Buenos dias/Buenas tardes, muchas gracias por darme la palabra.

Es un honor para mi poder compartir con ustedes, distinguidos panelistas y distinguidos miembros de delegaciones, la experiencia de la República Argentina en materia de prevención del delito cibernético.

Seguramente todos nosotros coincidiremos en notar el constante crecimiento del cibercrimen en nuestros países. La mayor penetración de internet en el mundo, y el desarrollo constante de la tecnología que facilita nuestras conexiones son aprovechados no sólo para garantizar derechos como el acceso a la información, la libertad de expresión y la igualdad de género sino también, lamentablemente, por las organizaciones criminales para extender sus operaciones.

Durante estos casi 7 años en la Unidad Fiscal Especializada en Ciberdelincuencia UFECI- de la Procuración General de la Nación Argentina, nuestro equipo se ha dedicado no sólo a investigar casos, capacitar a miembros de los organismos de aplicación de la ley y potenciar nuestras actividades fomentando, por ejemplo, una mejor y más amplia cooperación entre diversos actores nacionales e internacionales, públicos y privados sino que, también, ha aprovechado la rica información que proporciona el contacto con cada víctima no sólo para conocer cuáles son las principales modalidades delictivas sino también para intentar determinar qué aspectos de la actividad estatal pueden mejorarse para contrarrestar las actividades ilícitas en internet.

La principal conclusión que pudimos extraer de esa interacción fue que la mayoría de los usuarios de internet de nuestro país no están lo suficientemente preparados para utilizar la tecnología de forma segura. Si bien esas mismas personas adoptan

una serie de cuidados básicos en su vida diaria, en especial con su vivienda, objetos de valor y durante sus interacciones personales, no hacen lo mismo cuando utilizan internet: cuidado de la privacidad, uso de contraseñas robustas y conexiones seguras, activación de la verificación en dos pasos, etcétera no parecen ser prioridades para nuestros ciudadanos.

Esto, desde luego, facilita mucho la acción de los criminales. A modo de ejemplo, de los más de 5000 reportes que hemos recibido durante los meses de aislamiento preventivo por la pandemia del covid19, aproximadamente el 35% corresponden a accesos indebidos a cuentas de correo, billeteras electrónicas y plataformas de redes sociales. Estos casos podrían haberse evitado, o reducido sustancialmente, si los usuarios hubiesen estado al tanto de la existencia de maniobras de phishing o captación engañosa de datos, usado buenas contraseñas y activado el segundo factor de autenticación.

Basados en toda la información recolectada, desde nuestra unidad venimos desarrollando hace años una serie de acciones tendientes a mitigar esta situación:

1. Alertamos a la comunidad por medios de prensa y redes sociales sobre las principales maniobras delictivas (desde los ataques a la propiedad como el ransomware y el phishing, hasta los ataques a la intimidad y a la libertad individual, como la sextorsión, la pornovenganza, la pornografía infantil y el grooming), indicándoles cuales son los cuidados que deberían adoptar pero, además, proporcionándoles las vías de comunicación con las autoridades policiales para el caso que quieran formalizar una denuncia.

2. Desarrollamos programas de capacitación orientados al ciudadano, focalizándonos principalmente en niños, niñas y adolescentes, educadores, adultos mayores, y otras comunidades vulnerables

3. Generamos alianzas estratégicas con otros organismos del estado como la Dirección Nacional de Protección de Datos Personales y el Centro de Ciberseguridad de la Ciudad de Buenos Aires para llevar nuestro mensaje a más personas aún.

Pero lo nuestro es sólo un pequeño aporte, que consideramos que no es lo suficientemente efectivo para un país tan extenso, con tanta población y con un sistema de organización política federal.
Es necesario el desarrollo de una serie de políticas públicas a largo plazo, algunas de las cuales empiezan a gestarse, como una reciente campaña nacional contra el grooming -iniciativa del Ministerio de Educación- de la que tuvimos el honor de participar.
Desde nuestro punto de vista, esas políticas públicas deben incluir el desarrollo de campañas de difusión masiva sobre el uso seguro de internet que incluyan la posibilidad de acceder a recursos informativos por parte de los ciudadanos. Deberían, además, incluir en los programas educativos cursos sobre nociones básicas de seguridad informática dirigidos no sólo a estudiantes sino también a docentes.

Estas políticas públicas tendrían que estar, idealmente, en un marco más general: una estrategia nacional de ciberseguridad.
Hemos visto muy buenas experiencias en otros países del mundo y el nuestro ha empezado a transitar ese camino desde hace un tiempo.

Consideramos que es necesario no abandonar esa senda, ya que nuestra experiencia de trabajo nos ha permitido concluir lo que parece evidente: cuanta mayor información tenga el usuario de internet, más seguro será el uso que haga de la red, menor será el desarrollo del ciberdelito y, fundamentalmente, mayor será la promoción de derechos fundamentales.

Muchas gracias.