SITUACIONES DE INSEGURIDAD Y SUS CONSECUENCIAS

Los espacios digitales fueron creados y desarrollados con el objetivo de crear puentes de comunicación e información, y para expandir el alcance de todo tipo de realidades a nivel global. Ya es posible acceder a una variedad de información que antes no estaba a nuestro alcance, y lo mismo con oportunidades de educación a distancia. Hay espacios que albergan comunidades para discutir sobre distintos temas, y sí que sirven para fortalecer nexos y acciones de activismo. También sirven mucho cuando nos encontramos en una fase de transición a la hora de encontrar nuestra identidad y lugar en el mundo.

Habitar espacios digitales nos ayuda a crear visibilidad sobre ciertos asuntos, y a empoderarnos cuando encontramos apoyo y empatía. Podemos encontrar espacios en los que hallamos sinergia para elaborar acciones de manera colectiva y colaborativa, las cuales hoy en día, dentro de este ecosistema, se pueden dar a conocer como acciones conectivas.

A pesar de esto, también existen dinámicas que nos dañan. Fenómenos y amenazas como el ciber-acoso, el discurso de odio y el chantaje, violan el derecho de las mujeres a la privacidad, el trabajo, la participación pública, la libertad de expresión y opinión, así como el riesgo a la exposición no consentida y muchos otros tipos de situaciones.

Identificando amenazas digitales

Para entender mejor o dimensionar qué amenazas o situaciones pueden ocurrir a la hora de habitar espacios digitales, es importante identificarlos. A continuación, te proveemos unos ejemplos de los tipos de ataques digitales más comunes elaborados por ***GenderIT***:

● Acceso y control/manejo no autorizado de cuentas: Ataques no autorizados para ganar acceso a las cuentas o dispositivos de otros. Esto puede implicar que información no autorizada se junte, y/o el bloqueo de acceso a la cuenta a la persona dueña de la cuenta misma.

● Control y manipulación de la información: La junta o robo de información puede implicar una pérdida de control de la información en sí, y también la modificación de la misma sin autorización.

● Difusión de fotos íntimas o información privada: Compartir de manera no autorizada cualquier tipo de información, datos o detalles privados relacionados a una persona.

● Doxeo: Investigar y difundir información identificable sobre una persona sin su consentimiento, muchas veces con la intención de tener acceso o contacto con la persona con fines de acoso u otros fines nocivos.

● Vigilancia: El monitoreo constante de las actividades de la persona, su vida diaria, o información, sea pública o privada, pertinente a la persona o a la organización.

● Uso de spyware (software para espiar y obtener información de otros dispositivos) o acceso a cuentas sin el consentimiento del usuario.

● Uso de GPS u otros servicios de geolocalización para rastreo de movimientos.

● Robo de identidad/creación de perfiles falsos: El uso de la identidad de alguien sin su consentimiento, o la creación y compartición de datos personales falsos, con la intención de dañar la reputación de la persona o de la organización.

● Borrar, enviar y/o manipular correos y/o contenido sin consentimiento.

● Distorsión de imágenes o videos, u otro tipo de manipulación de contenido falso: Elaborar contenido falso, manipulado o sacarlo de contexto, y compartirlo con el fin de desprestigiar y dañar a una persona o grupo.

● Diseminar información privada (o sensible/controversial culturalmente) con la intención de dañar la reputación.

● Difamación y daño de la reputación a través de comentarios online falsos y ofensivos.

● Acoso: Actos repetidos y no solicitados contra una persona u organización que son percibidos como intrusivos o amenazadores.

● Ciber bullying y acoso repetido a través de mensajes no deseados, atención y contacto.

● Discurso de odio: Discurso que refleja modelos culturales que incitan violencia, ya sea a través de comentarios, insultos, o agresiones verbales.

● Amenazas: Discurso y contenido (verbal o escrito, en imágenes, etc) con un tono agresivo y/o amenazador.

Amenazas directas de violencia de cualquier índole.

● Comentarios abusivos.

● Envío y recepción de materiales sexuales no solicitados.

● Extorsión: Forzar a una persona a actuar de acuerdo a la voluntad de otra persona, a través de amenazas e intimidación.

● ***Mobbing:*** incluyendo tanto a una persona como a un grupo en sí.

● Hackeo de cuentas y dispositivos.

● ***Ataques coordinados:*** Son aquellos ataques que se realizan de manera coordinada y por más de una persona hacia otra, una publicación específica o una página en las redes. Los fines de estos ataques pueden ser varios: difusión de datos personales para causar hostigamiento y acoso, o incluso lograr la eliminación de los perfiles de las víctimas, crear identidades falsas para así poder esparcir publicaciones y noticias falsas.

¿Qué consecuencias tienen que las mujeres pasen por estas situaciones?

Estas situaciones de amenazas pueden provocar que las mujeres se autocensuren y que se abstengan de hablar libremente. Como consecuencia, hay una restricción de la capacidad de presencia y de ser parte de los diversos movimientos y comunidades de activismo. En otras palabras, estas situaciones limitan el grado de participación de las mujeres en debates de interés público, proceso de toma de decisiones, y perpetúa la misma manera en la que se construyen los espacios de ciudadanía digital: ***en base a la exclusión de las mujeres y otros grupos minoritarios.***

En un entorno de tal complejidad, las actividades que desarrollamos (en línea y fuera de Internet), nuestras identidades y realidades pueden parecer separadas, pero resultan estar, la mayoría de las veces, profundamente entrelazadas. Por todo eso, puede darse un alto nivel de confusión o incertidumbre acerca de las intenciones, identidades y acciones de los demás en los espacios digitales. Como resultado, todo eso puede llevarnos a la ansiedad o al deseo de retirarnos de cualquier espacio o tipo de actividad en caso de haber sido víctima de alguna situación de amenaza e inseguridad.

Existe más de una dimensión a la hora de hablar de las posibles consecuencias y el impacto de ser víctimas de estas situaciones de ***violencia digital:***

• Impacto físico: Sudoración, dolor en distintas partes del cuerpo (cabeza, espalda, estómago), pérdida o exceso de apetito, tensión, llanto, angustia.

• Impacto emocional: Estrés, angustia, ira, enojo, miedo, impotencia, frustración, depresión, paranoia, cansancio y confusión.

• Impactos varios: Temor a salir y exponerse, auto-limitación de movilidad, abandono de uso de las tecnologías, autocensura, sensación de constante monitoreo y vigilancia.

Lecturas para profundizar

- 13 manifestations of gender based violence using technology, por Take back the tech!, Luchadoras and SocialTic. 2018
- ¿Cuáles son las principales modalidades de violencia de género en línea?

BIO.

TEDIC

Es una organización sin fines de lucro creada en Paraguay por personas con trayectorias en diferentes disciplinas, que promociona y defiende los derechos digitales en América Latina. Buscamos el cumplimiento pleno de los derechos civiles en Internet. Investigamos, difundimos información y capacitamos en temas de privacidad, datos personales, ciberseguridad: cuidados digitales, libertad de expresión y manifestación, neutralidad en la red, derechos de autor, inteligencia artificial, biometría, entre otros, con un enfoque transversal de género.