18^{0} FORO DE GOBERNANZA DE INTERNET DE AMÉRICA LATINA Y EL CARIBE - LACIGF

Córdoba, Argentina, 5 y 6 de noviembre de 2025

RELATORÍA

Información de la sesión

Título de la sesión: Datos en fuga: cómo se exponen y explotan nuestros datos en internet

Fecha y hora: 6 de noviembre, 14h15 a 15h30 (hora de Argentina, UTC -3)

Lugar: Universidad Católica de Córdoba (Obispo Trejo, 323, Córdoba).

Moderación:

- Lucía León, Hiperderecho (Moderadora) – modalidad presencial
- Ximena Cuzcano Chavez, Derechos Digitales (Moderadora virtual)

Panelistas:

- Iagê Miola, Autoridad Nacional de Protección de Datos (ANPD) de Brasil– modalidad virtual
- Olga María Escudero Vílchez, Autoridad Nacional de Protección de Datos Personales, Ministerio de Justicia y Derechos Humanos de Perú-modalidad virtual
- Marcela Pallero, Universidad Tecnológica Nacional (UTN) de Argentina– modalidad virtual
- Paloma Lara Castro, Derechos Digitales (Ponente) – modalidad presencial

Relatoría:

- Heidy Elieth Balanta. Escuela de Privacidad- Colombia- Modalidad Virtual.

Contenido de la relatoría

Mensajes centrales:

El foro evidenció que el mercado ilegal de datos en la región es estructural, persistente y nutrido por fallas simultáneas en normativa, capacidades institucionales y seguridad digital.

Las filtraciones afectan de forma desproporcionada a mujeres, niñas y personas LGBTIQ+, y se utilizan para violencias, extorsión y ataques a infraestructuras críticas. El reto no necesariamente es la falta de normativa, sino la incapacidad de Estados y plataformas para prevenir, investigar y desmantelar este ecosistema. Se requiere coordinación real entre autoridades de protección de datos, ciberseguridad, policía y fiscalía, así como el fortalecimiento de capacidades técnicas, trazabilidad obligatoria, responsabilidad efectiva de plataformas y políticas públicas con enfoque de derechos y de género.

Puntos principales:

1. **Dimensión del problema.**

- Durante la sesión se explicó que la compraventa de datos personales funciona como un ecosistema regional que abarca Brasil, Perú y Argentina. Aunque Telegram es visible en las investigaciones, los panelistas enfatizaron que el mercado ilegal es más amplio y se mueve entre múltiples plataformas. Se mencionó que se identificaron al menos 27 grupos activos dedicados a estas prácticas. Se señaló que los datos filtrados incluyen información altamente sensible, como registros médicos, números de documento, nombres y apellidos, y que en muchos casos no es posible identificar la fuente que originó la fuga, lo que impide atribución y dificulta la reacción institucional.
- Se destacó que estos datos circulan fuera de contexto, desconectados del incidente original, y que este mercado alimenta tanto prácticas de violencia como ataques de ingeniería social e incluso riesgos para infraestructura crítica.
- También se mencionó que los servicios de inteligencia de amenazas suelen comprar estos datos para protegerse, lo que genera una diferencia entre organizaciones que pueden costear ese acceso y personas o entidades que no cuentan con esos recursos.

2. **Fragilidades estructurales**

Los panelistas coincidieron en que los tres países cuentan con legislación de protección de datos, pero existe un conjunto de debilidades transversales:

- Normativas: Las leyes existen, pero su aplicación es limitada y no corresponde con las capacidades reales de los Estados. En el caso de Paragüay recientemente el Congreso de dicho país aprobó la ley de protección de datos personales.
- Institucionales: Las autoridades de protección de datos carecen de independencia suficiente, de presupuesto, personal técnico y herramientas para investigar incidentes complejos.
- Seguridad de la información: En las entidades públicas persisten brechas significativas: ausencia de trazabilidad, controles de acceso insuficientes, interconexiones inseguras y falta de políticas de seguridad robustas. Se señaló una falta generalizada de cultura institucional en gestión de riesgos.

3. **Impacto diferencial y violencias**

- Se explicó que la venta ilegal de datos tiene impactos diferenciados, especialmente sobre mujeres, niñas y personas LGBTIQ+. Se destacó que la digitalización acelerada de los servicios públicos no ocurre en entornos neutrales y tiende a reproducir desigualdades preexistentes.
- Se mencionaron casos de inclusión de mujeres en grupos de Telegram con fines de hostigamiento, extorsión basada en datos filtrados, intimidación a personas que expresan opiniones sobre temas de género, y uso de información personal para coerciones dirigidas a comunidades vulnerables.

4. **Responsabilidad de plataformas**

- Se discutió ampliamente el rol de Telegram. Los panelistas señalaron que, aunque la plataforma se presenta como un espacio de privacidad y anonimato, estas características facilitan la coordinación de mercados de datos ilegales y distintos tipos de violencia digital.
- Se subrayó que no existe una respuesta efectiva por parte de la plataforma: no ofrece mecanismos rápidos de denuncia, no coopera de manera sistemática con las autoridades y no actúa de manera proactiva para detectar o bloquear grupos dedicados a la venta ilegal de datos.

5. **Casos nacionales**

- Brasil: Se describió un contexto de alta digitalización estatal, lo que también amplifica riesgos asociados a la integración de grandes bases de datos públicas. El principal desafío no es normativo, sino de implementación: falta de coordinación entre agencias, recursos limitados para prevención y grandes diferencias de capacidad entre los más de 5.500 municipios del país.
- Perú: La autoridad peruana informó que, solo este año, se han iniciado 25 procedimientos sancionadores contra entidades públicas por no contar con medidas de seguridad adecuadas. Se explicó el caso del RENIEC, cuya base de datos es consultada por diversas entidades que no poseen controles mínimos: no hay trazabilidad de accesos, no hay privilegios diferenciados, y muchas filtraciones provienen de usuarios válidos dentro de esas instituciones. Se destacó además que la autoridad carece del presupuesto y personal necesario para fiscalizar de manera suficiente, y que las plataformas no brindan una colaboración efectiva cuando se requiere información o bloqueo de grupos.
- Argentina: El informe presentado por la moderación muestra que los problemas son similares: brechas en implementación normativa, falta de capacidades técnicas y debilidades en seguridad de la información en entidades públicas.
- Regional: Los panelistas resaltaron que el mercado gris de datos, utilizado también por firmas de ciberseguridad para análisis de amenazas, genera desigualdad: las

organizaciones con recursos pueden protegerse mejor, mientras que personas naturales y entidades más pequeñas no tienen acceso a esa información.

6. Aportes de los panelistas.

- Las y los panelistas coincidieron en que el fenómeno requiere un abordaje integral que trascienda las respuestas aisladas. Se subrayó la necesidad de avanzar hacia mecanismos estables de coordinación regional, dada la naturaleza transnacional del mercado ilegal de datos y la velocidad con la que se desplazan los contenidos entre plataformas.
- También se planteó que la trazabilidad de accesos y la identificación de incidentes deben convertirse en estándares mínimos para todas las entidades públicas, sin excepción.
- Se insistió en que cualquier estrategia debe reconocer que las vulnerabilidades no se distribuyen de manera uniforme, y que los impactos diferenciados sobre mujeres, niñas y personas LGBTIQ+ obligan a incorporar un enfoque interseccional en el diseño de políticas, en la formulación de protocolos y en los sistemas de denuncia. En este sentido, se remarcó que las plataformas tecnológicas deben asumir obligaciones claras de transparencia, tiempos de respuesta verificables y cooperación efectiva durante las investigaciones.
- Otro aporte destacado fue la importancia de fortalecer la capacidad investigativa estatal, no solo en protección de datos, sino también en ciberseguridad y persecución penal. Se mencionó que la mayoría de las filtraciones documentadas provienen de entidades públicas, por lo que resulta indispensable mejorar los controles de acceso, las auditorías internas y la supervisión de personal con privilegios de consulta.
- Finalmente, se planteó que las futuras políticas públicas deberán integrar, de manera articulada, la protección de datos, la seguridad digital y la prevención de violencias en entornos sociotécnicos. Esto incluye avanzar hacia esquemas de colaboración estructurados con plataformas, agencias de seguridad digital, fiscalías y autoridades de datos, así como asegurar los recursos y capacidades necesarios para su implementación sostenida.

Preguntas del Público:

Pregunta 1. Consulta cómo balancear la protección de datos con la innovación (IA, datos abiertos) y cómo las leyes de protección pueden dificultar la lucha contra delitos como la extorsión.

Pregunta 2. Pregunta sobre la necesidad de voluntad política y recursos para fiscalías, y si se tiene "poder real" para presionar a plataformas globales.

Respuesta de Olga Escudero: Responde a la primera pregunta, indicando que la protección de datos es un derecho fundamental y que la innovación debe hacerse de manera ética y con consentimiento, no a expensas de los derechos

Respuesta de Paloma Lara Castro: Responde a la primera pregunta, aseverando que la protección de derechos humanos debe estar *por encima* de la innovación.

Respuesta de Iagê Miola: Responde a la segunda pregunta, explica que en Brasil, las plataformas deben tener representación local. Afirma que la agencia de datos brasileña ha fiscalizado y aplicado medidas cautelares a plataformas globales, y estas decisiones han sido mantenidas en el poder judicial