Ciberseguridad en Niños, Niñas y Adolescentes

Introducción

En el mes de diciembre del año en curso se llevó a cabo en Guadalajara, México, el 11° Foro de Gobernanza en Internet (IGF), una reunión global organizada por la Organización de las Naciones Unidas (ONU) y el Gobierno anfitrión, y que reúne todos los años a los personajes más influyentes y trabajadores por el desarrollo de un mejor ecosistema digital. Cada uno de los presentes, desde asistentes hasta disertantes, cumplen un papel muy importante en el desarrollo de lo que me atrevo a llamar, el nuevo continente —o el octavo continente—, reunidos todos bajo un solo camino que es el de generar políticas de desarrollo de Internet y una gobernanza estable y colaborativa.

En esta oportunidad, gracias a la empresa Amazon® y la South School on Internet Governance, fuimos invitados a participar a este importante evento un grupo de becarios sectorizados en diferentes campos, con la misión tal de no solo conocer cuáles eran los cambios que se venían produciendo en Internet y los temas que más se discutían; sino, demás, saber cómo colaborar a esta constante vertiente evolutiva. El ADN de este evento está configurado para el trabajo en equipo y no para el personalismo. Todas las organizaciones estuvieron presentes, desde las privadas como AMAZON®, pasando por las organizaciones internacionales como la ONU y la OEA,

acabando con algunas sociedades civiles y formadores de líderes como la Asociación Mexicana de Internet, Fundación Redes o la South School on Internet Governance, entre otros.

Este reporte es el resultado del 11° Foro de Gobernanza en Internet (IGF), pero centrado en el aspecto de la ciberseguridad en el campo infantil, al que considero, una zona gris dentro de Internet y que todavía tiene mucho que explorarse, hasta llegar a un momento en que podamos decir que ya podamos decir que ellos también se encuentran preparados para enfrentar los peligros que nuestro mundo nos muestra. Espero sea de su agrado.

Internet de los Juguetes

I

Desde la expansión popular de Internet y las tecnologías, la genética infantil parece venir acompañada de un nuevo código que permite entender estos componentes como un adicional de su cuerpo. Ya no es extraño hablar de migrantes, nativos, e incluso, analfabetos digitales desde hace más de diez (10) años; sino que, además, el sector tecnologías y entretenimientos busca desarrollar cada vez más productos que puedan entrelazarlos más a la sociedad de la información; pero, específicamente, a los consumidores populares por excelencia: los niños.

No es extraño, entonces, empezar a dialogar sobre Internet de

los Juguetes, un derivado de Internet de las cosas (IoT) que conecta el entretenimiento infantil con aplicativos y que ha despertado el interés en el sector ciberseguridad por sus escasas medidas de seguridad; incluso, se debate sobre los parámetros de la privacidad de los menores de edad, con lo que también se discute si ello debería o no tener privacidad. Uno de los productos que incentiva este debate es la muñeca **My Friend Cayla®**[1] de la compañía Genesis Industries Limited®, la competencia de la Hello Barbie®, la muñeca que habla de Mattel®, con la que sus creadores afirmar que es como una ***amiga de verdad***, y con la que sus ***posibles consumidores*** resaltan el espionaje a menores y otros peligros de los que aún no se hablan.

Durante el desarrollo del IGF, un grupo de investigadores de las Universidades más importantes de Norteamérica, junto con el Fondo de las Naciones Unidas para la Infancia (UNICEF) desarrollaron un workshop centrado en **Internet de las Cosas e Internet de los Juguetes**, en donde se dialogaron sobre los peligros de estos nuevos muñecos que componen su funcionalidad de Internet y otras aplicaciones. El debate empezó preguntándonos si este era el futuro de los juguetes; a lo que realmente me apego a decir que no es el futuro, sino el presente, y que las muñecas como Barbie® o Cayla® no deberían ser consideradas las primeras en su tipo. ¿A qué me refiero?

Mientras que **Hello Barbie®** era un producto cuya seguridad

[1] Puede encontrarse toda información en www.myfriendcayla.com

se discutía el 2015, y **My Friend Cayla®** la muñeca controversia del 2016, los videojuegos se transformaron, según la historia del entretenimiento, en los primeros Internet de los Juguetes; incluso, en el primer Internet de las Cosas. La interconectividad multijugador existe como proyecto desde el año 1979, más de treinta (30) años atrás de los proyectos antes mencionados; y como una conectividad estable por el año 2000 con algunos juegos de PlayStation®2, y del que jamás se debatió por seguridad en los menores, como se hace ahora con estas dos muñecas. ¿Qué hace estos objetos diferentes si todos se desarrollan en el campo del entretenimiento? Quizás que, los dos primeros, solo se centran en niños como sus principales consumidores.

II

Durante los primeros minutos del workshop se dejó en claro que no había nada en contra de las compañías, pero sí en su forma de trabajo quizás un tanto despreocupada por la seguridad de los menores de edad. Señalaron que productos como estos violaban el Acta de Protección de la Privacidad de los niños de Estados Unidos, pero que tampoco se percibía una mayor responsabilidad con los juguetes conectados a Internet o juguetes online. Pueda ser que **Hello Barbie®** no represente un peligro más allá del consumismo y la moda —haciendo hincapié en una de las inagotables bromas que se disfrutaron en la reunión—, pero constituye una nueva puerta en el tema de la inseguridad digital. Dicho de otro modo, los *especialistas en inseguridad informática* podrían acceder a

numerosos datos personales de los menores.

¿Cómo funciona una muñeca como la **Hello Barbie**® y porqué causa tanto peligro? Pues bien, según se informa, la muñeca tiene la capacidad de conversar con los niños, por lo que todo lo que digan los infantes se envía a un servidor de la empresa y se analiza mediante reconocimiento de voz, de modo tal que la muñeca pueda dar las respuestas apropiadas. Aunque en teoría suene a una actividad inofensiva, la empresa Bluebox ha descubierto ciertos agujeros que motivaron a la discusión en el workshop. Primero, las aplicaciones para IOS y Android, utilizadas para la conexión con la muñeca, siempre utilizan la misma palabra clave; en Segundo lugar, la muñeca es susceptible de ser atacado con el *exploit*[2] Poodle, un ataque *man-in-the-middle*[3] que ayuda a que el programa de la muñeca sea más débil y más fácil de modificar y recibir un ataque. A esos hechos debemos agregar que esta muñeca se conecta a cualquier sistema WiFi, la maravilla de los atacantes para programar redes maliciosas y así tener acceso a información de manera más fácil. Generar una red llamada Barbie® o WiFi Libre es una práctica común. La vulneración es práctica diaria.

[2] Un exploit es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, que son utilizados para aprovechar una vulnerabilidad de seguridad de un sistema para conseguir que se comporte de una manera no deseada. Ejemplos de ello son el acceso de forma no autorizada, la consecución privilegios no concedidos lícitamente o los ataques de denegación de servicio o DDoS, aunque este último, muchas veces, no sea considerado un ataque con consentimiento.

[3] También denominado **ataque de intermediario MitM** o **JANUS**, consiste en realizar un ataque que permita adquirir la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes, teniendo como ventaja el hecho de que ambas no guardan conocimiento de la violación de su enlace.

La discusión sigue en tela de juicio en los Estados Unidos. Como se concluía en le workshop, no se descarta la intervención de la Comisión Federal de Comercio (FTC) para este nuevo tipo de muñeco, más aún cuando ya existe un caso de ataque a este tipo de producto. La víctima, el fabricante de juegos educativos VTech, logrando los agresores apoderare de fechas de cumpleaños, nombres y demás datos de más de seis (6) millones de niños.

III

Otro de los temas que se discutieron en el afán de la protección de los menores de edad fue el de **abuso infantil en Internet**, en un workshop direccionado por **WeProtect**, una alianza global multistakeholder que busca poner fin a la explotación sexual de los niños en línea, basando su trabajo en dirigir la práctica internacional; poner promoción y la acción en el centro de su misión; promover la asociación mundial y regional, la integración y la colaboración como formas de acabar con la explotación sexual infantil en línea; trabajar de una manera que respete y promueva los objetivos de desarrollo sostenible de las Naciones Unidas (ONU) y los instrumentos jurídicos internacionales y regionales destinados a poner fin a la violencia sexual contra los niños[4].

En el workshop que reunió a representantes de WeProtect, Microsoft® y sociedad civil se planteó uno de las amenazas

[4] Información obtenida de su página web www.weprotect.org

más estables en los últimos años; y, con cierto aire de vergüenza, dieron a conocer que muchos estados no se preocupan por siquiera pedir ayuda a una organización como ellos para elaborar un sistema de trabajo. WeProtect informa que existen personas en la web que interactúan entre ellos, intercambian imágenes, fantasías, técnicas, incluso a niños reales, y todo en el ámbito de la web; es por ello que desde el 2014 quisieron entrar en este campo a luchar contra el crimen global que implica estas acciones, con el único afán de eliminar el material sexual en internet y fortalecer la cooperación mundial para rastrear y atrapar a estos depredadores. WeProtect es la única alianza global que adopta un enfoque multisectorial para este problema y es el elemento central en la implementación del objetivo de desarrollo sostenible. Son más de 70 países, 20 empresas y 17 organizaciones internacionales quienes están trabajando con ellos.

Fuente: www.weprotect.org

Fuente: www.missingkids.com

Fuente: www.iwf.org.uk

IV

Con el punto céntrico de los proyectos el debate tomó muchas vertientes, tanto de parte de los panelistas como de parte del público. Por un lado, el resalte de la alianza con WePROTECT, a efectos de generar y compartir mejores prácticas en la

moderación del contenido, así como de políticas y esfuerzos de sensibilización en el tema por parte de la población; para crear y usar herramientas de detección de imágenes, técnicas y otras innovaciones; y por el otro lado, los usuarios y sociedad civil quienes afrontaban el debate a no solo saber qué hacer ante un posible criminal sexual, sino que, además, trasladaron una de las preguntas claves del debate de Internet de las Cosas e Internet de los Juguetes: ¿Realmente podemos hablar de privacidad en el sector infantil?

Este fue uno de los temas más debatibles, especialmente porque en Internet existen áreas grises en donde se pueden seguir compartiendo imágenes, y en donde hasta esa actividad pueda no ser considerada ilegal. Quizás en ello impacta el factor cultura, pero todos estábamos de acuerdo en que abuso infantil era abuso infantil, sin importar cultura, religión o estilo de vida, y que esta epidemia debía parar.

El trabajo centrado en Internet que realiza WePROTECT es de admirar, pero no es suficiente. Se señalaron casos y la organización aclaró que, sin importar que, la violación de la intimidad y privacidad de un niño también debería ser considerado un delito; pero, ¿a qué costo? Si yo fuera un padre de familia, ¿podría aplicarse también la misma fórmula conmigo

V

El panel de UNICEF titulado **UNICEF INNOCENT PANEL**,

sería uno de los workshops de mayor audiencia, junto con el de Internet de las Cosas y de los Juguetes. Se dejó en claro que la conexión de menores a Internet se ha vuelto una tendencia internacional, especialmente con el aumento en el uso de los celulares móviles, señalando al cyberbulling y cyberstalking como elementos considerables en la Ley de Internet para niños. También son claro en señalar la importancia de buscar la manera de hacer llegar el saber de los niños ante problemas de internet; o, de alguna manera, hacerlos partícipes del IGF. Esto va de la mano con la idea que señalara Göran Marby al inicio del IGF, una idea que fue del agrado del público asistente y que dejaba en claro que los modelos multistakeholder debían ser más activos con la comunidad, pero que su trabajo debía empezar de abajo hacia arriba, formando generaciones de líderes nuevos en la Gobernanza en Internet.

Göran Marby es el actual es el CEO y Presidente de la Corporación de Internet para la Asignación de Nombres y Números de Internet (ICANN), una organización global de múltiples partes interesadas (multistakeholder) creada y fortalecida a través de acciones por parte del gobierno de Estados Unidos y su Departamento de Comercio; y desde la cual viene impulsando una visión que busca estar más conectada a los usuarios y a la sociedad que a otros modelos multistakeholder. Göran Marby anhela que la sociedad comprenda el poder de Internet y de cada uno de los temas que en este se desarrollan, con el fin que las futuras discusiones que se generan por el bien de los usuarios tengan

a estos como mayores participantes, alineando también su mayor compromiso para con su desarrollo; tiene como meta que nos olvidemos de los acrónimos y hagamos más entendible cada uno de los temas que nos atrevemos a discutir para el bien de los usuarios, que muchos de ellos no nos conocen. En otras palabras, dejar las sombras para ser más activos.

Lo que expresó Göran Marby en la inauguración se centró en los niños y de su participación más constante en estas reuniones. Es importante recordar que el IGF empezó con los jóvenes quienes se preocupaban por un mejor Internet, y el sector adulto se acopló al movimiento con experiencia y liderazgo, pero poco a poco el sector juvenil, el que está lleno de adrenalina y conocimiento, se fue alejando, y ahora busca recuperar ese terreno. Göran Marby quiere impulsar su protagonismo una vez más pues quién entiende mejor Internet que los jóvenes.

La materialización de la idea se dibujó con la participación de la delegación de Hong Kong. Niños de entre 12 a 15 años se encontraban en todas las reuniones que se enfocaban en protección a menores, debatiendo con miembros de UNICEF y otras organizaciones, soltando preguntan cada vez más complejas, una tras otra, evitando repetirlas, y demostrando lo que Göran Marby soltaba como nuevo requisito para los próximos IGF, pues nadie sabe mejor que es lo que necesita un niño sino un niño mismo; nadie conocerá mejor sus problemas, sus necesidades, sus enfoques y su sapiencia si no

los hacemos partícipes, si no los escuchamos, si no dejamos que trabajen con nosotros por un ambiente mejor, porque nos enfrentamos a una generación dividida, una generación que en un par de años tomará las riendas de Internet y que desde ya discute entre ella misma por la libertad y la desprotección de la privacidad, contra la protección de la misma y una libertad moderada, solo para nombrar algunos temas en lo que ponerse de acuerdo resulta una tarea complicada. En un par de años la generación actual jugará un papel más importante y ya no solo como espectador o como a los que buscamos proteger; sino más como actores del cambio. Mi pregunta: ¿qué cambio nos espera?

Conclusión

La finalidad de este micro reporte no era solo reunir información de reuniones resaltantes en el ámbito de protección al menor en Internet, sino de conocer más el trabajo de las organizaciones y ver que tenemos y qué nos falta. La idea inicial era hablar sobre ciberseguridad en general, pero desembarqué en el ámbito de protección de niños, niñas y adolescentes porque yo también fui parte de ellos, y me hubiera gustado que mi generación no hubiera crecido sobre la marcha y el cambio y error, sino con una guía que nos permita saber y entender que Internet es tan o igual de seguro que el mundo real, pero que no es un lugar de entero temor, como algunos padres lo comentan. Ahora entiendo cómo funciona el ecosistema. Ahora siento que es el momento de retribuir con la nueva generación.

No puedo dejar de destacar cada uno de los trabajos expuesto y desarrollados en cada uno de los workshops. La ciberseguridad de niños, niñas y adolescentes es un campo complejo y gris, pero todos están centrados en el punto de ***desarrollo del problema***; es decir, cuándo el problema ya se dio, recién es el momento de actuar. No pude escuchar un solo momento hablar de ***ciberseguridad preventiva***, un concepto que se basa en patrones seguidos por la seguridad ciudadana cuando hablamos de ***prevención del delito***. Es efectivo combatir contra estos cibercriminales; pero es mucho más efectivo prevenir el problema y dar estrategias que no solo se basen en la dependencia de las tecnologías para un cometido, beneficioso o malicioso. Los delincuentes que han sido sancionados por cometer abuso contra menores utilizaban la ingeniería social desde antes de Internet, solo que este último hizo más relajado su trabajo.

Por otro lado, sigue siendo admirable la participación de los niños miembros de la delegación de Hong Kong, pues demuestran la preocupación de esa parte de la generación que exige protección, y no quiere seguir en un presente gris. Sin embargo, sigo considerando que un trabajo preventivo con padres de familia, maestros y alumnos pueda ser una de las tantas claves que tendremos para mejorar la ciberseguridad en niños, niñas y adolescentes; especialmente en un sector como le abuso sexual. Sé que depender de la tecnología se ha vuelto una tendencia, pero debería ser un complemento en este tipo de trabajo antes de ser la única herramienta. Creo que el

trabajo colaborativo se nutriría más con fórmulas que no dependan netamente de la tecnología, pero sí sea una fuente fuerte de apoyo. De ser negativos todavía a esta corriente, llegaremos a ser iguales a los que queremos cazar, y tarde descubriremos que pasaron a otro campo, al que tendremos que volvernos a adaptar, y nuevamente un tiempo nos tomará. No tengo la respuesta absoluta ni soy el dueño de la verdad, pero deseo contribuir con aquello que considero correcto por el bien de nuestra comunidad digital. Pongamos de nuestra parte. Aún estamos a tiempo para trabajar en la ciberseguridad de niños, niñas y adolescentes. Aún estamos a tiempo de hacer un Internet más equitativo y desarrollado. Aún estamos a tiempo de cambiar nuestra realidad.