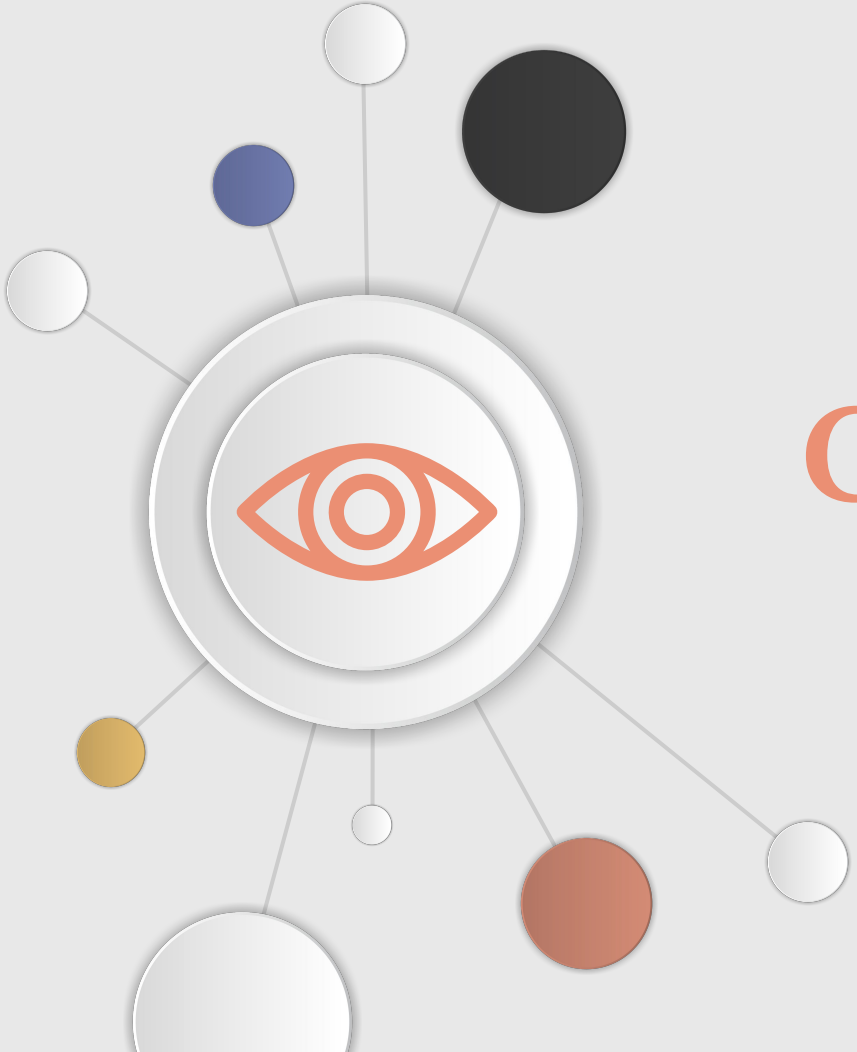

Integridad Contextual y Privacidad

Curso: Ética y Ciencia de la Información,
FIC, Udelar

Docente: Ay. Maximiliano Rodríguez - Fleitas

Problemas de privacidad actuales

A partir de la disrupción de las Tecnologías de la Información y la Comunicación (TIC) se complejizan los problemas de privacidad. Se plantea la necesidad de introducir abordajes interdisciplinarios que integren perspectivas y teorías éticas, derecho, política, ingeniería, entre otros.

Helen Nissenbaum

Profesora de ciencia de la información en Cornell Tech . Es conocida por el concepto de "**integridad contextual**" y su trabajo sobre privacidad, leyes de privacidad , confianza y seguridad en línea. Formación en matemática, filosofía y ciencias sociales.

¿Qué es la integridad contextual?

La teoría de la Integridad Contextual es presentada por HN en su libro *Privacy In Context: Technology, Policy, and the Integrity of Social Life* publicado en 2010.

"La teoría de **Integridad Contextual** identifica las raíces del desconcierto, la resistencia y, a veces, la resignación expresada por expertos y no expertos por igual. Según la teoría, los sistemas finalmente calibrados de **normas sociales, o reglas**, gobiernan el **flujo de información personal en distintos contextos sociales** (por ejemplo, educación, atención médica y política). Estas normas, que llamo **normas informacionales relativas al contexto**, definen y sostienen actividades esenciales y relaciones e intereses clave, protegen a las personas y los grupos contra el daño y equilibran la distribución de poder. Sensibles a contingencias históricas, culturales e incluso geográficas, **las normas informacionales** evolucionan con el tiempo en distintos patrones de una sociedad a otra. **Las tecnologías de la información nos alarman cuando se burlan de estas normas informacionales, cuando, en palabras de esta teoría, violan la integridad contextual**". (nuestra traducción de Nissenbaum, 2019)

Normas informacionales

“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 apud Noain Sánchez, 2015).

Las fuentes de estas normas son diversas: convenciones, hábitos, la ley, la historia, la cultura, las relaciones de poder, las expectativas, etc.

1. Normas de Pertinencia o Propiedad

Se trata de normas que **determinan qué tipo de información personal es apropiado compartir en un contexto específico.** Así, en una consulta médica resulta pertinente hablar de la salud, pero no del salario. La apertura de estas reglas varía según la situación: entre amigos la información fluye con mayor libertad, mientras que en una clase o entrevista laboral se restringe. Ningún espacio está exento de estas normas; incluso en lugares públicos como la calle, nos parecería una intromisión si un desconocido pidiera datos personales como nuestro nombre.

2. Normas de Distribución o Flujo de Información (FI)

Las normas de distribución **regulan cómo circula la información entre personas.** En contextos de confianza, como una charla con un amigo, es común compartir datos íntimos —desde rutinas hasta emociones o posturas políticas—, pero esas normas implican que el receptor no debe difundir esa información a terceros sin condiciones previas. En este sentido, funcionan como una protección contra la circulación indiscriminada de lo privado.

Los flujos de información

¿Cómo proteger la privacidad sin detener los flujos de información?

El secreto es una forma de interrumpir estos flujos. Por lo que minimizar los datos no siempre puede ser la opción correcta.

¿Qué es un flujo de información apropiado?

Es un flujo que se ajusta a las **normas informacionales** (reglas, leyes, convenciones expectativas sociales)

Mecanismos de consentimiento en línea

Los famosos “términos y condiciones o acuerdos de privacidad” que podemos encontrar en la mayoría de las aplicaciones digitales.

HN señala que tienen problemas y debilidades visibles:

1. Su estructura es compleja y legalista.
2. Utilizan el método “tomalo o dejalo”: si no los aceptas no puedes utilizar el servicio.
3. En cierto punto los mantenemos porque son convenientes para los proveedores y desarrolladores de tecnología.

La Integridad Contextual necesita conocer y explicitar las reglas que hacen que el flujo de información sea apropiado.

HN toma elementos de varios teóricos sociales (sobre todo la teoría de campos de Bordieu y la genealogía de Foucault) para la caracterización de los dominios (espacios) sociales: estos dominios emergen alrededor de ciertos valores, propósitos y principios.

Por ejemplo: a partir del valor de “educar a los jóvenes” se construye y evoluciona todo un dominio educativo. Lo mismo podría pensarse para el dominio político, la medicina, entre otros.

¿Cómo describimos un FI?

Es necesario explicitar los parámetros y valores que describen el flujo de información en un dominio determinado.

Parámetros	Valor
Actores: remitentes, destinatarios y canal	Los roles que cumple cada uno de estos actores son partes constitutivas de los dominios o contextos. Por ejemplo, un médico y sus pacientes, un profesor y sus estudiantes, etc.
Tipo de información	Conectada con la identidad del contexto. Por ejemplo: información médica, financiera, personal, entre otros.
Principios de transmisión	Restricción bajo la cual fluye la información: el consentimiento, la coacción, el robo, la compraventa, la confidencialidad, la administración de justicia, etc.

¡Todos los parámetros son importantes para evaluar el impacto de los flujos de información en la privacidad!

Obviar uno de los cinco parámetros en la evaluación del FI puede brindar resultados ambiguos.

Los parámetros nos permiten definir el dominio en el se materializa el FI.
Las normas de ese dominio nos permiten saber qué datos es conveniente desplegar para que el FI fluya de forma adecuada.
Si alguna de estas normas es violada, el FI deja de ser adecuado.

Por ejemplo, algunos tipos de lenguaje pueden dificultar el análisis: el uso de la voz pasiva para describir el movimiento de datos, el investigador o evaluador puede pasar por alto que existe un agente activo que realiza la transferencia de datos. Por ejemplo, la oración "A Juan le robaron la identidad" permite pasar por alto que alguien o algo robó la identidad de Juan. Si decimos que "Mónica pudo encontrar los registros de deuda de Luciana porque se habían publicado en internet", ignoramos implícitamente que alguien o alguna organización recopiló los registros de deuda y los publicó en línea.

Ejemplo: "Los residentes en Uruguay que posean dos empleos están legalmente obligados a presentar declaraciones juradas de IRPF ante la Dirección General Impositiva (DGI), las cuales deben incluir información como nombre, dirección, cédula de identidad, ingresos brutos, entre otros, en condiciones de estricta confidencialidad."

Ejemplo: "Los residentes en Uruguay que posean dos empleos están legalmente obligados a presentar declaraciones juradas de IRPF ante la Dirección General Impositiva (DGI), las cuales deben incluir información como nombre, dirección, cédula de identidad, ingresos brutos, entre otros, en condiciones de estricta confidencialidad."

Titular de los datos: residente uruguayo que tenga dos empleos.

Remitente: el mismo residente.

Destinatario: Dirección General Impositiva (DGI).

Tipo de información: información fiscal y personal.

Principio de transmisión: los remitentes están obligados a suministrar esa información, el destinatario mantendrá la información en estricta confidencialidad.

¿Cuando violamos la integridad contextual?

Los enfoques tradicionales

El individuo controla su información personal:
Desde la perspectiva de la Integridad Contextual (IC), reducir la privacidad únicamente al control de los datos personales resulta problemático. El riesgo de este enfoque es que se limita a un solo principio de transmisión y limita la protección de la privacidad a un único dominio, dejando de lado su complejidad contextual.

En algunos dominios perdemos el derecho de controlar nuestra información, por ejemplo, cuando somos obligados a presentar declaraciones juradas ante un ente público.

División del mundo informacional en sensible o no sensible:
Porque una información no sea sensible no está libre de estar sujeta a normas.
A igual que en el enfoque anterior, nos limitamos a un solo parámetro del flujo de información: el tipo de información.

¿Pero cuáles son las normas que rigen los FI en diferentes dominios? Es algo que hay que investigar. Debemos encontrar las normas que restringen el FI pero que no lo bloqueen.

¿Cómo defender la legitimidad moral de los contextos?

Develar de los contextos:

- Intereses y preferencias de las partes afectadas: ¿Quién se beneficia con el FI? ¿A quién perjudica?
- Cómo se sostienen los principios éticos, políticos y valores: ¿Se reduce la libertad de expresión?¿Quién ejerce el control?
- Cómo se promueven sus funciones, objetivos y valores contextuales: podemos observar las acciones pero necesitamos llegar al fondo del propósito.

La privacidad es fundamental a nivel social, no solo es importante para el individuo, un FI adecuado asegura la privacidad.

El caso de Cambridge Analytica: no solo es una violación a los consentimientos o acuerdos de privacidad de los usuarios. **Sus acciones desestabilizaron el sistema democrático.**

Presentación basada en:

- Capurro, R. (2024). Ética Digital: entre res privata y res pública. Eds. Petra Grimm, Kai Erik Trost y Oliver Zöllner. *Digitale Ethik*. Baden Baden: Editorial Nomos. https://www.capurro.de/eticadigital.html
- Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.
- Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus: Journal of the American Academy of Arts & Sciences,* 39-48. https://www.amacad.org/daedalus/protecting-internet-public-commons
- Noain Sánchez, A. (2015). La privacidad como integridad contextual y su aplicación a las redes sociales. *Zer: Revista de estudios de comunicación = Komunikazio ikasketen aldizkaria*, 20 (39). https://dialnet.unirioja.es/servlet/articulo?codigo=5498557