ICANN74 | Foro de Políticas – Presentaciones de NextGen (1 de 2)
Martes, 14 de junio de 2022 – 13:15 a 14:30 AMS

DEBORAH ESCALERA: Hola y bienvenidos a la presentación de NextGen, mi nombre es Deborah Escalera y soy coordinadora de la participación remota para la misma. Tengan en cuenta que se está grabando y se rige por los estándares de comportamiento esperado de la ICANN, durante la sesión las preguntas o los comentarios presentados en el chat se leerán en voz alta solamente si se ponen de la manera correcta, tal como se indica en el chat.

Voy a leer en voz alta comentarios y preguntas en el momento que lo indique la presidencia. La interpretación va a incluir inglés, francés, español y portugués, seleccionen el ícono de interpretación y el idioma que van a escuchar durante la sesión. Si desean tomar la palabra, por favor levanten la mano en la sala de Zoom y una vez que el facilitador diga su nombre, habiliten el micrófono y tomen la palabra.

Antes de hacerlo verifiquen haber seleccionado el idioma en el que van a hablar en el menú de interpretación, indiquen su nombre para los registros y el idioma en el que van a hablar, si no es inglés. Silencien todos los dispositivos y notificaciones,

cuando tomen la palabra háganlo con claridad y a un ritmo razonable para permitir una interpretación correcta.

Con esto le doy la bienvenida a todos a la sesión, gracias por participar y por el trabajo de la presentación, también a mis mentores Dessalegn Yehuala y Roberto Gaetano, por trabajar con los estudiantes en las últimas semanas y por ayudar en el proceso de la reunión de la ICANN, también a mi colega Betsy Andrews que va a pasar las diapositivas. Le voy a pasar la palabra al primer presentador, Joel Christoph. Joel, la palabra es suya.

JOEL CHRISTOPH: Buenos días a todos y gracias a todos los presentes por estar aquí, voy a hablar del crecimiento de internet en 2022 y su graficación, que es un proceso que considera el conocimiento demográfico de las distintas fuentes y lo que nos dice. Siguiente diapositiva, por favor.

Antes de comenzar me gustaría que consideren un momento, ¿qué proporción de la población de los países de bajos ingresos utilizan internet? Eso quiere decir que viven con €2.7 o menos por día. La siguiente pregunta es: En los países de bajos ingresos, ¿cuántas suscripciones de celulares hay por cada 100 personas? ¿Cerca de 25, 50, 75 u otro valor? Y, finalmente, ¿cuántos

servidores de internet seguros hay por cada 1.000 personas en Norteamérica?

Esto quizás es un poco más complejo de estimar en términos de la definición, pero son algunas preguntas que espero que puedan responder al final de la presentación. Siguiente, por favor.

En las últimas décadas hemos visto cambios respecto de las investigaciones y las publicaciones, hemos visto un crecimiento importante en las dimensiones de internet desde los 90' y más recientemente en las redes sociales, en comparación con la palabra censura en las publicaciones corporativas en inglés.

Entonces tenemos un crecimiento en el interés de muchos de estos temas que, en realidad, son persistentes indicando que van a seguir trabajando en estos temas, dado que lo consideran muy importantes y que son parte de la bibliografía que tenemos que considerar. Pasando entonces a la parte principal del asunto, acabemos la proporción de personas por región que utilizan internet.

Lamentablemente la leyenda a la derecha no quedó bien, pero el punto principal es que, vemos un incremento parejo en muchas regiones en las personas que están utilizando internet con una

aceleración particular en distintos puntos, de pronto en los últimos años en el sudeste asiático ha habido un incremento relativamente rápido y también hay convergencias hasta el 90% en las regiones de mayores ingresos.

En azul y rojo, Norte América, luego Europa y Asia Central la siguen, en marrón vemos el grupo de bajos ingresos que corresponde a los países con los menores ingresos, en categoría definida; según el concepto del banco mundial, el promedio es €2.7 o menos por día en cuanto a lo que gastan en la vida.

Esto también influye en el acceso a estas personas a internet y esto se asigna como la difusión de distintas tecnologías para acceder a internet, que son cada vez más, y también el acceso en algunos de los países o regiones con menores ingresos del mundo. Siguiente, por favor.

Comparemos esto con los valores absolutos, vemos que mientras ha habido algunos inicios precoces en el uso en Estados Unidos; que se muestra en verde, en la última década vemos un incremento importante de usuarios en China y en India, dada sus poblaciones esto va a seguir viéndose reflejado en gran parte del uso y también en la cantidad de ideas que se originan en las distintas partes del mundo.

La porción inferior de la gráfica tiene mucha información y representa a los otros 10 países entre los 10 superiores con mayor cantidad de usuarios de internet, Brasil, India y la Federación Rusa. Siguiente.

Para comparar, la cantidad de usuarios con las suscripciones de celulares, tenemos una idea de lo que puede representar a las distintas poblaciones que acceden al internet, estos son datos provistos por el banco mundial a través de la UIT y vemos que, en muchas regiones, tales como Norte América, Europa y Asia Central tenemos muchas más suscripciones de celulares que personas.

Entonces en los grupos económicos, no geográficos, de bajos ingresos se ve al menos una suscripción cada dos personas, esto apunta a la dirección del acceso a través de las redes móviles que se va a ir expandiendo. Si comparamos esto con el ancho de banda fija; que puede ser un medio distinto de acceso y comunicación, vemos un incremento menos marcado, especialmente en las últimas décadas, vemos en el eje de la “Y” no llega a 120, ni tampoco vemos convergencia en distintas regiones, especialmente en el sudeste asiático, en el África subsahariana y en la categoría económica de bajos ingresos.

El aspecto interesante es que, entre las regiones, tales como en Norte América hay un caso sumamente claro de haberse quedado por debajo del 50% referido al umbral, si vemos la cantidad de servidores de seguros de internet por cada millón de personas; aquí vemos las tecnologías de encriptamiento que se utilizan, hay una gran diferencia en comparación con las diapositivas interiores respecto a las regiones porque Norte América que, en este caso, son Estados Unidos y Canadá fundamentalmente, hay una gran cantidad por persona seguido por Europa y en la mayoría de las demás regiones estos certificados distintivos todavía no son muy frecuentes.

Si damos un paso atrás y vemos el uso del internet como porcentaje de la población, correlacionado con el PBI per cápita, hay una sugerencia de una relación positiva en el ingreso per cápita por países, más usuarios utilizan internet cuanto más alto sea, pero como vemos en la parte superior de la gráfica hay un punto de saturación alrededor de las $6.000 per cápita, que son los ingresos de Noruega, Baréin, Estados Unidos, Suiza y más allá de ese nivel no hay ningún incremento porque se ha logrado el punto de saturación de internet.

Aquí quisiera dar un paso atrás y considerar que, cuando estamos tratando de graficar esta expansión en espacio y tiempo, también representa la diferencia en el uso intensivo, no

solamente en el extensivo del acceso a internet. Esto se basa en datos de Estados Unidos cuando se le pregunta la cantidad de horas en las que están participando con medios digitales.

Ha habido nuevos dispositivos y sistemas desde 2008, pero notablemente los dispositivos móviles es un agregado al tiempo que las personas utilizan participando en estos medios, y a medida que se desarrollan distintas tecnologías y formas de acceso no va a ser un fenómeno de sustitución, sino más bien más tiempo en nuestras vidas, vamos a estar conectados a nivel digital; y con ello quisiera terminar esta parte. Agradezco mucho a todos, le voy a pasar la palabra a Deborah Escalera, nuevamente.

DEBORAH ESCALERA: Muchas gracias, Joel. ¿Hay alguna pregunta para Joel? Muchas gracias por su presentación, muy bien hecho. Entonces vamos a pasar a la siguiente presentación, que es de Mirabella Knoben. Mirabella, tiene la palabra.

MIRABELLA KNOBEN: Hola, muchas gracias a todos por estar en esta sesión. Hoy quisiera hablar sobre un trabajo que preparé el verano pasado, yo participé en un seminario sobre la ley de servicios digitales y también les voy a explicar el tema, yo hablé sobre la normativa

de regulación de contenidos a través de algoritmos, los principios que son necesarios para proteger los Derechos Humanos en el mundo digital.

Ley de servicios digitales, como todos sabemos, Facebook, Google, Instagram, etc., son las grandes plataformas en línea que usamos diariamente y, como todos sabrán, desempeña un papel importante en cuanto a influir sobre estas opiniones y brindarnos información, con el fin de actualizar las normas que ya quedaron desactualizadas de la directiva de comercio electrónico del año 2000 la comisión Europea publicó una versión preliminar de la ley de servicios digitales en diciembre del 2020.

Básicamente establecen normas más estrictas para lo que se denomina VLOPS, plataformas en líneas muy grandes. En abril hubo un acuerdo político con respecto a la DSA llevada a cabo por la comisión europea del parlamento y como es una regulación; y no una directiva, después de la adopción esto se compartió con toda la Unión Europea y se va aplicar a partir del 01 de enero de 2024 a más tardar.

Entonces, ¿qué son los algoritmos o los sistemas de recomendación en cuanto a la ley de servicios digitales? Se define en el artículo 2 de la ley de servicios digitales y la

definición es que, son sistemas totalmente automatizados que sugieren un código específico al usuario y esto aparece en la interfaz de usuarios, entonces las plataformas digitales pueden considerarse como sistemas de recomendaciones porque los usuarios de las plataformas ven contenido personalizado diariamente y este contenido tiene prioridad versus otro tipo de contenido.

Entonces vamos ahora al centro de mi trabajo, ¿qué interferencias podrían darse con los Derechos Humanos? Yo me centré en la libertad de información y en la libertad de expresión, ambos mencionados en la carta de derechos fundamentales.

Voy a hablar primero de la libertad de información porque las plataformas de redes sociales están diseñadas para que nosotros como personas volvamos a ver contenido con el que estamos de acuerdo o que ya conocemos, entonces obviamente esto puede llegar a que veamos solamente un contenido sesgado o un efecto de filtro de burbujas porque si solo vemos contenido que nos gusta es porque ya estamos de acuerdo con el mismo, esto puede ser algo muy sesgado.

En base a esto, la libertad de expresión también puede estar en peligro porque las personas forman sus opiniones en base a la información que reciben, entonces si la información que reciben

se creó en base a algoritmos, es decir, que no hay control humano, se puede influir también sobre la formación de sus opiniones, entonces la libertad de expresión también está en peligro cuando solo trabajan los algoritmos preparando la información.

Entonces la pregunta es: ¿Cuáles son los principios que necesitamos para evitar este tipo de interferencias? Yo me concentré en dos principios posibles en mi tesis, primero, sistemas basados en lo que llamo diseño participativo, un término que se explica por sí mismo porque significa básicamente que los sistemas que están basados en el diseño participativo incluyen más participación humana y, por lo tanto, representan más valores de más personas, la idea es crear un algoritmo que incorpore los valores generales de cada sociedad.

Y como todos habrán escuchado decir en los últimos días, se habló muchas veces del modelo de múltiples partes interesadas de la ICANN; que yo sé que es un modelo interno de la ICANN, pero creo que la idea básica de este modelo podría implementarse también en las plataformas de redes sociales y el objetivo principal de este modelo es lograr que se escuchen las voces de todos los grupos interesados de todas las partes interesadas en la misma medida.

Esto logra el control descentralizado y procesos participativos e inclusivos considerando el tamaño de las plataformas en línea, como Instagram y Facebook, que son plataformas muy grandes. Es difícil implementar este modelo, pero, como dije antes, yo creo que la idea básica es lograr que todos los grupos interesados puedan hacerse escuchar, esto sería una forma de garantizar más transparencia y una atmósfera en líneas más participativas.

Hablando de transparencia, en la ley de servicios digitales, artículo 29, incluye dos requerimientos. Primero, el requerimiento de mayor transparencia, esto significa que las plataformas en línea de gran tamaño están obligadas a comunicar y dar a conocer sus parámetros más importantes, para que los usuarios sepan qué parámetros están utilizando; hablando de los sistemas de recomendación.

En segundo lugar, tenemos la posibilidad de exclusión voluntaria, esto significa que cuando abrimos nuestra aplicación de Instagram o de Facebook se nos presente, en primer lugar, la posibilidad de usar la plataforma con sistemas de recomendación, la implementación concreta de esto todavía no se sabe cómo se va a hacer, pero es muy parecido a lo que vemos diariamente cuando abrimos un sitio web y damos nuestro consentimiento para que se utilicen.

La intención es evitar especialmente las interferencias con la libertad de expresión y otros derechos fundamentales, esto puede llevar a que los usuarios confíen más en las plataformas en línea, lo cual puede ser útil para las plataformas mismas.

Y para terminar, antes de que queden claras las funciones principales de implementación debemos prestar atención a los derechos fundamentales para garantizar más sensibilidad y consciencia con respecto al tema en general y como el internet no tiene fronteras, a pesar de que la ley de servicios digitales es una norma europea, estoy convencida de que es necesario buscar una solución internacional porque el internet no termina en las fronteras de la Unión Europea y la única manera de crear un mundo online atractivo y seguro a largo plazo es trabajar a nivel global. Gracias.

DEBORAH ESCALERA: Gracias, Mirabella, ¿hay alguna pregunta para Mirabella? Muchas gracias por su presentación. Ahora pasamos al siguiente presentador, Jan Batzner. Jan, le damos la palabra.

JAN BATZNER: Hola a todos, gracias por la oportunidad. La seguridad del internet es un objetivo que todos compartimos, entonces hablemos de los incidentes de la seguridad en el ciberespacio.

Un ciberincidente es un evento que hace que se pierda seguridad e integridad, así lo define la ICANN, un ejemplo puede ser un ataque de denegación de servicio, donde los atacantes hacen que los usuarios no tengan acceso a un equipo determinado o también ataques de spoofing, donde se simula ser otra persona, como, por ejemplo, Instagram que puede terminar con .XYZ para hacer un phishing o buscar información de los usuarios insertada allí.

Vamos una diapositiva hacia atrás por favor, gracias. Hoy quiero evaluar los diseños prevalentes de las fuentes de datos e incidentes de ciberseguridad, fuentes y bases de datos públicos que comparten información sobre unos incidentes cibernéticos, aquí vemos un gráfico de una red que creé y aquí ven los incidentes cibernéticos agrupados por países afectados, cada punto es un país y el código cromático muestra la intensidad del conflicto.

Hay diferencias en estas fuentes de datos, el registro de incidentes de ciberseguridad de la ICANN, por ejemplo, registra todos los incidentes de ciberseguridad que tienen lugar dentro

del espacio de la ICANN y en los productos de la ICANN para definir una buena medida de seguridad, es una debilidad en un producto que pone en peligro, entonces todo lo que pasa con los productos de la ICANN están aquí.

Todos los conjuntos de datos que siguen en la lista vienen del espacio de políticas públicas, donde se comparte públicamente información sobre ciberincidentes con las partes pertinentes. Hoy voy a hablar de esos conjuntos de datos y cómo han sido evaluados, vamos a ver qué podemos aprender de los mismos y si podemos llegar a una conclusión. Próxima diapositiva, por favor.

Aquí vemos el registro de incidentes de ciberseguridad, vemos la fecha, el problema, el estado y la información que aparece con un párrafo a la derecha, en este momento el estado de todos los incidentes en esta lista es cerrado. Ahora vamos a ver los abordajes de políticas públicas, si vemos estos conjuntos de datos, serían líneas superpuestas que mostrarán lo mismo porque la idea es que deben medir exactamente lo mismo, pero vemos algo diferente.

En verde vemos la información de la Universidad de Heidelberg, en amarillo vemos la información del consejo de relaciones exteriores y en azul vemos el conjunto de datos de otra

organización, en todos vemos diferentes conjuntos de datos, diferentes momentos, por lo tanto, vemos que hay metodologías diferentes para esta información.

La información más inclusiva es la que representa la línea verde de la Universidad de Heidelberg, trabajemos ahora con la información de la Universidad de Heidelberg y hagamos algunas preguntas. Si podemos agrupar esta información por país podemos ver la cantidad de incidentes que van hacia ese país o que salen desde ese país, in-degree, out-degree son los que salen de ese país y después vamos a la reciprocidad.

Entonces si un país recibe un ciberataque y también lo devuelve, eso es lo que vemos con reciprocidad. Aquí vemos los 10 países con mayor nivel de conflicto, incluso aquí la reciprocidad no es perfecta, una reciprocidad perfecta sería 1, falta de reciprocidad es 0, incluso en los países con mayor conflicto llegan máximo a 0,5 de reciprocidad.

Aquí podemos ver cómo se podría cuantificar esta información, aquí vemos el régimen medido por el puntaje de la Freedom House y las características de los conflictos de ciberseguridad. A la izquierda vemos la relación entre los ataques que salen y el puntaje de Freedom House, a la derecha vemos la reciprocidad, pero no vemos ninguna relación clara en estos diagramas.

Uno de los motivos es que, hay una pequeña cantidad de estados que tienen muchos conflictos, se escribió mucho sobre este tema y hay muchos abordajes que tratan de cuantificar todo esto, pero lo que quiero subrayar aquí es que, estos abordajes pueden ser muy peligrosos o llevar el error porque lo que vemos aquí en rojo son los países importantes, los países que debemos considerar y analizar.

Quisiera terminar diciendo que hay tres aspectos que podemos tomar aquí, el objetivo de todos esos abordajes es la transparencia y la transparencia se logra generalmente a través del análisis de los registros de incidentes, la cooperación de todas las partes interesadas y la concientización, la forma de responder preguntas lógicas. Ya vimos antes que la metodología tiene un gran impacto sobre las respuestas que podemos ver para la misma pregunta de investigación. Muchísimas gracias.

DEBORAH ESCALERA: Muchas gracias. ¿Hay alguna pregunta para Jan? De algún participante en línea. Bueno, muchas gracias por su presentación, Jan.

Ahora pasamos a la próxima presentadora, que es Nadezhda Arteeva.

NADEZHDA ARTEEVA: Muchas gracias, es un placer estar aquí con ustedes. Vamos a hablar del uso indebido del DNS en la Unión Europea, lo que sucede y cómo se le puede tratar.

El problema principal con la definición de uso indebido del DNS es que, los nuevos tipos de uso indebido se crean comúnmente y tienen una frecuencia, una variación temporal, tal como se vio en 2021. Hay una definición adoptada por la ICANN de las partes contratadas, de acuerdo a la ICANN es un malware, botnet, pharming, phishing y spam los daños que causan.

¿Por qué necesitamos una definición? Porque la mayoría de los registros quiere una definición acotada de los daños que comprendan, que tenga la capacidad de tratar y que mida los efectos de un enfoque desproporcionado a menudo e impreciso. En 2022 la comisión europea a principios de año presentó publicaciones de pertinencia para ccTLD, tales como el estudio de uso indebido del DNS y una comunicación sobre una estrategia del tema. Voy a hablar del estudio de uso indebido del DNS en mi presentación, dado que mi opinión es uno de los documentos más adecuados para la estrategia de combate del uso indebido del DNS.

De acuerdo a la comisión europea entonces el uso indebido del DNS el estudio en términos de la evaluación del alcance provee aportes en base a las brechas no definidas, define al uso indebido como cualquier actividad que utilice nombres de dominios o el protocolo del DNS para llevar a cabo actividad dañosa o ilegal.

Hablemos un poco sobre la evaluación del problema, no solamente en la Unión Europea, sino también en la comunidad de la ICANN en general, algunas disposiciones contractuales que tratan el uso indebido del DNS provienen originalmente del trabajo de política realizado por la comunidad en 2009 y 2010 a partir del grupo de trabajo de prevención de uso indebido del registro, lograron dar la definición; que se citó previamente, delineando los puntos principales de la estrategia de la ICANN.

Hace seis años atrás en el SAC077 el SSAC escribió sobre el índice de salud del mercado propuesto, que fue uno de los primeros que trató el problema del uso indebido del DNS, considerando las citas se trata de implementar actividad de auditoría, aspectos de divulgación respecto del registro y operaciones de los registradores y su comportamiento de manera que enfatice las normas sobre la industria de protección del consumidor.

No se ha realizado demasiado en los años siguientes y este problema ha pasado especialmente a ser algo crítico durante la pandemia del COVID-19 porque respecto de los nuevos registros de dominios de “COVID-19” o “coronavirus”, ha llevado este tema al 2020. El foro de colisión de nombres de dominios con expertos en seguridad publicaron que datos que muestra que hubo un incremento importante en los dominios en los últimos tiempos de pandemia y se habló de una pandemia severa que era probablemente inevitable, tal como dijo el CDC.

Inicialmente la ICANN alentó que se fuera más proactivo, pero no se implementó o no se asesoró sobre un mecanismo específico, sin embargo, el uso indebido del DNS por el tema del COVID-19 llamó la atención, hubo líderes de las empresas de dominios que recibieron algo de atención de los gobiernos a raíz de las consecuencias dañosas de la lucha de la pandemia.

Entonces luego, en mayo de 2020, ICANN implementó medidas para combatir el problema y se hizo un desarrollo que se compartió con el público, indicando la estrategia que tenían que seguir registros y registradores para definir los nombres de dominios maliciosos. Siguiente.

Sin embargo, hablemos de por qué se da el uso indebido del DNS, cuáles son los ambientes y los pre-requisitos que lo

permiten. Hay un estudio en 2021, que después se confirma en los informes de la Unión Europea sobre este tema, confirma que una de las razones principales por las cuales se da es la falta de datos de contacto por la normativa de la GDPR. Sabemos que la normativa general de protección de datos de la Unión Europea prohíbe la publicación de datos personalmente identificables.

En respuesta la ICANN estableció una nueva política que permite que los registradores y registros puedan eliminar los datos personalmente identificables en el WHOIS, como algunos estudios indican, tuvo consecuencias, tales como que, el 85% de los registratarios de dominios de gTLD ya no se pueden identificar y otras cifras que pueden ver en la diapositiva.

Otro problema que está relacionado con el uso indebido del DNS es el tiempo largo que toma un informe de uso indebido, se sugiere; según algunos estudios, que el promedio es de 32 días y muchos registradores dicen que estos informes se tratan en 10 días o menos, pero según el caso este período puede variar y para algunos registradores puede llegar a ser extremadamente largo.

Otro problema respecto de este tema es la falta de conocimiento sobre el mismo y también respecto de las acciones necesarias ha llegado al caso de que se encuentre el mismo. ¿Cómo el uso

indebido del DNS se puede resolver en la Unión Europea? Hay una serie de pasos y medidas que se pueden encarar de acuerdo a los autores de la Unión Europea para resolver este problema.

En primer lugar, tenemos una recomendación de seleccionar proveedores con mayores estándares de validación de registraciones de dominios, tenemos que tener estándares de nivel, un enfoque que verifique quién es el cliente para verificar que el uso indebido del DNS no se provoque. Otro punto es iniciar soluciones de prevención y remediación.

Como se sugiere, estos son servicios que se preveían originalmente como servicios legítimos, pero hay ataques de phishing y hay explotaciones diversas, entonces hay que tener una detección proactiva de nombres de dominios sospechosos con claves de marcas que constituyan blancos. Otro tema es el incremento de la adopción de los controles de seguridad, por ejemplo, los sistemas o las extensiones de los nombres de dominios se deben autenticar con las comunicaciones dentro de los servidores de DNS.

Hay que evitar que los hackers tomen control de una sesión de búsqueda en internet y que deriven a los usuarios a sitios ilegítimos, también se tiene que utilizar protocolos específicos como primera línea de defensa contra estos ataques. Y los

últimos puntos son: Tener mejores estándares o normas en los dominios de alto nivel, el TLD es el componente final de un nombre dominio, tal como sabemos, y lamentablemente los TLD genéricos son los que sufren mayor uso indebido del DNS.

Hay unos gTLD nuevos, sin embargo, y ccTLD también nuevos que tienen una alta concentración de fraudes, dado que hoy en día es muy sencillo conseguir un TLD por menos de un dólar, entonces el informe sugiere que debe haber alguna medida de control sobre este problema. Muchas gracias.

Si tienen alguna pregunta, por favor, estoy dispuesta a proporcionar la respuesta.

DEBORAH ESCALERA: ¿Alguna pregunta? Hay una pregunta en la audiencia me parece, ¿quiere acercarse al micrófono? Muchas gracias.

DAVID [MARKIN]: Soy David [Markin] de la ICANN, gracias por la presentación. ¿Usted está pidiendo que ICANN haga más que lo que ya está haciendo? Por la dificultad de este tema, la privacidad de datos, la política de la Unión Europea, incluido, por ejemplo, lo que se llama NIS2, la directiva NIS2. Quizás pueda hablar un poco de qué es lo que desea que haga la ICANN en este momento, usted

puede sentarse y decir: “Bueno, creo que lo que tienen que hacer es esto para reducir el uso indebido del DNS”. ¿Qué es lo que solicita y cómo prevé usted que eso puede llevarse a cabo?

NADEZHDA ARTEEVA: Gracias, por la pregunta. Creo que este punto en particular fundamentalmente tiene que ver con la etapa del COVID-19, cuando hay crisis; que se dan a menudo, de pronto en esta situación debe haber una reacción más rápida, durante la pandemia este tema es una consecuencia que puede costar vidas humanas y problemas, esto puede llevar a que la gente tenga acceso a información falsa y también otros resultados negativos.

Estos son puntos críticos que algunos los establecen contra la ICANN, pero, en mi opinión, simplemente estamos viendo la manera en que la ICANN resolvió la crisis.

DEBORAH ESCALERA: Gracias. Parece que hay una pregunta en línea… Ah, era usted, bueno, muchas gracias y muchas gracias, David. Muy bien, ¿quiere acercarse al micrófono por favor? Muchas gracias.

ORADOR NO IDENTIFICADO: Hola. Hay información de las extensiones de gTLD que comentaban respecto de las nuevas, sabemos que hay algunas más antiguas que ofrecen nombres de dominios gratuitos, ¿qué opina?

DEBORAH ESCALERA: ¿Podría repetirla?

ORADOR NO IDENTIFICADO: ¿Tiene datos sobre los gTLD que estén más involucrados en este proceso de uso indebido del DNS?

NADEZHDA ARTEEVA: En los informes fueron presentados de manera breve, sin ejemplos, si hace falta podemos buscarlos. Desde la audiencia se aclara.

ORADOR NO IDENTIFICADO: Usted mencionó específicamente que este problema se da especialmente con los nuevos gTLD, así que, sospecho que .XYZ es uno o algún otro nombre. Quizás podría pasar su comentario en datos y si puede compartir, por favor, el origen de los datos y si no lo tiene no hay problema.

NADEZHDA ARTEEVA: Ese es el informe de la Unión Europea sobre uso indebido del DNS, lo puedo compartir con usted si así lo desea o algún otro documento que utilicé, hay una sección sobre recomendaciones de políticas sobre este tema.

DEBORAH ESCALERA: Muchas gracias. Todas estas presentaciones se van a subir en el sitio de la ICANN después del día de hoy y la presentación final es por parte de Liubomir Nikiforov, tiene la palabra.

LIUBOMIR NIKIFOROV: No estoy acostumbrado a estas presentaciones, muchas gracias. La próxima diapositiva por favor, la próxima diapositiva por favor.

Yo soy Liubomir Nikiforov, estudio en la Universidad de Barcelona y mi investigación está basada en el consentimiento informado, la transparencia y la gobernanza de internet. Hoy voy a hablar sobre la falta de guías precisas sobre el consentimiento y acuerdos entre registros y, por lo tanto, hay riesgos para la transparencia y la credibilidad para la ICANN y las partes interesadas de la ICANN. También voy a hablar de las posibles soluciones.

El proceso de registración actual de los dominios genéricos de alto nivel es un procedimiento contractual que incluye tres partes, que son: Un registrador que procesa registraciones de nombres de dominios, un registratario, una persona o una entidad que quiere registrar un nombre de dominio y un operador de registro, que es la entidad que mantiene el registro de los nombres dominios registrados dentro de un dominio de alto nivel.

Este acuerdo incluye un artículo; tiene varios, pero hay uno que nos interesa ahora, que es el número 2, párrafo 18 y establece los requerimientos de protección de los datos. Este artículo contiene también una definición de datos personales, requerimientos de notificación para los fines de los datos y también la identificación de quienes van a recibir los datos, y también habla del consentimiento. La próxima diapositiva, por favor, la próxima diapositiva.

Este es el artículo del cual estoy hablando y como pueden ver es el único artículo en el acuerdo base dedicado a los datos personales y tiene por objetivo incluir toda la información pertinente, todas las disposiciones pertinentes en relación a los datos personales, es muy difícil leerlo y entenderlo. Esto plantea algunas interrogantes en cuanto a su objetivo previsto y con la posibilidad de aplicarlo. La próxima diapositiva, por favor.

¿Cuáles son los desafíos? Hay muchos, sin embargo, me voy a centrar en los desafíos que tienen que ver con el requerimiento de consentimiento sobre el artículo 2, párrafo 18. Los registros deben obtener el consentimiento de cada registratario en el dominio de alto nivel para la recolección y el uso de datos personales. El artículo 2, párrafo 18, sin embargo, no especifica cuáles son los requerimientos para que este consentimiento tenga validez, ni la forma del mismo.

Para darles un ejemplo de este problema voy a utilizar la GDPR, el modelo de la normativa de protección de datos de la Unión Europea, según el GDPR para que el consentimiento sea válido debe ser informado, específico, gratuito y sin ambigüedad. Del artículo 2, párrafo 18 del acuerdo de registros y registradores, no entendemos cómo y cuándo debe obtenerse este consentimiento, si decide incluir una descripción completa y estricta de todos los objetivos para el procesamiento de datos.

¿Qué medio se podrían utilizar? Quizás la violencia, la intimidación sean medios válidos y si la información dada al registratario debe ser entendible parta el mismo. No sabemos si el registratario puede negarse a brindar el consentimiento y cuáles serían las alternativas, en este caso, si se niega a dar la información. La próxima diapositiva, por favor.

Pero ¿por qué es importante todo esto en última instancia? Porque vivimos en una sociedad basada que utiliza los datos, la información y los datos son algo que se pueda comercializar, por eso es importante garantizar la confianza de las partes interesadas de la ICANN, la credibilidad del sistema y también la confiabilidad, y otra vez la confianza, en cuanto a que haya una internet abierta y transparente.

En la Unión Europea tenemos algunas salvaguardas para el procesamiento de datos, pero ICANN opera a nivel global, los acuerdos actuales quizás puedan dar lugar a abusos por parte de los registratarios, un proceso donde el registratario comprende el objetivo y los resultados previstos del procesamiento de los datos. Esto beneficia al registratario, reduce la posibilidad de mal entendidos, juicios y brinda una ventaja competitiva a los registratarios y también beneficios en términos de reputación a la organización en su totalidad.

La próxima diapositiva, por favor. Como les prometí, voy a hablar de posibles soluciones. Una de ellas es la más obvia, revisar el artículo que mencioné, hacer que sea más claro y más fácil de entender, quizás dividirlo en subartículos o clausulas. En cuanto al consentimiento se deben identificar los casos en los que se necesita el consentimiento, también debe definirse

cuándo y cómo debe darse el consentimiento, y también se deben establecer los requerimientos para que sea válido.

Como ejemplo de esto se podría tomar el GDPR, donde el consentimiento debe ser una actividad activa, específica, libre, informada y no ambigua. Si podemos ver nuestra huella digital, que representa nuestra personalidad, el consentimiento informado es una de las garantías democráticas para nuestra dignidad digital. Muchas gracias y espero responder sus preguntas.

DEBORAH ESCALERA: Gracias, Liubomir. ¿Hay alguna pregunta? Voy a ver si hay alguna pregunta de algún participante en línea. Bueno, quiero recordarles que todas las presentaciones van a estar subidas al sitio web de la ICANN y si tienen alguna pregunta que se les ocurra después siempre me la pueden mandar por correo electrónico.

Quiero agradecerles a todos por estar aquí hoy en esta sesión y quiero recordarles que el segundo conjunto de presentaciones tendrá lugar mañana, y los invito a participar en esa sesión. Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]