normas difíciles de percibir es imperativo ofrecer información adicional, de ahí, que aparezcan herramientas como el consentimiento informado, tomado del mundo de la medicina.

No obstante, para suplir esta falta de comprensión de los contextos digitales, se ha propuesto una versión adaptada de esta herramienta: el consentimiento informado activo por capas. Con el mismo se intenta cubrir la merma informativa indicando al usuario qué datos personales serán recogidos y para qué finalidad serán tratados, en una primera capa, y una información más en profundidad, en una segunda capa (**Noain-Sánchez**, 2016b y 2016c). Si bien la aplicación de estos consentimientos en la actualidad se ha convertido en un obstáculo a la navegación más que traducirse en un arma efectiva, la finalidad primigenia de esta herramienta se vinculaba más a la alfabetización digital e interiorización de riesgos asociados a prácticas de monetización y rastreo, que al actual salto inconsciente de pantallas para permitir la navegación.

De hecho, se propone que el uso del consentimiento se reserve únicamente a ciertos usos relevantes "de forma que los individuos presten una atención mayor cuando el consentimiento les es requerido y, de este modo, sea un mecanismo más efectivo" (**Gil-González**, 2016). En estas situaciones concretas en las que el usuario tenga que manifestar una cierta proactividad, el consentimiento informado recuperaría un valor real (**Gil-González**, 2016; **Barocas**; **Nissenbaum**, 2014).

> El consentimiento informado puede tener un valor informativo en un primer momento, pero su uso constante no se traduce en un usuario bien informado, que es lo que motivó su desarrollo. De nuevo la necesidad de impulsar la alfabetización digital, la capacitación crítica y la privacidad desde el diseño y/o por defecto son cruciales para asegurar la protección del usuario

Subyace así la idea de que el consentimiento puede tener un valor informativo en un primer momento, pero su uso constante no se traduce en un usuario bien informado, que es lo que motivó su desarrollo. De nuevo la necesidad de impul-

sar la alfabetización digital, la capacitación crítica y la privacidad desde el diseño y/o por defecto son cruciales para asegurar la protección del usuario.

2.6. Luces y sombras de la IC

Desde su aparición, la doctrina de Nissenbaum se ha aplicado al estudio de los flujos de información y recogida de datos en diferentes redes sociales como, por ejemplo, *Twitter* (**Casey**; **Proferes**, 2018), *Facebook* (**Noain-Sánchez**, 2015 y 2016a; **Hull**; **Lipford**; **Latulipe**, 2014) y ha servido como fundamento para el estudio de casos como el protagonizado por *Facebook-Cambridge Analytica*.

El razonamiento de Nissenbaum se ha convertido, además, en fuente de derecho y ha servido para sentar algunos de los pilares básicos en la protección de datos personales. En la Europa Comunitaria, por ejemplo, la vinculación del uso de los datos únicamente a la finalidad para la que los cedió el usuario al otorgar su consentimiento es un requisito que ya aparece contemplado a nivel de Reglamento: concretamente con el RGPD europeo que entró en vigor el 4 de mayo de 2016 (aunque el legislador comunitario estableció una *vacatio legis* de dos años para su aplicabilidad) y, particularmente en España, en la *Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales*, de 5 de diciembre, de 2018.

No obstante, aunque la doctrina de la IC se ha convertido en estándar de aceptabilidad respecto al flujo de información personal, el planteamiento de Nissenbaum no está exento de crítica. Según **Rule** (2019), por ejemplo, aun cuando

> "promete distinguir entre las formas de divulgación que están éticamente justificadas y otras, basadas en las relaciones sociales y los propósitos de los entornos en los que ocurren […] las nociones de que las normas que subyacen a cualquier dominio dado de la conducta humana no son ambiguas, ni cuestionadas simplemente no resisten un examen detallado" (**Rule**, 2019).

De hecho, mantiene Rule, para cualquier contexto existen muchas interpretaciones diferentes de lo que se consideran normas "correctas", por lo que, de manera interesada, se puede considerar aquellas interpretaciones que beneficien a alguno de los agentes del intercambio comunicativo. El hecho de que esta flexibilidad se transforme en laxitud provoca, en palabras de Rule, que sea una doctrina atractiva para aquellos

> "legisladores que buscan desactivar los conflictos entre los defensores de los nuevos usos de la información personal y los defensores de la privacidad. Pero casi no ha dado prescripciones políticas inequívocas que todas las partes puedan acordar" (**Rule**, 2019).

La traslación de esta laxitud la encontramos en algunos aspectos del citado RGPD. Este Reglamento concede, tal y como se indica en el propio texto amplios "márgenes de maniobra" a los Estados para concretar a nivel nacional sus disposiciones. A pesar de la lógica de la que parte el Reglamento, en la que se concede espacios de autonomía al derecho de los Estados, a efectos prácticos, la interpretación de parte de su articulado da lugar a no pocos vacíos. Esto es especialmente llamativo en aquellas situaciones que el texto denomina "situa-

ciones específicas de tratamiento de datos" y que constituye una miríada de casos en los que la protección de datos resulta inespecífica, como, por ejemplo, cuando esta aparece relacionada con la libertad de expresión.

3. Conclusión

El trabajo de Nissenbaum ofrece un marco de referencia conceptual para comprender las peculiaridades que la tecnología digital añade a la protección de la privacidad. La importancia de esta aproximación recae principalmente en:

El trabajo de Nissenbaum ofrece un marco de referencia conceptual para comprender las peculiaridades que la tecnología digital añade a la protección de la privacidad. La importancia de esta aproximación se debe a:
1) su adaptabilidad a las diversas concepciones de "privacidad" existentes en cada época, cultura o sociedad;
2) su capacidad de dar respuesta a la variabilidad y mutabilidad inherente a los contextos digitales

1) Su adaptabilidad a las diversas concepciones de "privacidad" existentes en cada época, cultura o sociedad, ya que Nissenbaum evita definir qué se entiende por público o privado y vehicula la protección de la privacidad a la interpretación de las normas informacionales que rigen gobiernan los flujos de información cada contexto concreto;

2) Su capacidad de dar respuesta a la variabilidad y mutabilidad inherente a los contextos digitales. Esta peculiaridad hace que dicha aproximación resulte apropiada para solventar la problemática derivada de las diversas nociones culturales de intimidad y vida privada que se dan en los distintos países y que confluyen en este espacio global y sin fronteras que es Internet. Refuta, asimismo, la idea de que solo por el hecho de que los usuarios emplacen cierta información privada en espacios públicos mediados deban perder todas las expectativas de control, poniendo en valor esa facultad del individuo de potestad sobre sus propios datos personales y que completa el derecho a la intimidad. No obstante, la ambigüedad que provoca un marco tan laxo se traduce en una falta de soluciones concretas acentuando la necesidad de alfabetización digital, conocimiento crítico y diseños que propicien un nivel máximo de privacidad.

4. Referencias

Barocas, Solon; **Nissenbaum, Helen** (2009). On notice: The trouble with notice and consent (2009). *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, October 2009.
https://ssrn.com/abstract=2567409

Barocas, Solon; **Nissenbaum, Helen** (2014). Big data's end run around anonymity and consent. In: Lane, Julia; Stodden, Victoria; Bender, Stefan;

Nissenbaum, Helen (eds.). *Privacy, big data, and the public good: Frameworks for engagement*. Cambridge University Press; 44-75.

Castells, Manuel (2001). *La galaxia Internet*. Barcelona: Plaza & Janés Editores.

Fiesler, Casey; **Proferes, Nicholas** (2018). "Participant" perceptions of Twitter research ethics. *Social Media + Society*, 4(1).
https://doi.org/10.1177/2056305118763366

Gil-González, Elena (2016). *Big data, privacidad y protección de datos*. Madrid: BOE/AEPD. ISBN: 978 84 340 2309 3
https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

Gonzalez-Gaitano, Norberto (1990). *El deber de respeto de la intimidad. Información pública y relación social*. Pamplona: Eunsa.
https://doi.org/10.1177/2056305118763366

Hull, Gordon; **Richter-Lipford, Heather**; **Latulipe, Celine** (2009). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology* 13(4):289-302
https://doi.org/10.1007/s10676-010-9224-8

Nissenbaum, Helen (2004). Privacy as contextual integrity. *Washington Law Review*, n. 79, 119-158.

Nissenbaum, Helen (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

Nissenbaum, Helen (2011). A contextual approach to privacy online. *Daedalus*, 140 (4): 32-48.
https://doi.org/10.1162/DAED_a_00113

Noain-Sánchez, Amaya (2015). La privacidad como integridad contextual y su aplicación a las redes sociales. *Zer - Revista de Estudios de Comunicación*, 20(39).
https://doi.org/10.1387/zer.15531

Noain-Sánchez, Amaya (2016a). *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*. XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Madrid: BOE/AEPD.
https://www.aepd.es/sites/default/files/2019-10/la-proteccion-de-la-intimidad.pdf

Noain-Sánchez, Amaya (2016b). "Privacy by default" and active "informed consent" by layers. *Journal of Information, Communication and Ethics in Society*, 14(2), 124-138. *https://doi.org/10.1108/JICES-10-2014-0040*

Noain-Sánchez, Amaya (2016c). Knowledge as an effective tool to protect ICT users' privacy. The layered informed consent as 'opt-in' model. *Doxa Comunicación. Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales*, 22, 149-155.
https://doi.org/10.31921/doxacom.n22a7

Rule, James B. (2019). Contextual Integrity and its Discontents: A Critique of Helen Nissenbaum's Normative Arguments. *Policy & Internet*, 11(3), 260-279. *https://doi.org/10.1002/poi3.215*

Solove, Daniel J. (2002). Modern studies in privacy law: Notice, autonomy and enforcement of data privacy legislation: Access and aggregation: Public records, privacy and the constitution. *Minnesota Law Review*, 86, 1137-1174.
https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2079&context=faculty_publications