Resumen ejecutivo: Diálogo sobre protección de datos personales desde una perspectiva de género

Introducción

Este resumen ejecutivo presenta los puntos clave del diálogo virtual "Protección de datos personales desde una perspectiva de género: difusión no consentida de material íntimo y *doxing*", organizado por la Asociación por los Derechos Civiles (ADC) con el apoyo de la Embajada Británica en Argentina el 27 de febrero de 2025. Cabe señalar que las ideas y conclusiones aquí presentadas emanan directamente de las discusiones y aportes de los y las participantes en la jornada, y no necesariamente reflejan las opiniones de la ADC ni de la Embajada Británica.

El evento reunió a especialistas de diversos sectores en un espacio de intercambio seguro y respetuoso. Su objetivo principal fue analizar las barreras para la aplicación efectiva de las normativas de protección de datos y su interrelación con las leyes contra la violencia digital y de género, con un enfoque específico en el *doxing* y la difusión no consentida de material íntimo. Se buscó no solo comprender en profundidad estas problemáticas, sino también compartir experiencias y perspectivas, e identificar estrategias para superarlas. Además, se exploraron formas de mejorar la coordinación entre actores clave, fomentando el debate en un contexto de disminución de políticas públicas en general, particularmente desafiante para las cuestiones de género y disidencias.

Panorama normativo y legal

Uno de los aspectos destacados es que la Ley N° 25.326 de Protección de Datos Personales, sancionada en el año 2000, ha quedado desactualizada frente a la acelerada transformación digital. Esta normativa no contempla de manera explícita el tratamiento de datos en entornos digitales ni las problemáticas derivadas del uso de tecnologías emergentes, ya que su enfoque se limita a la regulación de bases de

datos, en contraste con legislaciones más modernas que colocan a las personas en el centro de la protección. A pesar de estas limitaciones, Argentina revalidó recientemente su adecuación con la Unión Europea y ratificó el Convenio 108+, cuya próxima entrada en vigor contribuirá a elevar los estándares en la materia.

La normativa vigente tampoco aborda de manera integral las afectaciones a la protección de datos personales que pueden constituir formas de violencia de género facilitada por tecnología. Casos como la difusión no consentida de material íntimo, el *doxing* y otras prácticas expuestas durante el diálogo evidencian cómo la recopilación, exposición y uso indebido de datos personales pueden ser empleados para ejercer control, coerción y daño, afectando de manera desproporcionada a mujeres y diversidades. Aunque la Agencia de Acceso a la Información Pública, autoridad de aplicación de la Ley de Protección de Datos Personales, ha intensificado esfuerzos para asesorar a la ciudadanía sobre mecanismos de denuncia y términos de uso de las plataformas digitales, carece de atribuciones y herramientas específicas para intervenir formalmente en estos casos. Asimismo, la falta de disposiciones sobre extraterritorialidad restringe la capacidad de actuar frente a responsables ubicados fuera del territorio argentino, como las plataformas digitales. Se estima que entre un 10% y un 20% de las consultas diarias recibidas están vinculadas con estas problemáticas, lo que refleja la creciente necesidad de herramientas efectivas para abordar estos casos.

En este contexto, la sanción de la llamada Ley Olimpia en 2023 representó un avance significativo. Al modificar la Ley N° 26.485 de Protección Integral para prevenir, sancionar y erradicar la violencia contra las mujeres, incorporó un reconocimiento explícito de la violencia digital como una forma de violencia de género y estableció medidas para su abordaje. La Ley Olimpia sí contempla cómo el uso indebido de información personal puede convertirse en una herramienta de agresión y control, lo que amplía el marco normativo disponible para enfrentar estos casos. Sin embargo, la aplicación de esta normativa enfrenta serios desafíos como la falta de recursos, el desmantelamiento de políticas públicas en la materia y la ausencia de herramientas efectivas para garantizar el cumplimiento de las medidas judiciales. En este sentido, aparece una consecuente preocupación por la capacidad del sistema para recibir y atender denuncias de manera adecuada.

Otro punto destacado es que, si bien los códigos nacionales Civil y Penal aún no han incorporado plenamente el reconocimiento de las nuevas realidades derivadas del entorno y las tecnologías digitales, siguen siendo marcos legales para brindar asistencia a las víctimas y regular las relaciones con las plataformas.

En el intercambio resultó evidente una persistente necesidad de impulsar reformas legales y alcanzar criterios comunes mediante estrategias sostenidas de incidencia y promoción, construyendo consensos y promoviendo acciones de largo plazo. Al mismo tiempo, se identificaron medidas clave que pueden abordarse en el corto y mediano plazo, como el fortalecimiento de los servicios de asistencia con enfoques basados en evidencia y centrados en las sobrevivientes, así como la generación de evidencia e información más precisos sobre estas problemáticas. Estas acciones permitirían desarrollar recomendaciones concretas para responder de manera más efectiva a la problemática.

Obstáculos y Necesidades del Sistema Judicial

Durante el intercambio, se destacó que las afectaciones a la privacidad, la protección de datos y otras formas de violencia de género facilitadas por las tecnologías presentan desafíos significativos para el sistema judicial. A pesar de algunas excepciones positivas, persisten obstáculos críticos, particularmente en lo que respecta a la investigación, persecución, sanción y reparación de estos delitos. La falta de herramientas especializadas y la insuficiente sensibilización y capacitación de jueces, fiscales y operadores judiciales siguen siendo barreras importantes, limitando el acceso efectivo a la justicia y aumentando el riesgo de revictimización, lo que perpetúa la impunidad.

En este escenario se vislumbra la necesidad de fortalecer el reconocimiento del *doxing* y la difusión no consentida de contenido íntimo y otras agresiones digitales para evitar la desestimación de denuncias. Esto no solo contribuiría a reducir la minimización de estos casos, sino también a garantizar un acceso más ágil y adecuado a la justicia para las víctimas.

Asimismo, el acceso a pruebas en entornos digitales sigue siendo un obstáculo crítico para la investigación y sanción de estos delitos. En muchos casos, los exhortos

judiciales a plataformas como Google, Meta o X enfrentan demoras excesivas, lo que dificulta la obtención de evidencia clave y puede llevar al archivo de las denuncias. Sin embargo, la dificultad en la obtención de información por parte de estas empresas no puede justificar el renunciamiento de la administración de justicia a su deber de investigar los hechos.

Por otro lado, la publicidad de las sentencias en estos casos también supone un desafío en sí mismo para proteger la privacidad y la información personal de las denunciantes. Es esencial implementar herramientas tecnológicas y/o pautas internas que permitan anonimizar los datos sensibles en los fallos, de modo que la identidad de las víctimas quede resguardada. Además, se debe fortalecer el derecho de las denunciantes a decidir sobre la difusión de su información personal, garantizando el respeto de su privacidad a lo largo de todo el proceso judicial. La adopción de estándares como las Reglas de Heredia y el uso de software especializado, como AymurAI, puede resultar clave para salvaguardar estos datos sin comprometer la transparencia judicial.

La ausencia de protocolos judiciales específicos impide una respuesta ágil y efectiva del sistema de justicia. La creación de herramientas y recursos especializados para la recepción, tramitación e investigación de estas denuncias es clave para evitar la revictimización y reducir los niveles de impunidad.

Coordinación Multisectorial e Interinstitucional

A partir del diálogo surge que la respuesta ante estas problemáticas generalmente aparece fragmentada y carente de estrategias integrales. La falta de articulación interinstitucional limita el acceso de las víctimas a los recursos adecuados, lo que, en muchos casos, puede generar situaciones de revictimización e impunidad. En este sentido, aparece como fundamental la creación y el fortalecimiento de redes de trabajo y alianzas estratégicas, capaces de lograr acuerdos interinstitucionales con impacto.

Se destacó la formación de una alianza multisectorial para implementar acciones concretas, como protocolos interinstitucionales de intervención rápida y

herramientas para facilitar la retirada de contenidos, tanto antes como durante la intervención judicial. Fortalecer la colaboración entre el sector público, la sociedad civil y las empresas tecnológicas es clave para desarrollar mecanismos efectivos de protección, como canales de atención rápida y procedimientos expeditos para la eliminación de contenido sensible o abusivo. Modelos como StopNCII, Take It Down y el Canal Prioritario de la Agencia de Protección de datos española podrían servir como referencia para el despliegue de soluciones adaptadas a contextos locales.

Por otro lado, también se subrayó la necesidad de replantear el enfoque punitivo, reservando el derecho penal como último recurso. Si bien la probation se utiliza con frecuencia, esta herramienta no siempre garantiza la asunción de responsabilidad por parte del agresor, particularmente en el ámbito de las contravenciones, donde persiste una falta de mecanismos adecuados para la reparación del daño a las víctimas. Las reparaciones siguen siendo principalmente simbólicas, y las barreras culturales y de poder continúan presentes.

Finalmente, se reconoció la importancia del diálogo multisectorial para identificar puntos de conflicto y construir consensos, pero también se destacó la necesidad de avanzar hacia la implementación efectiva de soluciones. Para ello, se propone establecer agendas específicas con objetivos y niveles de esfuerzo diferenciados, así como articular los esfuerzos locales con los espacios globales y regionales de gobernanza de Internet y de derechos humanos, promoviendo consensos multisectoriales y fortaleciendo la cooperación internacional.

Concientización y sensibilización

El diálogo puso de manifiesto la necesidad de fortalecer las campañas de sensibilización y los programas educativos para fomentar una cultura de respeto en línea. Se hizo especial hincapié en la importancia de dirigir estas iniciativas a jóvenes, adolescentes y varones como agentes de cambio.

En este sentido, se coincidió en la necesidad de integrar contenidos sobre seguridad digital, consentimiento y derechos en entornos digitales dentro de la Educación Sexual Integral (ESI). Asimismo, se destacó la importancia de generar

espacios de reflexión sobre las pautas de convivencia digital y concientizar sobre los daños que puede ocasionar las violaciones a la privacidad de datos y otras formas de violencia facilitadas por las tecnologías.

Otro punto clave es el desarrollo de herramientas que faciliten la identificación y prevención de riesgos. Se señaló la necesidad de realizar campañas de concientización y difusión que brindan estrategias de cuidado y mitigación de riesgos, ya que se reconoció la desinformación existente sobre cómo actuar frente a estas situaciones. Esta falta de información contribuye a la normalización de conductas violentas y dificulta su prevención.

Finalmente, se enfatizó que estos esfuerzos deben ir acompañados de un trabajo continuo para transformar los patrones culturales, las estructuras sociales y económicas, y los sistemas de poder que perpetúan la opresión.

Consideraciones finales

Resulta oportuno subrayar que advertimos, la privacidad y protección de datos en este contexto plantea desafíos específicos que requieren un enfoque de género. Las mujeres y diversidades enfrentan formas particulares de violencia digital, como la divulgación no consensuada de imágenes íntimas o el acoso en línea, que vulneran su privacidad y seguridad de manera diferenciada. Encontramos que la intersección entre la privacidad y la protección de datos y el enfoque de género puede generar una interacción positiva, propiciando respuestas más efectivas e integrales que aborden de manera completa las diversas manifestaciones de la violencia de género digital.

Esperamos que este resumen sea útil para dar cuenta del estado actual de la situación y seguimiento a las discusiones. Reconocemos que este es solo un punto de partida y confiamos en que este documento sirva como base para la construcción de estrategias conjuntas, la identificación de oportunidades de colaboración y la exploración de posibles alianzas.

***