COMPARECENCIA DEL DIRECTOR DE TECNOLOGÍA DE MICROSOFT IBÉRICA, D. HÉCTOR SÁNCHEZ MONTENEGRO, EN LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES CELEBRADA EL DÍA 24 DE FEBRERO DE 2014

El señor **DIRECTOR DE TECNOLOGÍA DE MICROSOFT IBÉRICA** (Sánchez Montenegro): Muy bien, muy amable, muchas gracias. Yo creo que es de buena educación, primero, presentarse. Soy el director de Tecnología de Microsoft Ibérica; he sido anteriormente el director de Seguridad, de Microsoft también, llevo –ayer hice– 14 años en la compañía; anteriormente he estado trabajando en empresas españolas como DINSA, Banesto, Level Data, incluso en el INI; soy licenciado en Físicas por la Universidad Autónoma de Madrid. Y este tema, yo creo que nos toca, además ya no solo a nivel profesional; soy padre de tres menores, con lo cual, muchas veces andamos poniéndonos y quitándonos los gorros según corresponda.

Entonces, yo quisiera empezar esta exposición agradeciendo sinceramente la invitación que desde esta comisión conjunta del Senado han cursado a la compañía que represento, Microsoft Ibérica; es para nosotros un gran honor ser convocados en este foro, y para mí en particular, siempre lo es, es la cuarta ocasión en la que tengo el privilegio de exponer ante señorías de algunas de las cámaras sobre temáticas de diferentes ámbitos. Y en esta ocasión, sobre un terreno muy específico de la ciberseguridad como es la seguridad de los menores en Internet.

Y creo que es un acierto la preocupación y la ocupación de sus señorías por este asunto. Creo que es oportuno, es necesario, es importante, y es un asunto sobre el que sin lugar a dudas hay que reflexionar porque es y seguirá siendo de importancia durante mucho tiempo.

La ciberseguridad resulta más importante que nunca y plantea un campo de batalla del que todos formamos parte de forma activa o pasiva, incluidos nuestros menores; y es necesario conocer cuál es ese marco en el cual todo esto ocurre. No en vano acabamos de publicar como país la Estrategia de Ciberseguridad Nacional, posicionando al nivel de importancia que corresponde el ámbito de la tecnología y la seguridad en Internet, hasta el punto de incluso considerarlo en el ámbito militar como un mando más, Mando de Ciberseguridad, que se une a los tradicionales de Tierra, Mar y Aire. O en el ámbito civil, la ciberseguridad es también un área prioritaria respecto a la protección ciudadana, protección de empresas, protección de infraestructuras críticas.

De hecho, los centros de respuesta a incidentes en Internet en España, los denominados CERT, parecen tener últimamente más protagonismo del que han tenido hasta la fecha, tanto los CERT de ámbito público como el CCN-CERT, el organismo adscrito al CNI y dirigido a la protección de las infraestructuras tecnológicas de la Administración Central del Estado, pasando por INTECO-CERT, dirigido a empresas, CNPIC-CERT, dirigido a infraestructuras críticas desde el Ministerio del Interior, Red Iris, el próximo CERT que están montando desde el Mando de Ciberseguridad, etc.; así como un largo etcétera de CERT autonómicos, incluso CERT de grandes empresas en el sector privado. Actualmente, yo creo que no me equivocaría si dijera que en España podemos llegar, a lo mejor, a 10, 12, 14 CERT.

Lo cual forma parte realmente de nuestro panorama en materia de seguridad a nivel público; no sé si a veces puede ser un problema la coordinación de estos centros, duplicidad de esfuerzos, pero puede ser otro ámbito de discusión, ¿no?

Quería aproximarme paulatinamente al ámbito de estudio de la ponencia sobre la que ustedes trabajan comenzando por la absoluta

disrupción tecnológica, en primer lugar, que nos rodea. Es por ello por lo que he decidido estructurar esta exposición en dos partes claramente diferenciables pero muy relacionadas entre sí. Un primer apartado dedicado a la importancia de la tecnología, la innovación, los contenidos, los servicios a través de la red, incluyendo nuevas realidades que afectan a este escenario, como es el *cloud computing* (computación en la nube), que aunque no es el objeto específico de esta ponencia, lo sería sin duda de otra, tenemos que considerar que la computación en la nube forma parte protagonista de la revolución tecnológica que nuestra sociedad y sus menores experimentan a su alrededor.

A continuación incidiré en el ámbito de la ciberseguridad como nueva circunstancias, hasta llegar al paso particular de la seguridad en menores, cuya problemática no es sencilla de visualizar en profundidad sin entender el escenario global que como sociedad, incluyendo a esos menores, estamos construyendo y al que nos estamos dirigiendo.

A estas alturas, creo que queda claro que la tecnología no es una moda, no es un capricho, no es un esnobismo. Es más, creo que todo contrario, me atrevería a decir que, a diferencia de la realidad de hace unos diez o quince años, cualquier actitud personal o corporativa que en la realidad se resistiera a la tecnología, paradójicamente tendría más posibilidades de ser calificado de esnob; o sea, realmente forma parte de nuestro día a día.

Llevamos tanto tiempo hablando también en Internet en el capítulo de nuevas tecnologías, que realmente nos preguntamos cuál es el periodo de caducidad ya del adjetivo “nuevas”; esto ya no es nuevo.

Por tanto, no es mi propósito compartir con sus señorías obviedades sobre lo importante que es la red de redes, la importancia de su existencia, de su libertad, de su crecimiento, de las oportunidades que de forma democrática se ofrecen a cualquiera de sus usuarios, el acceso a la

información, los servicios, y un largo etcétera de beneficios tan evidentes como importantes, que no en vano en algunos países como Finlandia el acceso a la red se ha llegado a convertir en un derecho constitucional.

Pero es cierto que nuestras expectativas sobre el uso inteligente de la tecnología crecen, y de hecho pedimos con frecuencia que las políticas públicas sean favorables a un proceso de innovación tecnológica que:

uno, mejore la inclusión ciudadana, transparencia y confianza y colaboración en la administración como parte de un gobierno más abierto;

dos, estimule la competitividad, la creación de empleo cualificado y el crecimiento sostenible a través de *clusters* económicos que den fundamento a esas grandes apuestas que como nación decidamos como prioritarias;

tres, incremente los usos y alcances de los servicios de la administración electrónica fortaleciendo adicionalmente requisitos esenciales como aquellos relacionados con la sanidad, la educación o la seguridad pública;

cuatro, mejore la colaboración entre las administraciones públicas redundando en un mejor servicio al ciudadano, desde la interoperabilidad, seguridad y privacidad de datos y sistemas;

y cinco, incluso proteja el medio ambiente mediante un crecimiento sostenible.

Las inversiones tecnológicas resultan imprescindibles para tales cometidos. Y muy especialmente en un momento en el que adicionalmente queremos reequilibrar nuestro modelo productivo a favor de propuestas basadas en la innovación y en la tecnología. En efecto, la tecnología debe ser el vehículo principal que impulse dicho cambio.

Dicho esto, me gustaría compartir el siguiente contenido. Existen determinadas compañías que en un momento dado de la historia tienen la capacidad, por su predominancia, por su prevalencia, de visualizar, de

visionar cuál puede ser el futuro más inmediato en base a las experimentaciones propias y ajenas que pueden estar percibiendo a su alrededor. Es el caso, por ejemplo, en los años noventa, de una de esas compañías, que era AT&T. AT&T era una compañía con esa capacidad de visionado. Hicieron público un vídeo –que les voy a poner a continuación, muy cortito, AT&T Vídeo pongo por aquí–, que realmente lo que intentaban hacernos en el año 1993 es aventurar lo que en aquel entonces sería ciencia ficción de lo que iba a ser el mundo de la tecnología tan solo diez años después.

Vamos a verlo, y no sé si compartirán el sentimiento que yo tengo cuando veo esto, que me resulta hasta entrañable, de lo que en aquel entonces era ciencia ficción, en qué estado está ahora cuando lo vemos unos cuantos años después.

[VÍDEO]

Por lo menos resulta un poquito chocante lo que en aquel entonces... y cómo somos capaces de ir incorporando tecnologías sin apenas darnos cuenta, y visiones futuristas como esa, ahora resultan hasta entrañables en ese sentido.

Voy a poner un minuto de... en este momento vamos a asomarnos, es decir, una de las compañías, de las muchas compañías, no es la única, pero de las compañías que tienen ahora mismo esa capacidad de poder visionar qué puede ser ese mismo futuro dentro de los próximos diez años, pues es Microsoft. Hay otras, pero una de ellas es Microsoft. Y no solo en base a la tecnología que desarrolle Microsoft, sino a lo que Microsoft ve que se está haciendo en universidades, que están haciendo nuestros competidores; cuál puede ser el mundo de la tecnología y el mundo de la sociedad dentro de diez años. Es como que abramos una ventana al futuro, una ventana al futuro que a lo mejor dentro de cinco años visionamos este vídeo y nos parece igual de entrañable que nos ha parecido el de AT&T. Con lo cual,

creo que es interesante simplemente para ver cuál es el mundo al que vamos y los riesgos que realmente podemos estar experimentando también.

[VÍDEO]

Dispositivos inteligentes, hasta el cristal del taxi es un dispositivo inteligente que me está dando información de contexto. No se visualiza, pero aquí hay una computación en la nube brutal; cualquier dispositivo, una mesa de cristal, está leyendo datos de otro sitio; es decir, cuando se habla de *cloud computing*, es el futuro, y no se trata solo de acceder a cuatro servidores en la red, es que realmente estamos hablando de la computación que es ubicua, realmente en cualquier sitio eres susceptible de acceder, eres tú además el dueño de esa computación que se produce a tu alrededor. En tu contexto. El vídeo dura seis minutos, lo tienen en la presentación. No es mi intención... Quiero llevarles cuando antes a la temática que nos ocupa, pero sí me parecía imprescindible saber el porqué de las cosas que ocurren ahora en cuanto a una tecnificación absoluta, porque es que esto es lo que estamos visionando, estamos visualizando cómo va a ser nuestra sociedad dentro de no demasiados años.

Si les parece, lo voy a dejar aquí. Pero espero haber despertado su curiosidad para que puedan verlo completo, porque es un ejercicio que yo creo interesante.

Bien, esa es la realidad –lo que les comentaba– que debemos visualizar, esa ventana por la que nos hemos asomado nos muestra un futuro muy inmediato, absolutamente basado en tecnología, en tecnología implícita o embebida en la situación, pero que cimentará la forma de vivir en los próximos diez años. Y debemos preparar a nuestra sociedad, y en especial a nuestros hoy menores, para que no solo saquen partido de esa revolución, sino para que además la entiendan y la lideren.

Ojalá la regulación necesaria en todos los aspectos avance a la velocidad que la innovación exige y consigamos disminuir ese permanente

gap que observamos en diferentes ámbitos, y que en ocasiones resulta ser un terreno abonado para actuaciones improvisadas o inseguras.

Son cinco las tendencias tecnológicas que definirán nuestra sociedad en los próximos años, y que tienen que ver:

uno, con *social media*;

dos, interfaces naturales de interacción con la tecnología (ahí no aparecido ni un solo PC, es una forma nueva de interaccionar con la tecnología);

tres, *big data*, acceso masivo a información, datos, sacar conclusiones de parámetros realmente no relacionados, desestructurados, esa es la palabra que más recoge el fenómeno del *big data*;

cuatro, *cloud computing*, lo hemos visto en cada paso;

cinco, movilidad.

Entonces, de los cinco, cuatro confluyen directamente en la problemática que esta comisión examina. De ahí incidir en lo realmente importante y acertado, que de verdad considero, de la constitución de la comisión, y además voy a ir luego a hablar al final más en detalle de este tema.

Llegado a este punto, y si ya intuimos el mundo al que nos dirigimos, y es muy probable que en nuestros propios domicilios familiares (hijos, hermanos, nietos, sobrinos) podamos chequear por nosotros mismos, sin necesidad de recurrir a eruditos estudios, que algo nuevo está pasando cuando menores desde los 9 o 10 años comienzan a manifestar su interés por el acceso a Internet desde dispositivos móviles, traspasando una barrera que es la que más les define. Mientras que generaciones anteriores hacen un uso intensivo de Internet pero como opción de *switch on*, *switch off*, es decir, lo utilizamos para algo concreto y específico, nuestros menores lo manejas desde un concepto diferente, desde la perspectiva del *always on*, viven o pretenden vivir en Internet. Por pura estadística son, en

consecuencia, aquellos colectivos que más tiempo de exposición puede tener, tanto a lo bueno como a lo malo de la red.

Los adolescentes a partir de 14 años, definen con una palabra contundente y cargada de emotividad su sentimiento en el caso de haberse visto privados de su *smartphone* durante un periodo prolongado de tiempo, semanas o meses. Y esa palabra es “aislamiento”. No tienen ni que pensarlo un segundo: aislamiento, es el sentimiento que tienen cuando se sienten privados. Si bien las relaciones de verdad, obviamente, se producen en el mundo físico, el llamado mundo virtual les sirve de medio facilitador o mecanismo para favorecer la comunicación en el mundo real, no son mundos diferentes.

La ciberseguridad se ha convertido, en consecuencia, en un elemento de vital importancia, en la medida en que aumenta el uso que hacemos de Internet, y especialmente en lo que respecta a los usuarios más desprotegidos por falta de conocimientos, experiencia, derivados, lógicamente, de su corta edad, como es el caso de los menores.

Algunos han llegado incluso a establecer la relación entre la famosa jerarquía de necesidades de Marlow y los diferentes estados de ciberseguridad de una persona, obviamente en el primer mundo. Es decir, solo puedo llegar a obtener un beneficio productivo de la tecnología cuando tengo garantizadas una serie de necesidades previas, entre las que está la seguridad. Es una aproximación, como poco, curiosa, y que pongo igualmente a disposición de sus señorías si tuvieran interés en examinar ese documento; es decir, un *matching* entre toda la teoría de Marlow y la ciberseguridad. Resulta sorprendente, pero tampoco era cuestión de contarlo aquí en detalle.

Y la ciberseguridad es importante, no solo por el uso que de la red hacemos las personas y la criticidad de las interacciones y transacciones que a través de Internet se realizan; también aumenta su protagonismo en la

medida en que cada vez más dispositivos no humanos se conectan a Internet. Hablo del Internet de las cosas, de las ciudades inteligentes, de las redes inteligentes, de los sensores en entornos de *smartcities*, hasta el punto de que existen ya más dispositivos inteligentes conectados a Internet que personas, y en muchos casos manejando infraestructuras críticas.

Las enormes ventajas para la vida de los ciudadanos derivadas de vivir en un entorno de los llamados inteligentes, presentes en la evolución de nuestras ciudades (los llamados CityNext) presentan igualmente riesgos, y tenemos una enorme literatura de casos reales: algunos conocerán lo que ha ocurrido en los canales de Ámsterdam hace tres o cuatro meses, Ámsterdam es una ciudad construida por debajo del nivel del mar, la criticidad del manejo correcto de los canales es que es vital para la ciudad. Bueno, pues verse sometido realmente a la incidencia de *hackers* que realmente hicieron... es como si aquí se hubiera hackeado la fábrica de la moneda y los certificados que emite, vulnerando toda la confianza establecida en los mecanismos de seguridad y control de elementos físicos; eso ocurrió en la ciudad de Ámsterdam. Los enriquecedores de uranio de Irán, esos ataques que se hicieron vía ciberseguridad, vía ataque cibernético, para acelerar y que no pudieran producir como era deseado por ellos. Posibilidades: alterar las mezclas en potabilizadoras de agua, que puedan realmente afectar al consumo de una población.

Había traído aquí un ejemplo un poco también muy particular, sobre el manejo de infraestructuras críticas a través de Internet

[VÍDEO]

Está en un atasco; ha conectado con el sistema de control de señales de tráfico en tiempo real, con mensajes en las autopistas.

Él se lo está pasando muy bien, ¿no? Pero, obviamente, sí que la vulnerabilidad de nuestros sistemas puede ser preocupante.

Al final esto no ha tenido demasiada consecuencia, pero muchas infraestructuras críticas pueden tener un grado de vulnerabilidad similar, por eso es tan importante, efectivamente, la creación dentro del Ministerio del Interior de un CNPIC que trabaje en este ámbito.

Es decir, las cosas en materia de ciberseguridad han cambiado por cuatro o cinco factores fundamentalmente:

uno, los ataques que se reciben permanentemente que se detectan proviene de cualquier sitio, no hay que buscar lejanos lugares de Oriente,... no, no, miremos con más atención al vecino, que igual nos podríamos llevar sorpresas; pero es que además,

dos, se dirigen a cualquier objetivo, no hace falta ser un banco para ser objeto de un ataque. Son muchos los ataques dirigidos, por ejemplo, a robar la intimidad de una persona, de un menor, para posterior chantaje; o ataques dirigidos a capturar la propiedad intelectual de una industria, que sufre un ataque, que,

tres, es dirigido solo a ella, para conseguir una información determinada y no otra; son lo que se llaman los ataques persistentes avanzados, y realmente preocupan mucho a todas las fuerzas de seguridad;

cuatro, ya no se trata de *script kids*, ya no se trata de chavales detrás de un programita haciendo cualquier acción escondida detrás de una dirección IP; la ingeniería inversa sobre estos ataques demuestra la existencia de auténticos equipos profesionales de desarrollo, lo que indica la profesionalización y negocio detrás de estas actividades;

cinco, la tecnología es vulnerable, *full stop*; no existe la invulnerabilidad cien por cien, por eso es muy importante que cuando tomemos decisiones en materia tecnológica, la seguridad sea considerada en su aspecto más amplio y nos hagamos preguntas del estilo de cuáles son los criterios de desarrollo seguro del fabricante, cómo de ágiles son sus mecanismos de respuesta a incidentes de seguridad, ¿mantienen espacios

de colaboración con el sector, clientes y usuarios en materia de seguridad?, ¿mantienen una voluntad clara de ayudarme a cumplir con mis obligaciones legales en ámbitos como la seguridad y la privacidad?, etc.

Igualmente, son tres las acciones que en ciberseguridad se plantean, que son prevención, detección y respuesta. Cada una de ellas necesita de sus acciones, herramientas, inversiones, y no siempre de la mano de la tecnología.

Bien, Microsoft, y en particular Microsoft Ibérica en este caso, somos una de las compañías tradicionalmente más comprometidas con la seguridad y la protección de los menores, y que posicionaré con una sola frase: somos la única compañía tecnológica en España que luce con tremendo orgullo el haber sido condecorada por tres fuerzas policiales, como son los Mossos d'Esquadra, la Policía Nacional y la Guardia Civil, con medallas al mérito policial con distintivo blanco, y créanme sus señorías que tales distinciones son resultado de muchos años de trabajo conjunto, eficaz, de relación de socios, de alta sensibilidad mutua ante la persecución de delitos en la red. He puesto aquí algunas...

Mantenemos igualmente acuerdos de seguridad con muchos de los organismos de nuestras administraciones relacionados con la ciberseguridad, como INTECO, con el que tenemos firmados dos acuerdos, uno de los cuales es pionero en este momento a nivel internacional (es el que aparece aquí firmado por el secretario de Estado Víctor Calvo-Sotelo, este junio de 2013); con el Centro Criptológico Nacional del CNI, con quien compartimos los bienes más preciados de Microsoft como es el código fuente de los productos más importantes que desarrollamos (es más, creo que en esta imagen aparecen los últimos tres secretarios de Estado del CNI,...); CESICAT, hemos trabajado y publicado manuales conjuntamente con la Agencia Española de Protección de Datos, hasta cien empleados voluntarios de Microsoft Ibérica han colaborado codo con codo con Policía

Nacional para recorrernos más de cien colegios por toda España dando charlas a padres y alumnos; hemos colaborado con ONG como Protégeles formando a monitores y grupos *scouts* de toda España, desarrollando materiales formativos sobre seguridad infantil, y un largo etcétera.

Pero también somos conscientes de que este es un proceso que no puede detenerse, ni hay demasiado tiempo para la autosatisfacción; los riesgos evolucionan, y nuestra respuesta ha de hacerlo en la misma medida.

Visualizamos los riesgos como el de las cuatro C: riesgo en el contenido, riesgo inherente al contacto, riesgo en la conducta, riesgo en el comercio. Nuestra aproximación a esos riesgos se hace desde una triple perspectiva, tres pilares a cuál más importante y que con mayor o menor pericia hay que contemplar de forma global: educación y guías, herramientas tecnológicas, y *partnership* o colaboración.

Con respecto al primero, con respecto a la educación y guías, tenemos que tener en cuenta que el conocimiento es cambiante. En Internet es simplemente una realidad que no puede ignorarse, lo que hoy es útil, en tres meses deja de tener sentido por la aparición de nuevas herramientas, moda, aplicación, etc. Y los destinatarios de la información no solo son los menores, lo son los padres y educadores, que en muchas ocasiones están a años luz del conocimiento de sus hijos y alumnos respectivamente.

Pero existe una constante que debemos potenciar, y no es otra que la comunicación, la conversación con los menores. Es fundamental que les ayudemos a identificar aquellos parámetros sospechosos o aquellas acciones frente a las cuales siempre han de ponerse alerta. Debemos entender que, independientemente de lo que hagamos como padres, como educadores, como sociedad, llegará el momento en el que el menor se enfrente a una decisión él solo. Igual que ocurre en otros muchos ámbitos de la vida, como el consumo de drogas, alcohol, etc. Y llegado ese momento, que llegará más pronto que tarde, será muy importante haber

mantenido conversaciones abiertas y transparentes, no culpabilizadoras con el menor, y sobre todo haber conseguido crear un lazo de confianza tal que el menor no tenga reparos en consultarnos o pedirnos consejo ante una situación como esa. No es en absoluto sencillo, pero es probablemente más eficaz que otras alternativas más obstaculizadoras como la restricción de acceso. Los menores encontrarán la forma de saltarse, en un alto porcentaje, cualquier tipo de barrera, mediante dispositivos prestados, WiFi públicas, amigos, etc.

Herramientas tecnológicas: existen muchas tecnologías de control parental. Desde Microsoft proveemos herramientas de este estilo, claro que sí. Pueden llegar a ser muy útiles. También es cierto que bajo la categoría de "menor" caben actitudes, comportamientos y niveles de madurez que nada tienen que ver unos con otros: para menores hasta 10, 12 años, puede resultar útil el uso de herramientas de control parental que filtren contenidos o información; en adelante, resulta bastante más difícil implementar herramientas de esas características sin abrir debates en la familia sobre la intimidad del menor o la confianza depositada en él.

A nivel de proveedor, Microsoft ha desarrollado tecnología denominada PhotoDNA, por ejemplo, tremendamente eficaz en la persecución de delitos de pornografía infantil, y donada a todo organismo, empresa, fuerza de seguridad que quiera utilizarla. Sin ir más lejos, ahora mismo Facebook o Google hacen uso de esa tecnología en sus sistemas centrales. Esta tecnología se ha donado también a una empresa para que lo integre dentro de sus soluciones de ámbito más amplio en materia de soporte a las fuerzas de seguridad, pero con la condición de que cuando la fuerza de seguridad vaya a utilizar esa tecnología PhotoDNA, se le dé la licencia de forma gratuita con respecto a esa funcionalidad concreta.

Y *partnership* y colaboración, como tercer pilar. Probablemente sea uno de los puntos más importantes: colaboración en todos los ámbitos,

educativos, judiciales, políticos, policiales, administrativos, tecnológicos... Los reconocimientos recibidos por Microsoft de las medallas al mérito policial con distintivo blanco, que fueron otorgadas en 2010 y 2011 respectivamente, tienen que ver especialmente con este pilar. Microsoft da respuesta, al mes, a del orden de 200 peticiones judiciales de información, al mes, en España, a Ertzaina, Mossos d'Esquadra, Guardia Civil, Policía Nacional fundamentalmente, y resto de policías, pero fundamentalmente con las que más trabajamos son estas cuatros. Es nuestra obligación, obviamente, pero a nadie se le premia por cumplir con su obligación. La implicación de Microsoft en la persecución de este tipo de delitos es lo suficientemente ágil y responsable como para que las investigaciones de nuestras fuerzas de seguridad aumenten sus posibilidades de llegar a buen puerto. Les invitaré además a sus señorías que lo contrastaran por ustedes mismos, al contacto con diferentes fuerzas de policía, cuando hablan de proveedores internacionales y les pregunten, por ejemplo, a quién les gustaría que se pareciera el comportamiento de multinacionales al respecto, en lo que respecta al trabajo de persecución de delitos,. Apostaría que les dirían directamente que Microsoft es el ejemplo a seguir, Microsoft Ibérica, que aquí también lo hemos estado persiguiendo de forma especial, incluso enseñando al resto de nuestra corporación cómo se pueden hacer las cosas en esta materia.

Eso sí, hay que invertir, obviamente; tenemos personas dedicadas 24x7, que solo se dedican a esto, nada más; y es una inversión que hace Microsoft, pero que necesitamos sentirnos, obviamente, a gusto, reconocidos e integrados en la sociedad en la cual estamos viviendo, que es la de aquí y no es otra.

A nivel internacional, algunas actuaciones de Microsoft son especialmente relevantes, como colaboración con organismos como el ICMEC, el International Center for Missing and Exploited Children

Y llegados a este punto, y dado el carácter multinacional de la compañía a la que pertenezco, quería compartir con sus señorías alguna información relativa a estado del arte de esta problemática en relación con otros países de nuestro entorno. Hemos elaborado un estudio reciente al respecto de diversas problemáticas relacionadas con la protección de menores, y en concreto en materia tan delicada como el ciberacoso o *cyberbullying*, es decir el abuso entre iguales.

El análisis se ha hecho en 25 países (Australia, Argentina, Brasil, Canadá, China, República Checa, Egipto, Francia, Alemania, India, Italia, Japón, Malasia, Marruecos, Noruega, Pakistán, Polonia, Qatar, Rusia, Singapur, España, Turquía, Reino Unido y Estados Unidos) entre niños y niñas entre 8 y 17 años.

Algunos datos interesantes obtenidos: pues el 37% reportan haber sufrido algún tipo de acoso *online*, como media, el 37%; adelanto que esa es la media, además, de España, en España estamos justo con ese valor, justo en la media. El 24% reconoce haber acosado a alguien; estar más de 10 horas por semana *online* aumenta las probabilidades de sufrir acoso, que pasan de un 29% a un 46%; el 86% reconoce haber sido acosado *online* u *offline*; el acoso *offline* se da el doble que el *online*, un 73% versus un 37%; el 42% dice no saber nada sobre *bullying*; el *bullying online* es más frecuente entre los 13 y los 17 años, y sin embargo entre los 8 y los 12 sufren más el *bullying offline*.

Algunos datos geográficos interesantes son: España se mantiene en valores intermedios en el estudio de esos 25 países; solo destaca especialmente por ser el segundo país cuyos menores expresan mayor preocupación sobre el *bullying online* (a continuación Brasil). Los países con mayores índices de *bullying online*, de forma muy destacada, el primero China, con un 70%, seguido de India, Argentina, Rusia, Turquía. España se encuentra justo en la media, con el 37%, y luego los países con

menor índice de *bullying* son Japón, Francia, Italia (con un 28%), Estados Unidos (con un 29%), Noruega, Pakistán, Egipto, Qatar, Malasia... Es *bullying online*. Muchos de estos países, luego resulta que son lo *top* en los *bullying offline*, por ejemplo Estados Unidos, es uno de los países con mayor incidencia. El país donde más *bullying offline* existe es Marruecos, Canadá, Reino Unido, Estados Unidos, Australia.

El informe es muchísimo más amplio, y lo pongo en su totalidad a disposición de sus señorías, si quieren examinarlo. De hecho, lo tengo puesto como anexo en esta *slide*, con lo cual ya lo tienen.

En resumen, y para concluir esta exposición, queda mucho por hacer en el ámbito de la ciberseguridad en general, y en el de la protección de menores en la red en particular. Identificar las palancas de acción es un excelente primer paso, y sinceramente –y además subrayo la palabra "sinceramente", porque he vivido situaciones en ese sentido–, creo que sus señorías en el transcurso de esta ponencia, comprendiendo a los comparecientes que han ido compartiendo su conocimiento y preocupaciones ante ustedes, les pone en una situación privilegiada, y créanme que única, para identificar y facilitar la acción de esas palancas. No resulta muy habitual, aunque puedan pensar lo contrario, reunir tanto conocimiento experto como el que ustedes han conseguido en el desarrollo de esta ponencia, no es habitual; ni piensen, en mi opinión, que existe un diálogo permanente y fácil entre muchos de los comparecientes que han pasado durante todo el año pasado y este en esta ponencia, no es habitual.

Es por ello por lo que la foto global que ustedes manejan puede ser única. Es probable que igualmente hayan observado el enorme interés que los comparecientes habrán puesto en compartir sus preocupaciones, exponer sugerencias desde la realidad de los hechos; y es que al final del día, aunque vengamos aquí con la etiqueta que nos toca, en mi caso la de Microsoft, todos tenemos otra etiqueta personal que nos motiva

especialmente, y es la de miembros de una sociedad, ya sea como padres de familia (en mi caso), educadores, etc., que a su conocimiento profesional suman el interés adicional de proteger hijos, alumnos, etc., inmersos en un mundo digital tan apasionante como complejo.

Nada más; muchas gracias de nuevo por la atención, y quedo a disposición para cualquier pregunta. Muchas gracias.