SENADO
ARGENTINA

VERSIÓN TAQUIGRÁFICA

BUENOS AIRES – 2 de octubre de 2018

REUNIÓN PLENARIA DE LAS COMISIONES DE JUSTICIA Y ASUNTOS PENALES, Y DE SISTEMAS, MEDIOS DE COMUNICACIÓN Y LIBERTAD DE EXPRESIÓN.

SALÓN ILLIA– SENADO DE LA NACIÓN

PRESIDENCIA DE LOS SEÑORES SENADORES PEDRO GUILLERMO ÁNGEL GUASTAVINO Y ALFREDO HÉCTOR LUENZO

DGT DIRECCIÓN GENERAL DE TAQUÍGRAFOS

- En la Ciudad Autónoma de Buenos Aires, en el Salón Illia del H. Senado de la Nación, a las 14.17 del martes 2 de octubre de 2018:

Sr. Presidente (Luenzo).- Buenos días a todos.

Vamos a dar comienzo a esta reunión plenaria de comisiones, por disposición de la presidencia de la Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión. Por consiguiente, de manera conjunta, participa la Comisión de Justicia y Asuntos de Penales a fin de avanzar en el tratamiento de los siguientes proyectos de ley: el expediente S.-163/17, proyecto de ley de la señora senadora Fiore Viñuales, que reproduce el proyecto de ley modificando el Código Penal, tipificando los delitos de publicar por medios informáticos las imágenes de personas en actividades sexuales, y el robo de identidad.

Luego, el expediente S.- 2.449/18, proyecto de ley del señor senador Pichetto y otros, que modifica el Código Penal, sobre tipificar la usurpación de identidad virtual.

Además, se encuentra en consideración el expediente S.- 2.630/18, proyecto de ley del señor senador Lovera, por el que se incorpora el artículo 139 ter al Código Penal de la Nación por el cual se tipifica el delito de suplantación de identidad digital.

Finalmente, el expediente S.-2.722/18, proyecto de ley de la señora senadora Elías de Perez, que incorpora el artículo 139 ter al Código Penal de la Nación, por el cual se establecen penas por suplantación de identidad digital.

Dado este marco, en el día de hoy contamos con la presencia de varios invitados y obviamente vamos a escucharlos, más allá de lo que cada uno de estos proyectos considera.

Intentaremos avanzar, fundamentalmente, en las políticas de privacidad con las que se manejan las distintas plataformas −Facebook, Twitter y Google−; sobre todo las plataformas digitales, que obviamente hoy dominan las redes sociales aquí y en el resto del mundo.

La idea es poder avanzar, llegar a un punto de encuentro en cada uno de estos proyectos, pero también fijar algún tipo de política donde se hable de la responsabilidad no solo del usuario que se asume cuando se integra una de estas plataformas, sino cuál es la responsabilidad y hasta dónde llega la responsabilidad en la política de privacidad a respetar de estas plataformas digitales.

En principio, vamos a ir avanzando con cada uno de nuestros invitados en el día de hoy para conocer su opinión, como disparador de lo que acabamos de mencionar.

A continuación, vamos a escuchar al director de Políticas Públicas para Latinoamérica de Facebook, el señor Juan de Dios Batiz García.

Por favor…

Sr. Batiz García.- Buenas tardes, senadoras, senadores de este honorable y –tengo que decir también– muy bello recinto legislativo.

Me gustaría agradecer la invitación del senador Alfredo Luenzo, presidente de la Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión, así como la invitación del señor senador Pedro Guastavino, presidente de la Comisión de Justicia y Asuntos Penales, para poder estar con ustedes el día de hoy. Además, saludo y agradezco la presencia de los senadores y demás autoridades aquí presentes. Es para mí una distinción acudir al Honorable Senado de la Nación

Argentina y responder a las preguntas que los legisladores aquí presentes tengan el día de hoy.

Mi nombre es Juan de Dios Batiz. Soy director de Asuntos Públicos de Facebook para Latinoamérica.

El propósito de mi presencia es brindarles detalles sobre las políticas que rigen el uso de los servicios de Facebook y, de forma particular, la exigencia que tiene la plataforma para que las personas se identifiquen con su nombre auténtico. De esta forma, espero contribuir al importante debate que están realizando estas dos comisiones en torno al desafío de la suplantación de identidad.

Antes de adentrarme en las políticas de Facebook y en los esfuerzos de la empresa para prevenir en la plataforma los abusos, quisiera resaltar que Facebook es utilizado por más de 2.000 millones de personas alrededor del mundo, que constantemente publican miles de millones de piezas de contenido en forma de textos, fotografías y videos. Es por eso que las normas políticas y recursos de seguridad de la plataforma fueron desarrollados con el objetivo claro de dar a las personas el poder de conectarse y crear comunidades.

Asimismo, me gustaría informarles que las normas comunitarias de Facebook determinan claramente lo que está y lo que no está permitido en la plataforma. Navegar esa línea entre promover la libertad de expresión y mantener a la comunidad segura es uno de los grandes retos que enfrenta la empresa. Es por esto que cada una de sus políticas está basada en tres principios fundamentales: primero, dar a las personas la oportunidad de usar su voz; segundo, mantener a las personas seguras en la plataforma; y, tercero, tratarlas de manera justa, aplicando las políticas de manera consistente.

Las normas comunitarias evolucionan con el tiempo en base a la retroalimentación de la comunidad y a los cambios sociales y del lenguaje. Lo que no ha cambiado, y no cambiará, son los principios subyacentes de seguridad, voz y equidad en los que estas normas están basadas. Para Facebook, la equidad es un principio sumamente importante a la hora de aplicar las normas en una manera consistente y justa en todas las comunidades y en todas las culturas. Prueba de ello es que la empresa ha duplicado el número de personas que trabajan en más de 50 idiomas, las 24 horas al día, los 365 días del año, con el objetivo de proteger a los usuarios haciendo cumplir las normas comunitarias, la política de datos y la política de publicidad.

Me gustaría ser claro y decirles que lo más importante para Facebook es proteger la información de las personas. Como parte de nuestro compromiso de proteger la información de las personas, Facebook publica periódicamente un Informe de Transparencia que detalla los resultados de cómo hace cumplir sus normas, cómo responde a las solicitudes de datos, así como las acciones que realiza para proteger la propiedad intelectual.

Ahora bien, el objeto de la reunión es compartir con ustedes los esfuerzos que Facebook hace en torno a la suplantación de la identidad. Por ello, y con el propósito de dar puntual cumplimiento a lo solicitado, quisiera enfocarme en tres importantes políticas de Facebook que se relacionan directamente con el tema que discuten el día de hoy en las comisiones: primero, nuestra política de identidad real; segundo, políticas referidas a las figuras públicas; y, tercero, el trabajo para prevenir cuentas falsas y la suplantación de identidad.

Empecemos con la política de identidad real. Facebook está convencida de que las personas se comportan de manera más responsable cuando usan su

identidad auténtica en el mundo *online.* Por eso, exige que la gente que usa la plataforma se identifique con el nombre con el que son conocidos en sus comunidades. Esta política es importante, pues según algunos estudios las personas pueden ser hasta cinco veces más propensas a comportarse de manera respetuosa en la plataforma cuando usan sus nombres e identidades auténticas, o bien el nombre con el que son conocidos en sus respectivas comunidades.

Es importante enfatizar que Facebook prohíbe representar una identidad de forma engañosa mediante acciones como usar un nombre diferente al de la identidad real o al nombre por el que es conocido en su comunidad, o indicar una fecha de nacimiento falsa. También está prohibido suplantar a otras personas, lo que se entiende como crear un perfil o una página con el objetivo explícito de pretender ser o fingir hablar en nombre de otra persona sin su autorización, con intenciones evidentes de engañar a los demás para que, incorrectamente, piensen que ese perfil pertenece a alguien distinto a su verdadero creador. Ese comportamiento viola las políticas y, cuando Facebook toma conocimiento a través de reportes de usuarios o bien a través de órdenes judiciales, remueve esos perfiles o páginas.

Ahora bien, las políticas referidas a las figuras públicas: para Facebook es vital proteger la seguridad de las personas, incluyendo las figuras públicas. Quisiera resaltar que las políticas de Facebook prohíben la existencia de perfiles impostores sobre personas públicas, siempre y cuando se tengan pruebas y elementos suficientes que permitan tener certeza de que ese perfil es falso o impostor. El acoso, incluidas las amenazas de daño o violencia, discursos de odio, amenazas violentas con el fin de intimidar o silenciar a las personas están prohibidas, están prohibidas. También está prohibido el contenido creíble que pueda derivar en un daño en el mundo real; declaraciones que incentiven la violencia o sobre violencia condicional; expresiones como, por ejemplo, "desearía que alguien te mate" están prohibidas. Sin embargo, es importante manifestar que Facebook permite algunas páginas con nombres diferentes al del usuario que los creó como, por ejemplo, páginas de clubes de fans usados para compartir memes, hacer críticas a autoridades o empresas, o páginas de sátira, una forma de libertad de expresión protegida y necesaria. Facebook permite ese tipo de perfiles siempre que no representen engañosamente a una persona real.

Asimismo, considero importante resaltar el trabajo que Facebook viene realizando para prevenir el daño causado por cuentas falsas y la suplantación de identidad. Quiero ser enfático en señalar que las cuentas falsas en Facebook están prohibidas. Facebook está convencido de que las cuentas falsas ahogan las voces legítimas, dificultando una conversación auténtica. Es por ello que invierte tanto en la prevención, identificación y eliminación de la creación de cuentas falsas. Como explicaba antes, en el último año Facebook ha duplicado el tamaño de sus equipos dedicados al área de seguridad hasta llegar a las 20.000 personas. Facebook también está invirtiendo en nuevos y más sofisticados sistemas de aprendizaje automático e inteligencia artificial para detectar, bloquear y remover cuentas falsas. En el primer trimestre del 2018 identificamos y eliminamos más del 98 por ciento de las cuentas falsas, incluso antes de que éstas sean reportadas por la comunidad. Es importante destacar que Facebook analiza todos los reportes o denuncias recibidas, priorizándolas según el riesgo de daño, y que las investigaciones son realizadas de manera confidencial.

Otro punto relevante es que Facebook es respetuoso de las leyes locales y

coopera con las autoridades.

Para cerrar, quisiera reforzar la idea de que Facebook promueve la interacción verdadera entre las personas, y es por eso que exige que se registren en la plataforma usando su identidad auténtica. Para Facebook la seguridad es lo más importante y no está permitido el uso de perfiles falsos, la suplantación de identidad ni las cuentas falsas.

Espero contribuir en el debate del día de hoy para la formulación de leyes que promuevan una Internet libre, abierta y segura. Reconozco la disposición y el compromiso de todos ustedes para construir un mejor país, donde la libertad de expresión siga siendo la máxima en la vida de sus ciudadanos.

Quedo atento, y a entera disposición de las señoras y los señores senadores, para responder las preguntas que puedan tener respecto de esta intervención.

Por su atención, muchas gracias.

Sr. Presidente (Luenzo).- Bien. ¿Alguna consulta?

Senadora Brizuela.

Sra. Brizuela y Doria de Cara.- Gracias, presidente.

Muy buenas tardes; bienvenido y gracias por estar aquí.

Quisiera pedirle que nos explique cuál es el procedimiento que usa el sistema para verificar que una persona sea quien dice ser a efectos de evitar, justamente, la sustitución de identidad o abrir un perfil con un nombre que no es real.

Sr. Batiz García.- Gracias, senadora, por la pregunta.

Nosotros, como lo explicaba, tenemos un equipo de cerca de 20.000 personas que trabajan en todos los idiomas, incluyendo el castellano. La manera más sencilla de reportar cualquier contenido en nuestra plataforma es haciéndolo directamente en la plataforma. Cualquier perfil o cualquier posteo –con "contenido" me refiero a un posteo– en la parte superior derecha encuentra una serie de opciones. Al usted apachurrar o presionar ese botón le aparece una serie de opciones que le permite reportar los casos de suplantación.

Por otro lado, también invertimos en remover estas cuentas faltas: invertimos en tecnología y en sistemas automatizados con los que se detectan algunos patrones que nos permiten realmente, antes de que las cuentas sean reportadas, darnos cuenta de que se trata de cuentas falsas. La mejor manera de reportar una cuenta falsa o la suplantación de identidad es a través de nuestra herramienta, precisamente.

Sra. Brizuela y Doria de Cara.- Perdón que insista, pero es para tratar de entender.

Está claro cuáles son las políticas –estrictas– y el proceso que hay que hacer para reportar una cuenta; pero en forma previa a la apertura de un perfil, ¿no hay ningún procedimiento que permita constatar la identidad de la persona que está generando ese perfil?

Sr. Batiz García.- En forma previa, nosotros realmente nos basamos en nuestra comunidad. Le voy a dar un ejemplo: mi nombre es Juan de Dios Batiz García; eso aparece en mi DNI. Sin embargo, mi cuenta de Facebook aparece como Juan Batiz; y aparece como Juan Batiz porque mis amigos, mis familiares, mis conocidos me conocen como Juan Batiz. Aún si yo pidiera una identidad previa a eso, no habría un "macheo" entre Juan de Dios Batiz García y un Juan Batiz.

Habiendo dicho esto, lo que sí nos parece importante es compartir con ustedes que nosotros recibimos miles y miles y miles de reportes todos los días. Entonces, si alguien de la comunidad –miembro de la comunidad–, en cualquier parte del mundo, decidiera reportar que quizás la cuenta del señor Juan Batiz es

falsa o impostora, eso se va al equipo que revisa esto; y, en algunos casos muy específicos, pudieran preguntarle al señor Juan Batiz que nos mandara una identificación para cerciorarnos de que efectivamente es la persona; y, si no es, se remueve. Pero sí dependemos mucho de los reportes de la comunidad.

Sr. Presidente (Luenzo).- Senadora Fernández Sagasti.

Sra. Fernández Sagasti.- Gracias, presidente; buenas tardes.

Sr. Batiz García.- Buenas tardes.

Sra. Fernández Sagasti.- Quería hacerle varias preguntas; muy concisas las respuestas, si es posible.

Obviamente, los proyectos que tenemos a la vista –no sé si usted los ha podido leer– tienen una sanción penal en caso de usurpación de identidad en las redes sociales: Internet, etcétera, etcétera.

La primera pregunta que le quería hacer es: primero, ¿cuántos reportes por año tienen de suplantación de identidad en la Argentina? Si usted tiene ese número: las denuncias que recibe Facebook de suplantación de identidad.

Segundo, ¿si nos pudiera usted ilustrar qué pasa con la legislación comparada? ¿Si en esto existen condenas civiles o penales respecto de la usurpación de identidad en Internet o en las redes sociales? Y, si es así, ¿cuáles fueron los fundamentos en uno u otro caso?

También, si usted tiene una opinión o la empresa ha trabajado una opinión respecto de cómo se podría obtener el mismo resultado evitando una condena penal; si lo han trabajado como propuesta o como aporte al debate, porque hemos recibido los legisladores varias manifestaciones en contra de legislar penalmente o penar la usurpación de identidad en las redes sociales, porque entienden algunas organizaciones de la sociedad civil que se estaría afectando la libertad de expresión. Entonces, quería saber cuál es su opinión y si tienen alguna alternativa que hayan trabajado respecto de esto.

Sr. Batiz García.- Gracias, senadora, por su pregunta.

A la primera pregunta "cuántos casos en la Argentina sobre suplantación de identidad", la respuesta es que específicamente, de suplantación de identidad, no lo sé. Lo que sí sé es que en el año 2017 recibimos aproximadamente dos mil peticiones de autoridades locales –de la Fiscalía, de la Policía Federal, de la Policía de Seguridad Aeroportuaria–, y se dio cumplimiento y se dio respuesta al ciento por ciento de esas solicitudes. Nosotros tenemos un equipo especializado que trabaja muy de cerca con estas autoridades que nos solicitan información para los fines que la autoridad en este punto corresponda y nosotros en 2017 dimos respuesta al ciento por ciento de esas solicitudes. De esas dos mil, había casos de suplantación de identidad.

Sra. Fernández Sagasti.- Si bien usted no tiene el dato, como acaba de decir, me gustaría preguntarle si nos podemos hacer de ese dato para que nos lo mande a la comisión, porque la verdad es que estaríamos viendo cuál es la magnitud de lo que estamos hablando: cuántas solicitudes a través de la misma página, no oficios judiciales ni de lo que estamos hablando, si no cuántas solicitudes, que es una aplicación que tiene la página, de denuncia, de usurpación de identidad o por sustitución de identidad han registrado ustedes en la Argentina.

Si usted después puede acercarlo a la Presidencia, si se puede hacer de ese dato, me parece que sería muy conveniente para poder tomar la decisión de qué es lo que estamos legislando.

Sr. Batiz García.- Con mucho gusto: podemos conseguir ese dato y, efectivamente,

lo puedo dejar aquí con los presidentes.

En el tema de la opinión acerca de la legislación, sí tuve oportunidad de verlas. En lo que sí quiero ser claro es en que siento que la participación de Facebook es aportar en lo que hacemos nosotros como empresa. Creo que depende de los senadores y de los diputados, en su momento, decidir cuál es la regulación que es mejor o no para sus ciudadanos.

Entonces, en ese sentido, no puedo comentar puntualmente porque no me corresponde, no me corresponde.

Sr. Presidente (Luenzo).- ¿Alguna otra consulta?

– No se producen manifestaciones.

Sr. Presidente (Luenzo).- ¿Cómo ven ustedes la posibilidad de la regulación? Porque este es un tema que se está debatiendo a nivel global: se está intentando en Europa; en Estados Unidos, frente a un caso emblemático por el cual ha tenido que atravesar Facebook. ¿Cómo ven las regulaciones y hasta qué punto ustedes entienden que los Estados tienen que involucrarse también en esas políticas de privacidad, de protección de la identidad, y de todo lo que usted acaba de enumerar? No solamente sustitución de identidad sino de contenidos de toda naturaleza. ¿Cómo debe actuar el Estado, o cómo entenderían ustedes que debe actuar, en función de una política que ustedes desde la misma plataforma están aplicando?

Sr. Batiz García.- Gracias, senador, por la pregunta.

A mí me parece que la regulación… Podemos hablar de muchos temas y creo que la pregunta acertada –como usted lo indica, senador– es qué tipo de regulación; qué tipo de regulación es la que se necesita; en qué ámbito; en qué tema. En ese momento, obviamente nosotros podemos expresar cómo funciona, cómo opera, qué es lo que hacemos; podemos aportar en el conocimiento de nuestra plataforma y en el desconocimiento de ésta, porque también hay mucho desconocimiento de cómo funcionamos. Me parece que con esa información que nosotros podemos aportar –y repito un poco–, corresponde a los legisladores ver qué tipo de regulación. Pero sí quiero ser claro en que Facebook no se opone a la regulación.

Creo que la regulación tiene que ser sensible, práctica y también que no inhiba la innovación, porque al final del día la innovación ha sido y sigue siendo un motor importante económico en la Argentina y en otros países alrededor del mundo.

Sr. Presidente (Luenzo).- ¿Cómo articulan su relación con la Justicia, señor?

Sr. Batiz García.- ¿Discúlpeme, senador?

Sr. Presidente (Luenzo).- ¿Su relación con la Justicia cómo la articulan? ¿En función de las demandas, de los pedidos de intervención, cuando se trate no solamente sustitución sino de comentarios agraviantes o de cualquier otra naturaleza o de imágenes no permitidas? ¿Cómo articulan ustedes ese vínculo con la Justicia para poder actuar?

Sr. Batiz García.- Gracias, senador.

Nosotros tenemos en nuestra página distintos recursos que son diseñados exclusivamente para las autoridades. Entonces, mucha de la relación que nosotros tenemos en Facebook es una relación proactiva que se basa en la capacitación a esas autoridades para mostrarles a dónde ir, qué procedimiento seguir, cuándo requieren información nuestra.

Nosotros en todo momento cooperamos con las autoridades locales; mencioné algunos ejemplos aquí. El año pasado –me parece que en septiembre de

2017– tuvimos una capacitación con 400 agentes de la Fiscalía, a los que se les enseña y se les apoya para enseñarles –si lo queremos de alguna manera decir– cuál es la mejor forma para obtener la información que ellos necesitan, que pueden ser contenidos, imágenes, datos, etcétera.

Sr. Presidente (Luenzo).- ¿Alguna otra consulta?

– No se producen manifestaciones.

Sr. Presidente (Luenzo).- Muchísimas gracias, señor García.

Sr. Batiz García.- Muchas gracias.

Sr. Presidente (Luenzo).- Muy amable, muy gentil.

Seguimos avanzando. Vamos a escuchar la opinión del señor Hugo Rodríguez Nicolat, responsable de política pública de Twitter en Latinoamérica.

Sr. Rodríguez Nicolat.- Buenas tardes.

Honorables senadores y senadoras: estoy agradecido por la oportunidad de poder dialogar con los miembros de estas comisiones el día de hoy.

El propósito de Twitter es servir a la conversación pública y logramos esto al servir a la audiencia global, así como al enfocarnos en las necesidades de las personas que usan la plataforma. Esta es la razón por la cual nos esforzamos por construir un espacio confiable y saludable, que apoya el debate libre y democrático, así como la razón por la cual agradecemos esta audiencia el día de hoy.

Ahora, antes de profundizar en la temática que nos convoca en esta sesión, permítanme primero describir aspectos claves de Twitter que serán importantes para nuestras discusiones.

En Twitter estamos comprometidos con brindar un servicio que fomente y facilite el debate abierto, libre y democrático, donde las personas reaccionen, comenten, interactúen y critiquen el contenido que ellos mismos, u otras cuentas, deciden compartir.

Creemos que todos deberían tener el poder de crear y compartir ideas e información de forma instantánea, sin barreras de por medio. Para lograrlo, Twitter necesita proveer un espacio donde las personas se sientan seguras de comunicar en la plataforma.

Es fundamental tener la capacidad de eliminar a los actores de mala fe que pretenden utilizar la plataforma de Twitter para dividir, amenazar o manipular; pero al mismo tiempo, el éxito de compañías como Twitter, que han permitido a millones de personas en todo el mundo nuevas oportunidades de expresión, ha dependido de un marco legal que reconoce que los usuarios son responsables de lo que publican. Cambiar esto puede poner en riesgo avances en materia de innovación, competencia y libertad de expresión, que han permitido plataformas como ésta.

Es importante subrayar que, para proteger la experiencia de las personas en Twitter, existen ciertas limitaciones al tipo de contenido y conductas que permitimos en la plataforma. Estas limitaciones están establecidas en las reglas de Twitter. Todos los individuos que acceden o utilizan los servicios de Twitter deben adherirse a estas políticas establecidas. En caso de no hacerlo, Twitter puede derivar en alguna de las siguientes acciones o medidas: requerir al dueño de la cuenta que elimine el contenido en violación de las reglas; limitar temporalmente a los usuarios la posibilidad de postear o interactuar con otras personas en la plataforma; solicitar la verificación de la propiedad de la cuenta; requerir al propietario de la cuenta ciertas acciones que comprueben que la cuenta no está automatizada; o suspender cuentas de forma permanente. Si las personas intentan evadir una suspensión permanente, creando nuevas cuentas, por ejemplo, seguiremos suspendiendo

dichas cuentas.

Las reglas de Twitter son un documento vivo. Continuamos ampliando y actualizando tanto nuestras políticas, como también nuestras opciones de aplicación, para responder a los entornos siempre cambiantes de la conversación en línea.

Continuemos ahora con la temática que nos convoca el día de hoy: cómo enfrentar casos de suplantación de identidad digital.

Entre las reglas de Twitter mencionadas anteriormente, hemos desarrollado la política de suplantación. Dicha política –y cito– establece: No puede suplantar la identidad de otras personas, grupos u organizaciones, de manera que intente o, de hecho, logre confundir, engañar o comunicar una idea equivocada a otras personas. Si bien puedes administrar cuentas de parodias y admiradores, no puedes hacerlo si el propósito de la cuenta es enviar *spam* o cometer abusos.

Es importante señalar que las cuentas con nombres de usuario o apariencia similares –por ejemplo, que utilicen la misma foto de perfil– no están consideradas automáticamente como violación a la política de suplantación de identidad. Para ser considerada como tal, la cuenta debe representar a otra persona de manera errónea o engañosa.

Las personas pueden reportar una cuenta ante sospecha de suplantación de identidad directamente desde el perfil de esa cuenta o en nuestro Centro de Ayuda. Aclaramos que no es necesario tener una cuenta en Twitter para informar sobre la violación de esta regla en la plataforma. Tras recibir un reporte, Twitter investigará las cuentas para determinar si infringen las reglas de Twitter descritas anteriormente. En caso de ser necesario, el equipo de Twitter pedirá a la persona que reporta que envíe información adicional que ayude a contextualizar el caso. La debida diligencia de esta documentación es importante para garantizar que hemos recibido información precisa que nos permita determinar la respuesta al caso reportado. Aquellas cuentas que infrinjan nuestra política de suplantación, o las que no cumplan con la política de parodia, serán suspendidas o se les pedirá que realicen cambios para que no violen nuestros términos. Si esos cambios no son realizados serán suspendidas.

También existe una forma para que las personas en Twitter identifiquen rápidamente la veracidad de las cuentas de interés público: las insignias de verificación. La insignia azul de Twitter permite a las personas saber si una cuenta es auténtica. Esta insignia aparece justo al lado del nombre del perfil y al lado del nombre de la cuenta, en los resultados de búsqueda.

Aclaramos que, si bien por el momento, hemos suspendido la solicitud pública de verificación, en lo que respecta a los funcionarios públicos nos hemos comprometido a verificar las cuentas de funcionarios electos y públicos, así como las cuentas de los principales líderes del sistema político argentino como una forma de facilitar la identificación de estas figuras en la plataforma de Twitter.

Dado que actualmente los formularios públicos para verificar las cuentas están en pausa, invitamos a los funcionarios y actores del sistema político previamente referidos a contactarnos para recibir instrucciones sobre cómo verificar estas cuentas.

Honorables senadores y senadoras: aprovecho esta oportunidad para también referirme a los esfuerzos que hemos emprendido en Twitter para abordar cuestiones relacionadas con los intentos de manipulación en nuestra plataforma.

Como mencionamos anteriormente, el propósito de Twitter es servir a la

conversación pública. Twitter es utilizado globalmente como un ágora donde personas de todas partes del mundo se reúnen en un espacio abierto para intercambiar ideas libremente.

Trabajamos para ser una plataforma confiable, que respalda la discusión libre y abierta. Twitter se ha comprometido públicamente a mejorar la apertura, la civilidad y la salud de las conversaciones públicas en nuestra plataforma.

Medimos nuestra salud por la forma en la que ayudamos a fomentar un debate más abierto, con conversaciones y pensamiento crítico. Por el contrario, el abuso, la automatización maliciosa y la manipulación, menoscaban la salud de nuestra plataforma.

Nos comprometemos a hacernos responsables públicamente del progreso de nuestras iniciativas de salud. Por ello, durante el año pasado perfeccionamos nuestras herramientas y mejoramos nuestra velocidad de respuesta, a la vez que identificamos áreas de evidente necesidad de mejora.

Twitter es una plataforma única en cuanto provee un espacio abierto, donde la naturaleza de la información en tiempo real es un poderoso antídoto contra la difusión de todo tipo de información falsa. Esto es fundamental, dado que no podemos distinguir si cada twit de cada persona es veraz o no.

Creemos que no deberíamos ser los árbitros de la verdad. Día a día vemos a periodistas, expertos y ciudadanos comprometidos que twitean ambos lados de la historia, corrigiendo y deshaciendo el discurso público en segundos, como parte de una vibrante conversación pública. Estas vitales interacciones ocurren en Twitter todos los días. Por ello, trabajamos para asegurar que el contenido y el contexto de mayor calidad y relevancia sean lo que primero vean y lo que predomina en la plataforma.

Twitter cree firmemente que debe haber un compromiso significativo, con métricas rigurosas e independientes, que ayuden a mantener una conversación pública saludable en la plataforma. Para lograrlo, hemos tomado iniciativas colaborativas que nos permiten contar con el aporte de externos. Por ejemplo, a comienzos de este año colaboramos con el Centro de Investigación sin fines de lucro Cortico y con el Instituto Tecnológico de Massachusetts, el *Media Lab,* para explorar cómo medir aspectos de la conversación pública. Y, con el fin de desarrollar estas métricas referidas, solicitamos también expertos de distintas organizaciones que propongan las métricas y métodos para capturar, medir, evaluar e informar sobre nuestros resultados. Nuestra expectativa es que estas alianzas produzcan artículos de investigación revisados por pares y que sean públicamente disponibles.

Como resultado de este llamado a la colaboración, nos estamos asociando con la Universidad de Oxford, con la Universidad de Leiden y otras instituciones académicas, para mejorar la métrica de salud en Twitter, centrándonos en las cámaras de eco informativas y el discurso insalubre en la plataforma. Esta colaboración también nos permitirá estudiar cómo la exposición a una variedad de perspectivas y opiniones es beneficiosa en la reducción de los prejuicios y la discriminación en general.

Aclaro que estos proyectos no se centran en ningún grupo ideológico en particular, y los resultados se publicarán en su totalidad en su debido tiempo para un debate posterior.

Con respecto a las cuentas de actividades que buscan manipular o interrumpir la conversación y violar nuestras reglas contra el *spam*, estamos

trabajando activamente para mitigar este daño. Vale la pena aclarar qué es *spam*, que se define en Twitter como una actividad masiva o agresiva que intenta tergiversar o interrumpir la experiencia de las personas en Twitter para traer tráfico o atención a cuentas, productos, servicios o iniciativas no relacionadas con la conversación que se está dando.

Debido a las mejoras en la tecnología y a los procesos que hemos implementado, ahora eliminamos un 214 por ciento más de cuentas, año tras año, por violar las políticas de manipulación de nuestra plataforma. Por ejemplo, en el transcurso de los últimos meses, nuestros sistemas identificaron y desafiaron entre 8.5 millones y 10 millones de cuentas semanales bajo sospecha de violar nuestra regla de automatización y *spam*. También frustramos más de 530.000 inicios de sesión sospechosos por día: aproximadamente el doble de los inicios que detectábamos hace un año. Aclaro: esto no quiere decir que el problema se haya acrecentado sino que nuestro sistema se ha vuelto más capaz de hacer frente a este reto.

Estas mejoras tecnológicas han reducido significativamente el número de denuncias que por materia de *spam* realizan los usuarios de Twitter. Recibíamos aproximadamente 25.000 de esos informes de manera diaria en marzo de este año, y este número ha bajado hasta 16.000 en lo que corresponde diariamente al mes de septiembre.

Senadores y senadoras: por último, en relación a la legislación específica que está considerando este Honorable Senado, como hemos dejado en claro en el número de acciones que he enumerado, en Twitter coincidimos con el interés de los legisladores por proteger al público de la posible práctica de desinformación. No obstante, y de manera respetuosa, discrepamos sobre los medios para lograrlo. Sobre este tema, coincidimos con los argumentos generales expuestos por las organizaciones como CELE y otros grupos en la carta enviada a la Comisión de Justicia y Legislación Penal del 28 de agosto del año en curso. Estos argumentos se basan en su mayoría en los principios establecidos en la Declaración de Principios de la Comisión Interamericana de Derechos Humanos.

Sobres estos comentarios es importante subrayar que el uso de un nombre específico no puede justificar por sí solo un delito punible. La parodia y la sátira son componentes esenciales del discurso democrático.

En Twitter protegemos y respetamos la capacidad de las personas de elegir su propio nombre. Es por eso que nuestra política de suplantación considera que la intención de la cuenta es relevante al reforzar que, para violar estas reglas, no es suficiente tener el mismo nombre o un contenido similar sino representar a otra persona de manera engañosa.

Además, coincidimos con la conclusión de estas organizaciones de que, para poder enfrentar los desafíos de la desinformación sin correr el riesgo de menoscabar la libertad de expresión, se requiere un abordaje más amplio y creativo, como puede ser una campaña de concientización y formación cívica para el buen manejo ciudadano de información en redes sociales y en otros entornos digitales.

Para ser claro: Twitter está comprometido con cuidar y facilitar el debate democrático y abierto en su plataforma, y promover así un cambio positivo en el mundo.

De enero de 2017 a la fecha hemos anunciado alrededor de 100 cambios de productos y docenas de nuevos cambios de política, mejoras en la seguridad de la aplicación y sus operaciones, así como hemos fortalecido la estructura de nuestro

equipo con el objetivo de hacer que Twitter sea más seguro e incrementar la calidad de información en nuestra plataforma.

Continuaremos mejorando nuestros sistemas internos para detectar y prevenir actividades que degraden la calidad de la información, al mismo tiempo que continuamos trabajando para educar al público sobre nuestras reglas y herramientas de seguridad, ayudándolos a identificar y utilizar contenido de calidad en Twitter.

Nuestro trabajo está lejos de haber terminado. Esto es solo una parte del esfuerzo que realizamos para mejorar la salud de la conversación y la experiencia de todos en Twitter.

Nos estamos moviendo hacia un modelo operativo donde somos más abiertos y transparentes sobre cómo trabajamos y operamos. Reconocemos que este es solo un primer paso de un largo viaje, pero reforzamos nuestro compromiso de seguir mejorando la experiencia de nuestros usuarios en la plataforma.

En verdad, señores presidentes, senadoras, esperamos esto abone a las discusiones y me refrendo a su disposición para dudas que puedan tener al respecto; muchas gracias.

Sr. Presidente (Luenzo).- Gracias.

¿Alguna consulta, senadores?

– No se producen manifestaciones.

Sr. Presidente (Luenzo).- Usted admite que, evidentemente, hay un mecanismo que se tiene que ir perfeccionando frente a las dificultades que van apareciendo. Estas dificultades uno las puede entender como personas que se han visto perjudicadas por cuentas que, obviamente, no han sido debidamente verificadas o por múltiples razones.

¿Usted no cree que tanto Twitter, como cualquier otro tipo de plataformas, como intermediario entre los actores que tienen estas plataformas, no tiene que asumir algún tipo de responsabilidad?

Sr. Rodríguez Nicolat.- Gracias, senador.

La responsabilidad principal que asume Twitter es con la salud de la conversación; y, por eso, toda la tecnología, procesos y políticas –los más de 100 cambios que hemos hecho–, están con el fin de nutrir este debate libre, abierto y democrático, que es servir a la conversación pública.

La otra responsabilidad que asume la plataforma es dar herramientas claras, entendibles y accionables para reportar conjuntamente este contexto que es tan cambiante como es la discusión *online.*

Nuestro compromiso es ser diligentes cuando recibimos un reporte, accionarlo y dar la respuesta que requiere esa situación.

Sr. Presidente (Luenzo).- Pero a veces la inmediatez no repara el daño que se ha provocado. Digamos, ¿quién se hace responsable de ese daño?

Sr. Rodríguez Nicolat.- Gracias, senador.

El tema esencial que buscamos nosotros con tener procedimientos claros es que la gente y los usuarios de la plataforma conjuntamente entendamos esta responsabilidad que tenemos al tomar medidas como la eliminación permanente de sus cuentas. Repito –esto es sumamente esencial–: una vez que los eliminamos no pueden regresar a la plataforma. Tenemos una regla de eliminar a esos usuarios para que no puedan volver a transferir.

Creemos que de manera paulatina, conjuntamente, podremos lograr un espacio en el cual impere la libertad de expresión sin ningún socavamiento.

Sr. Presidente (Luenzo).- Si me permite, le voy a hacer una analogía. Los medios

tradicionales de comunicación, que tienen los mismos principios –exactamente los mismos principios– pero que tienen, obviamente, un formato diferente, si me remito a un diario hay un editor responsable: es decir que cuando transita por un medio hay un responsable de las cosas que se publican y que transitan por ese medio.

¿Por qué no debería ser de la misma manera en las plataformas digitales?

Sr. Rodríguez Nicolat.- Gracias, senador.

El éxito y lo que ha cambiado la tecnología, lo que apuntala espacios de libertad de expresión *online* –que es más viral, más horizontal, más participativo–, es precisamente lo que permite que estas plataformas –no somos quienes publicamos la información sino quienes damos el espacio para que los usuarios sean los generadores de contenido– tengan esta salvaguarda.

Los usuarios son, al final de cuentas, responsables de este tipo de interacción pero, ¡ojo!: coincidimos en el hecho de que hay cierto tipo de interacciones que no son deseables. Por eso hay líneas, reglas y procedimientos que hacemos públicos a cualquier persona que se inscribe en la plataforma y que damos seguimiento.

El objetivo es que todos los usuarios conozcan las reglas, sepan que son accionables y, por ende, tengan conciencia de las repercusiones que pueden tener sus acciones para no reincidir. Pero este espacio público y horizontal depende de este marco y andamiaje legal donde se reconoce que los usuarios son responsables de lo que producen. Las plataformas somos responsables de tener mecanismos a través de los cuales se ejecuten las reglas.

Sr. Presidente (Luenzo).- ¿Hay reclamos? ¿Con qué periodicidad, cuál es el nivel de demanda que tienen por parte de la Justicia frente a hechos que –no voy a remitirme a ninguno en particular– son de público conocimiento, o no, que suceden, te diría, casi todos los días?

Sr. Rodríguez Nicolat.- Claro, senador: en este tema, dos elementos que me parece son muy útiles para su abordaje en la materia. El primero, al igual que otras industrias en la materia, Twitter tiene un Reporte de Transparencia que publica de manera semestral, en el cual los usuarios pueden ver el número de requisiciones o solicitudes de información que se han dado por parte de las autoridades a nivel global. Evidentemente, esto incluye también a la Argentina. El otro tema es el número de reportes que tenemos, que son producto de los propios usuarios.

Una métrica ahí interesante para conocimiento de todos ustedes es que la gran mayoría, sino es que casi la totalidad de los reportes de violaciones a las reglas de Twitter, proviene de un uno por ciento de la plataforma. Entonces, el objetivo es ser muy diligentes con el seguimiento que recibimos para que ese uno por ciento –¡ojalá!– se reduzca hasta un porcentaje minúsculo que abone a la buena conversación en línea.

Sr. Presidente (Luenzo).- ¿Cuántas cuentas tienen en la Argentina aproximadamente?

Sr. Rodríguez Nicolat.- Tenemos 335 millones de usuarios activos a nivel global, senador. No damos…

Sr. Presidente (Luenzo).- ¿No pueden identificar por región o por países?

Sr. Rodríguez Nicolat.- No tenemos datos públicos sobre países en particular, senador.

Sr. Presidente (Luenzo).- Bien; te agradezco; muy amable.

Vamos a escuchar al doctor Eduardo Bertoni, que es el director de la Agencia de Acceso a la Información Pública.

Sr. Bertoni.- Muchísimas gracias por la invitación.

Algunas precisiones que entiendo la mayoría de quienes están aquí presentes –senadores, senadoras, asesores, expertos, expertas– conocen, pero que creo que es importante hacer la mención.

Desde el año pasado la Agencia de Acceso a la Información Pública, como ente autárquico y con autonomía funcional creado por la Ley de Acceso a la Información Pública sancionada en el año 2016 –la Agencia también es, como decía, desde el año pasado la Autoridad Nacional de Protección de Datos Personales–, es el órgano de control que menciona la ley 25326, que es la ley que nos rige sobre protección de datos personales. En ese sentido, entiendo que ha sido girada la invitación para exponer ante estas honorables comisiones del Senado y, en esa capacidad, voy a hacer algunas referencias al tema que estamos discutiendo, sin perjuicio, por supuesto, de quedar abierto para responder algunas preguntas o comentarios que quisieran hacerse.

Me parece que alguna información puede ser útil para el proceso que está llevando adelante el Senado vinculado con este problema, que lo vamos a poner bajo el título de suplantación de identidad.

Sin perjuicio de que los distintos proyectos se aproximan al problema de distinta manera –algunos hablan de usurpación, otros de apoderamiento, algunos de suplantación–, si nos pusiéramos el gorro de profesor de Derecho Penal de la Universidad de Buenos Aires podríamos discutir algunas cuestiones vinculadas con el principio de legalidad; pero lo que sí quiero señalar es que esta cuestión bajo el título "suplantación de identidad" es un problema. No podemos soslayar que estamos frente a un problema. La pregunta es cómo aproximarnos a la solución de este problema; y había una senadora que preguntaba si la herramienta penal era o no era, pero eso no es parte de mi comentario ahora. Puedo ampliar después, si fuera necesario.

Partiendo de la base de que es un problema, sí quiero destacar que en la legislación vigente, particularmente en la Ley de Protección de Datos vigente, existe la posibilidad de ejercer tanto el derecho de acceso a nuestros datos personales como al derecho de supresión de datos que pudieran ser atribuidos a nosotros y que estuvieran incorrectos. Esto ya está fijado en la Ley N° 25.326 –de antigua data–, del año 2000. Son derechos que recogen casi todas las leyes de protección de datos personales en el mundo y son derechos que también han sido incluidos como derechos importantes en el proyecto de reforma de la Ley de Protección de Datos Personales que el Poder Ejecutivo Nacional envió al Congreso, y que entiendo ya se encuentra en trámite ante el Senado.

¿Qué significa la posibilidad de ejercer el derecho de supresión? Significa que en tanto yo detecte un dato personal –y aquí el nombre sin dudas es un dato personal, inclusive en los términos definidos por la ley; "dato personal" es todo aquel dato que identifica o hace identificable a una persona; me parece que al discutir si el nombre es un dato personal o no ya estaríamos en otro tenor de la discusión–, la ley permite solicitar al responsable de la base de datos que contiene ese dato tanto que me informe qué datos personales míos se tienen como la posibilidad de suprimir algún dato que sea inexacto.

Este andamiaje, este diseño de la ley vigente –e, insisto, también contenido en el proyecto que prontamente estará en estudio–, creo que se aproxima a este problema. La cuestión sería qué pasa después; y, en el qué pasa después, el procedimiento que se establece en la ley vigente a través del órgano de contralor es un procedimiento de un órgano administrativo sancionador y que puede culminar

con una sanción al responsable de la base de datos que no haya hecho lugar al ejercicio del derecho del titular de los datos y que ese derecho, obviamente, corresponda. Ahí sí tengo que hacerme absolutamente cargo de una cuestión, que es cuál es el tipo de sanción. La ley vigente establece como máxima sanción un monto de 100 mil pesos. Por supuesto que para compañías grandes, y algunas no tan grandes, esta sanción puede no ser muy influenciable para que hagan lugar a este tipo de ejercicio de derechos. Por eso, entre otras cosas, una de las cuestiones importantes del proyecto lo que hace es modificar el régimen sancionatorio para cualquier infracción que pudiera ocurrir en los términos de la ley.

Tal vez ustedes habrán escuchado que, desde la entrada en vigencia del nuevo reglamento europeo para la protección de datos personales, una de las cuestiones importantes que ha circulado es el monto de las multas, que están relacionadas con un porcentaje de las ganancias globales de las empresas. Esto ha generado una discusión importante; pero si las multas pueden tener un efecto disuasorio, para que se dé, tienen que tener montos que en la realidad tengan un efecto disuasorio.

Quiero contarles ahora algunas otras cuestiones que también hacemos desde la Agencia de Acceso a la Información Pública –más precisamente desde la Dirección Nacional de Protección de Datos Personales, que es una de las dos direcciones nacionales que posee la Agencia– y que se vincula con esta cuestión de la suplantación de identidad, que es lo que nosotros llamamos como la Base de Datos de Documentos Cuestionados. Esto es algo que está implementado desde hace mucho tiempo en lo que era antes la Dirección Nacional de Protección de Datos Personales y consiste, muy sencillamente, en que cualquiera que haya perdido o le hayan robado o hurtado su Documento Nacional de Identidad tiene la posibilidad de acercarse –ahora, incluso hemos agilizado el sistema y se puede hacer a distancia– a la Agencia y denunciarlo como tal. Ese documento –ese número de documento– entra en una base de datos, que es nuestra Base de Datos de Documentos Cuestionados, y lo que genera, a través de disposiciones del Banco Central de la República Argentina, es que todas las entidades financieras, bancarias o crediticias, antes de otorgar un crédito tengan que consultar esta base de datos. Es decir: si alguien va con un documento que no es el propio sino el que encontró para sacar un crédito, ese documento enseguida va a aparecer como un documento cuestionado y ese crédito no se le va a otorgar a la persona. Tenemos varios casos o ejemplos de casos en que esto ha funcionado de esta manera.

Me hago cargo también de que estoy hablando de una suplantación de identidad, ya no en el mundo digital sino en el mundo predigital, en el mundo analógico. Estoy hablando de mi viejo DNI marrón o verde, después celeste y ahora una tarjeta, y no hablo de una identidad digital, que también debería definirse de qué se trata.

Números como para ir terminando y dar alguna información a la comisión que trabaja en estos temas y que les pueden ser útiles. Denuncias por documentos cuestionados del presente año, tenemos 4.282. La Base de Datos de Documentos Cuestionados no llega a las 100 mil: son alrededor de 95 mil documentos cuestionados. Eso es desde la creación de la Base de Datos.

Ahora, fíjense ustedes cuando hacemos el salto a cuántas denuncias tenemos por violación a la Ley de Protección de Datos Personales, que podría ser violación al derecho de supresión: es decir, pedí que supriman un dato y no lo suprimieron. Bueno: el total de denuncias durante este año por violación a la Ley N°

25.326 no llega a las 150; por intentar ejercer el derecho de supresión, no llegan a las 60: y por un perfil falso en una plataforma hay una sola. ¿Qué quiero decir con todo esto? Quiero decir que la herramienta de la Ley de Protección de Datos Personales es una herramienta que existe, que está ahí y que no se está usando, tal vez a cabalidad. La respuesta puede ser que haya algún grado de desconfianza sobre qué va a pasar cuando se hace la denuncia: desconfianza en el sentido de si sirve o no sirve.

Algunos datos son positivos, en algunos casos que nosotros hemos intervenido –no de perfiles falsos, pero sí de desindexaciones de contenidos– las plataformas digitales han desindexado contenidos una vez que los notificamos de la denuncia que se está tramitando en la Dirección: en otros casos, no. El caso que le estoy refiriendo de perfil falso es un caso que esta abierto y que, eventualmente, podrá terminar en una sanción del tipo de las que yo le comentaba.

Por supuesto que el desafío por delante no solo es mejorar la legislación vigente sino también promover esto como una herramienta posible para mejorar –y vuelvo al comienzo– el problema del cual nos tenemos que hacer cargo; muchas gracias.

Sr. Presidente (Luenzo).- Perdón, una acotación: hoy, las plataformas ejercen el rol que debería estar ejerciendo el Estado, porque hoy las denuncias –como se ha admitido– tanto de Facebook como de Twitter están llegando a las mismas plataformas, pero no llegan a esa herramienta que tiene el propio Estado para poder actuar.

¿No debería haber una articulación distinta, mucho más efectiva y real, entre las plataformas, quienes manejan estas políticas de privacidad y el Estado, con estas herramientas que tiene o que vamos a discutir a partir de ahora, como este proyecto que ha sido girado al Congreso?

Sr. Bertoni.- Si "articulación" se refiere a que exista una posibilidad de llevar adelante el control de lo que hacen las plataformas por parte del Estado, o tener una conversación con las plataformas… Yo creo que nosotros somos un órgano de control: quiero ser claro en este sentido. Y nosotros lo que protegemos son los derechos de las personas que están garantizados por las dos leyes madres que tenemos: la de acceso a la información pública y la de datos personales. Con lo cual, si nosotros advertimos una violación a la ley, nosotros tenemos que avanzar con nuestro rol de órgano sancionador, por llamarlo de alguna manera. La sanción es la que dije.

Eso no quita que en el trámite del expediente pueda haber un intercambio que, en definitiva, solucione el problema: por supuesto, eso es posible en cualquier expediente. Lo que sí es cierto es que, muchas veces, las personas que se enfrentan a estos problemas acuden directamente… ¡Bueno! Lo dijo hace un ratito –se fue ahora– el representante de Facebook. Dijo claramente: "La mejor manera es que vengan a nosotros". Yo ahí sí, conceptualmente, coincido con usted: si hay una violación de derechos es el Estado el que tendría que intervenir. Pero no quiero dejar de insistir con lo que decía hace un momento: estamos frente a un problema y tenemos que encontrar cuál es la mejor vía para solucionárselo a las personas. Entonces, si la ventana es una herramienta más, vía los privados, si es útil...

Sr. Presidente (Luenzo).- ¿Alguna consulta?

– No se producen manifestaciones.

Sr. Presidente (Luenzo).- ¿No? Bien; muchas gracias, Eduardo.

Vamos a convocar al doctor Enrique del Carril, director del Cuerpo de

Investigaciones Judiciales del Ministerio Público Fiscal de la Ciudad de Buenos Aires.

Sr. Del Carril.- Buenas tardes a todos.

En primer lugar, quiero agradecer esta oportunidad de estar ante el Senado para tratar tan importante ley.

No quiero ser autorreferencial, pero un poco poner en contexto cuál es mi función, mi trabajo y mi papel, para mostrarse como una voz más en este tema que tiene una perspectiva muy particular, que es la perspectiva del Cuerpo de Investigaciones Judiciales; y, con esto, un poco aportar desde ese lugar en esta discusión.

El Cuerpo de Investigaciones Judiciales es un órgano de investigación, precisamente, de la Fiscalía de la Ciudad de Buenos Aires; un órgano que se ha volcado muy fuertemente a la investigación tecnológica, a la investigación del cibercrimen y a la investigación en tecnología en general. En ese marco, a partir de una serie de acuerdos, hemos llegado a un acuerdo con una serie de organizaciones norteamericanas las cuales nos envían toda la detección de pornografía infantil y *grooming* que ocurre en la Argentina. Estamos hablando hoy de cien casos por día de tráfico, desde perfiles de redes sociales, de pornografía infantil o de intentos de *grooming que,* como ustedes saben, son intentos de acceder a menores para obtener de ellos imágenes o alguna actividad sexual en concreto.

Por eso, este tema del robo de identidad, desde esta perspectiva –que, insisto, es la nuestra: la del investigador que está en los casos todos los días–, es una perspectiva que la vemos como auspiciosa, si bien hay mucho que habría que pensar, discutir y matizar. Pero, realmente, lo que nos ocurre es que en estos hoy 70 mil casos que tenemos nos encontramos con perfiles falsos: es decir, con apariencia de verdaderos, pero falsos.

Por una serie de especificaciones técnicas –no quiero aburrirlos, pero si después alguno quiere se lo puedo explicar– es muy difícil detectar esos perfiles por el dato técnico de la conexión y el problema que nos encontramos es que tenemos que investigar la realidad de esos perfiles en las redes.

¿Por qué este marco? Porque en este delito de usurpación de identidad o de robo de identidad, como queramos llamarle –también el tema de la denominación es un tema que a los hombres de Derecho no se nos escapa y habría que también generar alguna discusión sobre esto–, es una herramienta bastante útil para investigar, por supuesto, y también para prevenir. Nosotros detectamos perfiles que están –y perdónenme la expresión metafórica y cruda– cazando en las redes a nuestros niños para obtener de ellos imágenes o videos; y, a veces, no podemos hacer nada hasta que el niño no sea cazado, y esto es bastante crudo. Por ese lado, es una ley que tiene para nosotros ciertos ribetes muy interesantes.

Otro aspecto que me interesa resaltar es que realmente, en algún punto, esta ley está pensando… Dije "ley", ya la asumí como una ley hecha. Mejor dicho, estos proyectos, todos y cada uno desde su perspectiva, están pensando en la identidad digital como un valor en sí; esto es distinto de la expresión que se haga con ese perfil o para qué se usará después o antes; y eso me parece también una perspectiva muy interesante.

En esta nueva sociedad que estamos viviendo, con la que a mí me toca convivir con la parte más oscura –y me hago cargo de que esa es mi mirada–, esta idea de una identidad digital que tiene que ser protegida y que tiene que tener una

protección penal es una idea que me parece muy aceptable.

Realmente, estoy convencido de que esta sociedad nos va a llevar a que esa identidad digital que tenemos sea una parte constitutiva de nuestro ser: una parte realmente constitutiva como es nuestro nombre real, como es nuestra cara y como es nuestro entorno. Con lo cual, en algún punto podemos decir que esta ley se adelanta un poco a lo que creo que va a venir. Así que también, por ese lado, lo veo como algo muy auspicioso.

Después, por supuesto, los proyectos de ley tienen una serie de temas sobre los que habría que entrar en discusión.

Es muy importante proteger esa libertad de expresión, donde el representante de Twitter hizo mucho énfasis; y es cierto que muchas veces esa libertad de expresión se da desde la parodia o se da desde la imitación de alguna persona pública o privada, y eso es muy sano. Y Twitter, de alguna manera, podemos decir que es especialista en eso basta uno buscar los perfiles de nuestros próceres, como San Martín o Sarmiento, y se va a encontrar con alguno que intenta leer nuestra realidad desde cómo pensaría aquel prócer, y eso es muy interesante. Por eso, en algún punto comparto tanto la perspectiva de Facebook como la de Twitter porque son distintas miradas sobre el producto digital. Facebook es un lugar social donde nos intercomunicamos entre personas. Por lo tanto, para ellos, la identidad es mucho más importante que Twitter, que es un ágora, como bien dijo una persona.

Creo que la ley tendría que contemplar esto; tendría que pensar en que no todo perfil creado implica un delito; que habría que matizar un poco; que habría que, incluso, pensar en los distintos formatos de las plataformas. No es lo mismo Instagram, donde vemos fotos y donde el robo de una identidad es mucho más intenso, que Twitter, donde es sólo un nombre que tira ideas.

No quiero molestarlos más y estoy dispuesto a las preguntas que ustedes quieran hacerme. Quiero poner este perfil: la idea, como idea, me parece una idea –de todos los proyectos– muy loable y muy entendible y que, en algún punto, se adelante a un problema que, si no lo tenemos ahora, lo vamos a tener en breve, que es el tema de si nuestra identidad digital es un derecho en el sentido más profundo de la palabra –un derecho constitucional, un derecho humano–; pero, por el otro lado, tenemos que cuidar que eso no coarte esa innovación, esa capacidad de discusión que nos dan las redes sociales.

Así que este era mi aporte; muchas gracias.

Sr. Presidente (Luenzo).- Seguramente lo volveremos a convocar en el momento que tengamos definida esta síntesis que podamos hacer de los cuatro proyectos de ley que hoy estamos poniendo a disposición de los senadores.

Sr. Del Carril.- Encantado y muchas gracias.

Sr. Presidente (Luenzo).- Doctor, muchas gracias.

A continuación, corresponde dar el uso de la palabra al doctor Daniel Monastersky, abogado especialista en delitos informáticos.

Sr. Monastersky.- Gracias por la invitación.

Como decía el doctor Del Carril, hace más de diez años yo fui uno de los autores del proyecto de ley –el primero que se presentó en toda la región– para tipificar el robo de la identidad digital. En ese momento, no tuvo ni tratamiento en comisión. Si bien esto sería un gran adelanto, hubiera sido mucho mejor que hace diez años hubiésemos tenido una normativa que tipificara este tipo de conductas.

El honor no es lo único que se ve afectado. La reputación es la opinión que los terceros tienen respecto de una persona. En la era de Internet, ésta se construye

a partir de lo que los individuos piensan en virtud de la información que existe sobre ellos en la red. Uno es quien Google dice que es; uno es quién Internet dice que sos. De ahí radica la importancia el contenido que se exterioriza y difunde a través de las plataformas digitales. Incluso, una mala reputación *online* genera un sinnúmero de daños que no solamente abarcan la percepción de los demás sobre uno sino también una afectación económica y laboral.

La doctrina históricamente sostiene que uno de los fines de la pena es mantener la vigencia de la norma y que, mediante la sanción ante su incumplimiento, se reafirman el valor social y los bienes jurídicos lesionados que por ser estos penalmente protegidos se consideran fundamentales. Es así que, no castigando la afectación del buen nombre y honor, la Justicia contribuye a que el mismo bien se siga afectando. De esta manera, se erosiona la conciencia social del valor del bien, y el respeto por la norma y el derecho.

Debemos encontrar una solución a estas lesivas arbitrariedades a las que nos vemos expuestos, no solamente por su gravedad sino también porque el deliberado daño y afectación de nuestro buen nombre y honor que acarrean es permanente e irrecuperable.

Este uso impune de las redes sociales tiene un correlato con la impunidad que, hasta ahora, los tribunales en general han resuelto.

Es conocido que casi la totalidad de las empresas que buscan candidatos los googlean. Una reputación *online* negativa es peor que una primera mala imagen y, como ésta, te niega una segunda oportunidad.

La viralización que se consigue a través de Internet maximiza el daño: lo convierte en un perjuicio con alcance global.

El ciberdaño, como vemos, causa perjuicios a las personas a nivel, físico, psicológico y reputacional. Con relación a este tema, pueden leer *papers* de la Universidad de Oxford que ahondan muchísimo en esta cuestión.

Aunque mucho se habla sobre el impacto de cibercrimen en la economía, estas consecuencias que recaen sobre los individuos no están siendo magnificadas en su totalidad.

Internacionalmente, se ha consagrado el derecho al honor y a la dignidad de la persona como uno de los derechos fundamentales del hombre. Entonces, desde esa óptica, ¿bajo qué criterio podemos dejar que se avasallen los mismos con impunidad? Vivir en una democracia implica poder expresar lo que uno quiere, pero también hacerse cargo de lo que uno dice y hace.

De ningún modo puede acusarse de restringir la libertad de expresión a quien ve vulnerado su derecho al honor, pues estos derechos son autónomos y en un Estado de derecho moderno no se puede permitir que se sacrifique a un individuo en pos del resto; o que se menoscaben los derechos de un ser humano en pos del interés público.

Es tal la magnitud de la suplantación de la identidad digital que la ONU ha determinado que esta situación puede llegar a ser una amenaza contra la seguridad de las naciones.

Esto es solamente algo de lo que opino respecto de esta problemática en la que vengo trabajando hace muchísimos años. Así que estoy totalmente de acuerdo.

Como es obvio, habría que analizar los proyectos más en detalle. Ninguno me parece que es suficientemente correcto para poder elegirlo; pero creo que se puede hacer un *mix*, obviamente, para poder tener una normativa que tipifique en forma definitiva esta cuestión.

Sr. Presidente (Luenzo).- Doctor: lo voy a convocar para que en ambas comisiones podamos seguir trabajando a fin de ir evolucionando y, en el momento que tengamos definido cuál es el proyecto final, seguramente también vamos a contar con su presencia. Pero, en principio, lo comprometo para trabajar en el ámbito de las comisiones. ¿Puede ser?

Sr. Monastersky.- ¡Cómo no! Un gusto.

Sr. Presidente (Luenzo).- Doctor, muchísimas gracias por venir.

A continuación, corresponde el turno del doctor Hernán Gonçalvez Figueiredo, secretario de Actuación Judicial de la Cámara Nacional Electoral.

Sr. Gonçalvez Figueiredo.- En nombre de la Cámara Nacional Electoral y mío propio, muchas gracias al Senado de la Nación –a las comisiones, a los senadores y a las senadoras– por la invitación a charlar sobre este tema novedoso desde la perspectiva electoral. Si se quiere, mi intención es hacer un aporte acerca de algunos de los efectos que proyecta en lo que se refiere al Derecho Electoral el uso de cuentas falsas, ya sea por suplantación o por ser anónimas.

Estas plataformas, sobre todo cuando funcionan como plataformas de noticias o de campañas políticas o electorales en un proceso electoral, han cobrado una relevancia bien conocida.

Creo que pocas veces las democracias en general, sin importar el grado de robustez que tengan los sistemas… Todos los países, creo que están siendo protagonistas de este nuevo fenómeno de la intromisión de la tecnología en la formación del debate democrático que va a dar lugar a la elección del pueblo de sus representantes.

Es algo que todos sabemos que es irreversible, que avanza muy rápidamente, según *Latinobarómetro* del año pasado, en América latina el 30 por ciento de la población forma su opinión política exclusivamente a través de redes sociales, desplazando a los medios tradicionales; y esto enfrenta desafíos para las autoridades electorales de una superposición de lo que es la vida real y regulada respecto de la vida virtual y no regulada.

Hace varios años, advirtiendo este nuevo campo de medios de comunicación política, la Cámara Nacional Electoral empezó a hacer auditorías. Decidió, justamente, auditar las redes sociales como parte del rol que tiene el Cuerpo de Auditores contadores en fiscalizar las cuentas de los partidos políticos en los cuales se destinan en las redes recursos para la publicidad electoral.

De esa experiencia –a partir de 2011; hace cuatro elecciones nacionales que se viene haciendo–, hay algunas conclusiones importantes. Por una parte, en cuanto a lo que se refiere al uso de estas plataformas como medio para hacer campañas electorales, es indudable su crecimiento exponencial. En 2011, el uso de las redes sociales no llegaba al 5 por ciento dentro de lo que era la inversión de publicidad declarada por los partidos políticos en total, mientras que el año pasado, en la última elección, superó el 30 por ciento, siendo el rubro de las declaraciones de los partidos más importante en inversión de publicidad electoral formal.

Pero, además de esto, fueron surgiendo otros fenómenos que se fueron advirtiendo en el resultado de estos monitoreos o auditorías que tienen que ver con las campañas microsegmentadas: el uso de *Big Data* para dirigir publicidad individualizada, que puede ver un elector en su buscador en un momento y otro elector en la misma página, en ese momento, no ve esa publicidad, basada en el historial de búsqueda o las preferencias de los electores.

También, la dificultad de aplicar a la realidad *online* las normas pensadas para la vida real: por ejemplo, la Ley de Financiamiento de los Partidos Políticos establece algunos límites a los aportes de personas que no residan en el país. Está prohibido el aporte de una persona que no resida en la Argentina. Sin embargo, a través de estas redes, por supuesto, se puede contratar desde otro país. Y resulta difícil también controlar los períodos de campaña que, probablemente, desde las cuentas oficiales de los partidos políticos o candidatos puedan respetarse, pero a través de cuentas falsas, o no, es más difícil controlar las épocas de prohibición de desarrollo de campaña.

Pero, puntualmente, más vinculado con el debate que acá se está dando, también se advirtieron las maniobras de desinformación y manipulación que se conocen con la etiqueta de *false news*, aunque a veces es más complejo que una noticia falsa.

Es decir, en el campo electoral la problemática es muy importante. Por una parte, tiene que ver con la protección de la identidad de las personas, que es –entiendo– a lo que apunta directamente la modificación del Código Penal; pero también tiene una dimensión colectiva, porque el uso de cuentas falsas o suplantación de identidad puede proyectar efectos en la formación de la decisión pública, la decisión política, afectando un debate auténtico. En alguna medida me pregunto si no podrían también, por esta vía, afectarse derechos políticos de –por ejemplo– un candidato al que horas antes de la elección le roben la identidad digital y genere algo en la campaña que pueda tener impacto en el proceso electoral directo.

Me parece, por eso, muy interesante la discusión acerca de si las normas tradicionales o las soluciones clásicas sirven para proteger la identidad digital, o si la identidad digital es un fenómeno que requiere una tutela específica, una regulación propia, que no es alcanzada por las normas protectoras de la identidad real; siempre, por supuesto, partiendo de la complejidad que significa que acá está en juego la libertad de expresión, que también es la piedra angular de cualquier sistema democrático, y una complejidad operativa que entiendo es parte de la propia naturaleza arquitectónica de Internet, que es una naturaleza aparentemente inabarcable. Hoy estamos planteando estos problemas acerca de las redes abiertas, cuando ya están apareciendo algunos otros problemas vinculados con la difusión de cadenas por los mecanismos de chats: WhatsApp, Telegram, etcétera.

Básicamente, quiero decir que la experiencia comparada indica que no se trata de un fenómeno aislado. No solo ha habido famosos casos del *brexit* en 2016 o las elecciones norteamericanas de 2016, sino que es un fenómeno globalizado que no depende de la malicia de pocos actores sino que es parte de la distorsión que se hace de las redes sociales.

A mediados de este año la Universidad de Oxford, a través de uno de sus institutos de investigación, publicó un informe sobre este tema en concreto. Tomando como muestra cuarenta y ocho países, llegó a la conclusión de que en cuarenta y seis se utilizaban cuentas falsas para manipular la discusión en procesos electorales. Estableció cuatro grados de capacidad de estos equipos de trabajo a partir del presupuesto que invierten, el periodo de actividad, el tipo de campaña que hacen; y es interesante el documento acerca de los tipos de maniobras que se utilizan y los diferentes niveles de influencia en los procesos.

El Parlamento británico también tiene un documento muy sólido que desarrolla toda esta problemática; y en ambos documentos lo que queda claro es

que una de las principales herramientas de desinformación es el uso de cuentas falsas, ya sea porque son automatizadas –se llaman *bots* políticos– o cuentas humanas que manejan seres humanos o híbridos que son más difíciles de detectar porque se comportan como personas, pero también tienen un componente de automatización. Además, los comentaristas que se ocupan de interactuar con usuarios reales en blogs, sitios de noticias, foros de discusión, etcétera, también es parte del uso de cuentas falsas. Básicamente, el propósito a través de estas cuentas es difundir noticias basura o propaganda en las elecciones; fabricar un falso sentido de popularidad o apoyo a determinados candidatos; o, incluso, abogando conversaciones auténticas de otros grupos de personas. De los cuarenta y ocho países que aborda el estudio, en treinta y tres casos se detectaron operadores humanos coordinando las acciones de cuentas falsas.

¿Por qué importa y por qué es interesante la discusión en lo que se refiere al Derecho Electoral, a los procesos electorales y al sistema democrático en sí? Principalmente porque está en juego, como decía al principio, el acceso a la información: el derecho constitucional de difundir y acceder a la información. Cuanta mejor calidad tenga la información, más auténtica y más libre sea, mejor calidad va a tener el sistema democrático. La Corte Interamericana de Derechos Humanos ha dicho que una sociedad que no está bien informada no es una sociedad plenamente libre.

Por eso, la cuestión del perfil falso o de las cuentas falsas tiene que ver con la protección de la identidad de las personas a las cuales se les suplanta, en la hipótesis de suplantación; pero también tiene impacto, como les decía al principio, en la dimensión colectiva de lo que es el proceso electoral y, en particular, en el elector, que es lo que le preocupa a la autoridad electoral: cómo al elector le llega información sobre la cual va a formar su opinión y decidir su voto. La Cámara Nacional Electoral hace muchos años que viene trabajando un concepto de voto informado, donde se propende a que el elector cuente con la mayor información determinante para decidir su voto.

El segundo punto por el cual resulta relevante es porque hay normas que regulan las campañas electorales en temas de financiamiento y de periodos, que tienden a buscar cierta equidad en la participación de los actores: cierto equilibrio razonable en los recursos y en los tiempos con los que se cuenta para hacer las compañías. Se regula el tiempo de asignación de publicidad electoral en TV, en radio; se regula lo que se puede invertir; y en este campo, naturalmente, pueden evadirse por esta vía de las redes sociales algunas de estas normas, y afectarse la equidad.

Por último –y creo que es lo más importante–, porque el sistema democrático se funda en un sistema de creencias. Es necesario que las personas confíen en el procedimiento por el cual se designaron a los representantes; y por más que este procedimiento sea estrictamente puro y transparente, si las personas creen –basados en una noticia falsa– que ese procedimiento no fue auténtico, no va a cumplir su finalidad, que es legitimar a la autoridad electa; se va a deslegitimar el proceso electoral, lo cual para el sistema es algo de mucho daño, resulta algo fatal.

En esto creo que viene a cuento el Teorema de Thomas: un teorema de la Sociología que dice que, si las personas definen las situaciones como reales, éstas son reales en sus consecuencias. Es decir: aunque el dato sea falso, si las personas entienden que la elección fue fraudulenta, no se va a cumplir el objetivo de legitimación que tiene el proceso electoral.

El poder de la noticia falsa es conocido históricamente. Quizá uno de los casos más emblemáticos fue aquel programa de radio de Orson Welles de fines de los años treinta que transmitía la *Guerra de los mundos* y personas llamaban a las comisarías diciendo que habían visto extraterrestres. Hoy, la diferencia es que no hace falta ser Orson Welles ni tener un programa de radio de gran audiencia para generar un efecto similar: a través de cuentas –automatizadas o no, pero cuentas falsas– se puede lograr un efecto muy perjudicial para los procesos electorales.

¿Qué están haciendo las autoridades electorales a partir de esto? Porque es un campo nuevo para los legisladores, para los reguladores y también para la autoridad electoral. Hay varias experiencias. El Instituto Nacional Electoral de México, para las elecciones presidenciales de este año, suscribió convenios con Google, con Facebook y con Twitter, con diferentes finalidades, para difundir la problemática y capacitar a la ciudadanía sobre esta cuestión digital. Es una experiencia que la Cámara Nacional Electoral está mirando con atención. Tenemos ya conversaciones con estas empresas para ver qué se puede hacer, parecido.

Brasil generó también una serie de memorandos de entendimiento y compromisos con diferentes actores para combatir lo que es la difusión de noticias falsas.

Y Colombia trabajó también en algo que es más novedoso, que es el chequeo de información, el *fact-cheking*, a través de las cadenas de WhatsApp, que hoy por hoy es un problema específico porque es una caja cerrada, a diferencia de las redes abiertas, en las cuales es más fácil el monitoreo.

Desdé la Cámara Nacional Electoral hace aproximadamente un mes se dictó una acordada, que es una decisión de tipo reglamentario, que tiene por objeto principalmente poner el tema a la luz pública: llamar la atención sobre esta problemática teniendo en cuenta el proceso electoral del año que viene. Tuvo entre otros fundamentos en cuenta la utilización de cuentas falsas. Se dice entre los fundamentos de la Cámara acerca de las sofisticadas técnicas que incluyen la utilización de perfiles falsos de dirigentes políticos, así como la difusión de noticias falsas, o acción de comentaristas pagos que utilizan perfiles falsos. Y abordó la cuestión desde diferentes aristas, siendo conscientes de que lo principal es la información: a la desinformación combatirla con más información.

Entonces, para empezar lo que decidió es transparentar los mecanismos. Con estas auditorías, que se hacen principalmente para ver el gasto electoral, se producen informes que el tribunal va a publicar. Ya, de hecho publicó el de la elección pasada en su página de Internet para que cualquiera pueda ver los movimientos identificados como manipulación de la información.

Por otra parte, para fomentar mecanismos de verificación de la autenticidad de las cuentas, que viene en particular a cuento de lo que se está discutiendo acá, creó un Registro de Cuentas Oficiales, de canales de comunicación oficiales de los partidos políticos, que son los sitios webs o las páginas, los foros, blogs que tengan, y las cuentas en redes sociales de las autoridades de los partidos políticos y de los candidatos y precandidatos que van a participar el año que viene. En principio, contamos con la participación voluntaria de los partidos políticos, desde ya, de ir registrando como un modo de tutelar sus propias cuentas y sus vías de comunicación.

Por otra parte, hay algunas medidas que tienen que ver no con lo que acá se discute sino con el control de financiamiento.

Finalmente, con lo que les decía: la idea de promover la concientización y la

formación cívica en este problema, para lo cual está pidiendo colaboración con el Centro de Información Judicial de la Corte Suprema de Justicia de la Nación, para el año que viene tener algún tipo de programa de difusión y educación en este sentido.

Sr. Presidente (Luenzo).- Por lo tanto, tenemos otra tarea agregada a todo esto, que es la dimensión política que tiene la utilización en las sociales.

También, sobre esto creo que deberíamos complementar lo que estamos debatiendo hoy, que es sustitución de identidad, pero en este caso en el mundo de la política. Esto, por la salud de la democracia misma y la legitimidad que tienen que tener aquellos que sean elegidos.

Por lo tanto, nos vamos a volver a ver. (*Risas.*) ¡No tengo ninguna duda! Gracias, muy amable.

Sr. Gonçalves Figueiredo.- ¡Por favor; gracias a usted, senador!

Sr. Presidente (Luenzo).- Vamos a nuestro último invitado: el doctor Horacio Azzolín, titular de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación.

Sr. Azzolín.- Muchas gracias por la invitación; buenas tardes a todos.

Escuchaba atentamente las intervenciones precedentes. Algunas cosas que no voy a decir no las digo porque ya las dijeron. Pero, primero, para hablar de sustitución, asunción de identidad ajena, usurpación de identidad, que son más o menos los conceptos comunes que se tratan en este tema, yo les quiero contar un poco qué es lo que detectamos nosotros desde una unidad del Ministerio Público Federal dedicada a investigar crímenes cibernéticos.

Pretendo hacerles un paneo de cuáles son los casos que hemos visto, más allá de los casos que les ha mencionado el doctor Del Carril, que tiene otro de los aspectos sumamente relevantes de estos crímenes cibernéticos, que son los que tienen que ver más con los niños.

Nosotros estamos detectando en los últimos años el uso de identidad de personas jurídicas reales, existentes: bancos, empresas de tarjetas de crédito, las principales empresas de servicios en línea. La utilización de esta identidad para captar credenciales: es decir, número de usuario y contraseña, datos de tarjetas de crédito, maniobras que se conocen en la temática nuestra como *phishing* –es decir, el pescado bajo engaño–, o directamente para cometer fraude en contra de las personas que reciben las comunicaciones. Generalmente, se usan correos electrónicos, cuentas de redes sociales o sitios webs. Esta mañana, sin ir más lejos, emitimos una alerta por un incremento de casos que se están recibiendo en la Argentina de falsas ofertas de trabajo: empresas del extranjero multinacionales o se usa la identidad de empresas multinacionales que contactan a ciudadanos argentinos que por lo general han ingresado "búsqueda de trabajo" en redes sociales dedicadas a esto, y le prometen una excelente oferta laboral a cambio de entregar determinada información. Esa información, esos datos personales después se trafican en mercados negros; o directamente pidiéndole la entrega de dinero a cambio de gastos administrativos. Esta es una modalidad bastante conocida: se llama fraude de reclutamiento. En la Argentina está creciendo por campañas. Por lo general son bastante generalizadas. En los últimos tiempos, en las últimas dos semanas hemos detectado entre 30 y 50 consultas sobre eso, específicamente. Eso es también asunción de identidad ajena o usurpación de identidad.

También, lo que estamos viendo es uso de identidad de personas físicas reales usualmente para causar fraudes. Por lo general, es la compra-venta de bienes y servicios, o pedidos de dinero entre redes de conocidos; y para eso se

usan sitios webs, fundamentalmente n lo que tiene que ver con la oferta de bienes y servicios. Se falsean, por ejemplo, el *look and feel* de los sitios institucionales de las principales plataformas de comercio electrónico y, a través de ellas, se ofrecen bienes y servicios más baratos. La gente entrega credenciales, entrega datos de tarjetas de crédito: termina siendo un fraude. Se utilizan para eso las campañas del Día del Padre, Día de la Madre, Navidad, *hot sale*, *black friday* y todas las campañas de venta que nosotros nos podamos imaginar. También, se usan cuentas de redes sociales para eso.

También, se usa la identidad de personas físicas reales para difamar, para insultar a terceros, para acosar. Se crean cuentas de redes sociales en las que, por ejemplo, se muestran los movimientos que hace una persona. Se crean cuentas de redes sociales en las que le mandan a la persona fotos de adentro de la casa de la persona. Sin amenaza, sin insultos, es simplemente para decirle: "Estuvimos en tu casa". "Sabemos dónde estás". "Sabemos a qué hora salís". "Sabemos a qué hora volvés". "Sabemos cómo estás vestido o vestida hoy".

A veces, para mortificar se asocia la imagen de una persona a determinadas conductas. Por lo general, después de rupturas de relaciones se sube la foto de la expareja en sitios de citas en línea o sitios de ofrecimiento sexual, con el número de teléfono de esa persona. La persona empieza a recibir incontables mensajes. Eso no es una amenaza, no es una difamación y, sin embargo, es una molestia en el plan de vida de la persona. Usualmente, para eso se usa redes sociales.

También, hay creación en redes sociales de perfiles de personas inexistentes, pero en los que se usan datos personales: fundamentalmente, la imagen, las fotografías de personas reales. Y después dicen: "Vi tu foto. Tenés un perfil en tal red". Generalmente, esos perfiles son usados para cometer algún tipo de fraude. Hay uno bastante difundido en la Argentina y en la región últimamente que se llama "estafa romántica": personas de determinada edad que conocen en redes a su príncipe azul y ese príncipe azul después le pide plata para liberar un destino; y la gente entrega muchísimo dinero. Hemos tenido casos de gente que entregó prácticamente todos sus ahorros para salvar a una persona que estaba supuestamente presa en algún lugar del lejano Oriente, etcétera.

Además, lo que tenemos es la utilización de identidades falsas, que no están asociadas a ninguna persona concreta, para cometer fraude. Por ejemplo, la famosa o denominada "estafa nigeriana", en la que nos contacta una persona que recibió una herencia millonaria y nos dice que si nosotros lo ayudamos a rescatar esa herencia vamos a tener una parte etcétera, etcétera, etcétera, que es la versión 2.0 del "cuento del tío". Sería el único caso que no está gobernado por estos proyectos.

Pero estos proyectos nos ponen en el debate acerca de una cuestión bastante importante que tiene que ver con el esto del uso de la identidad ajena, que hasta ahora no estaba contemplado directamente en ninguna de las normas de nuestro Código Penal vigente. Si bien tenemos una norma que protege la identidad, está protegiendo la identidad tradicionalmente conocida; y, de hecho, todos los proyectos que estamos discutiendo incorporan un 139 bis a la suplantación de identidad clásica. El ejemplo más claro es el de los niños apropiados, etcétera.

Sin embargo, hay algunas normas en el Código Penal que hablan sobre estos temas. Yo pretendo no aburrirlos, pero sí darles un pantallazo técnico acerca de algunas cuestiones que ya están cubiertas y que, a lo mejor, se mencionan en los proyectos.

"El nombre supuesto": es decir hacerse pasar por otro, o simular determinada

calidad, es una forma de comisión del delito de estafa.

La falsificación o el uso indebido de una marca, también está protegido por la ley de marcas y designaciones: es decir que, cuando yo envío un *mail* haciéndome pasar por una empresa y uso el logo de esa empresa, por lo menos podemos actuar penalmente contra la persona por el uso de ese logo. Es una actuación deficitaria, que no recepta el contenido real del delito, pero por lo menos nos permite colarnos de alguna manera por ahí.

También hay una norma que sanciona la usurpación de determinada autoridad, títulos y honores: hacerme pasar por un abogado cuando no lo soy; hacerme pasar por un funcionario policial cuando no lo soy; por un funcionario público. Esto tiene determinada sanción penal.

El *grooming* es una norma nueva que se estrenó hace muy poco, en la medida en que aceptemos que el *grooming* es un adulto que se hace pasar por un niño para contactar a otro niño, niña o adolescente, con el objetivo de cometer un delito contra la integridad sexual. La esencia del *grooming* es sancionar el "no hables con extraños" cuando es muy fácil hacerse pasar por un extraño en una red social.

La tenencia y el uso de un documento ajeno también están contemplados como delito en la Ley del DNI, la 17.671.

La falsificación de documentos destinados a acreditar la identidad de las personas también está sancionada como delito.

Así que hay algunas normas en el Código Penal –es un Código Penal bastante viejo; todos lo sabemos– que, de alguna forma, permite a nosotros o a los operadores judiciales encarar algunas de estas usurpaciones de identidad, uso de identidad ajena, desde el punto de vista del delito penal.

Ahora, hay cosas que directamente no están gobernadas, y ese es el mayor problema. Crear una cuenta en una red social utilizando el nombre de cualquiera de ustedes, utilizando la fotografía de ustedes que yo pueda encontrar googleándolos –más si son funcionarios públicos; es mucho más fácil; en mi caso, también–, no está sancionado como delito. Me refiero a la creación de esa identidad.

Estos debates –lo escuchaba a Enrique del Carril y coincido con él– ponen sobre el tapete la idea de si la identidad digital la tenemos que proteger como un bien jurídico independiente, si la tenemos que proteger asociada a la identidad, o si la tenemos que proteger asociada a otros bienes jurídicos.

No se trata aquí de pensar en lo que se llama "adelantamiento de la punición": vamos a penar el perfil falso en una red social para evitar una estafa. No necesariamente es eso. La creación de un perfil falso es, en sí misma, una cosa que debe ser tutelada; y nos parece que, en determinado supuesto, la tutela penal puede ser efectiva.

Lo que trasuntan todos los casos que hemos tenido es que, cuando a uno le crean un perfil con sus imágenes públicas –y más si usan las imágenes de sus hijos, que pueden sacar de la página del colegio al que van; no necesariamente se trata de que uno las exponga, sino que tal vez las ha expuesto un tercero, una mami en un cumpleaños que sacó una foto y la subió– lo que se altera es el ánimo. Es lo que puede llegar a pasar con esas imágenes: una estafa, una difamación, una afectación de un resultado electoral. Pueden pasar muchas cosas con ese tipo de cuentas. Entonces, la sanción de esto nos va a permitir atacar con mayor eficacia determinadas conductas que después pueden convertirse en fraudes; y atacar con eficacia, también, determinadas conductas que en sí mismas deben ser

consideradas, al menos, preocupantes.

Quiero hablar concretamente de algunos números que hemos tenido. En lo que va del año –yo algo les dije– hemos tenido unos cincuenta casos en total de uso de identidades falsas. Hemos tenido consultas, reportes, denuncias de cincuenta casos en total de uso de identidades falsas para cometer crímenes. Esto, sin hablar de otros cien casos que hemos tenido de consultas por *mails*, donde los autores se hacen pasar por bancos, los principales son tarjetas de crédito o de servicios, para captar credenciales. Estos ciento cincuenta casos desde mayo hasta ahora son una mínima porción de los casos que quedan abajo del tapete, que no se denuncian por falta de conciencia, por falta de conocimiento o porque, directamente, son bloqueados por los servidores de los correos electrónicos. En los correos electrónicos institucionales de todos y cada uno de ustedes seguramente habrán recibido alguno que se ha filtrado; y, si no, pregúntenles a los administradores de sistemas cuántos se han filtrado en los últimos tiempos, para darse cuenta de la dimensión de esto que está pasando. Los proyectos, entonces, tienden a solucionar este vacío.

Si bien –como les decía anteriormente– los proyectos se enmarcan dentro de lo que es la protección de la identidad, otra opción posible es considerarlo como una protección autónoma que tiene que ver con la identidad y con el uso indebido de los datos personales, como lo prevé de alguna manera el anteproyecto de Código Penal que se elaboró en el marco del Programa Justicia 2020.

Por otro lado, los proyectos también tienen una coincidencia al establecer una pena de privación de libertad de seis meses a dos años –la mayoría de los proyectos–. Esto también está en coincidencia con la norma que establece el anteproyecto del Código.

Entre las sanciones previstas, nos sentimos cómodos con la opción del proyecto S.-2.449/18, que establece además una pena alternativa de multa para que, en algunos casos que tal vez no sean extremadamente graves, la sanción de prisión no sea la alternativa sino una sanción económica que, en muchos casos, es mucho más efectiva que la pena de prisión para este tipo de casos.

Los proyectos no coinciden en los verbos típicos: es decir, cuáles son las conductas que la ley va a establecer como prohibidas. Y en esto hay que tener la mayor precisión posible de los estudiados. El que nos parece mejor es el 2.630/18, que sanciona el adquirir, tener en posesión, crear, transferir o utilizar la identidad de otra persona. Además, incluye no solamente la identidad de la persona física sino también de la persona jurídica. En ese sentido, la identidad de las corporaciones también es utilizada para cometer fraude.

Acá, no estamos pensando exclusivamente en la protección de esa identidad de las corporaciones, que tal vez está protegida de alguna manera por la Ley de marcas, sino también en la confianza que el usuario doméstico de Internet puede tener frente al logo de una corporación, un correo, o un sitio que asimila el *look and feel* de determinada corporación, y que solamente los ojos de un experto o de alguien que ve estos casos todos los días puede detectar que no es el sitio de tal plataforma sino el sitio de una organización criminal.

Le agregaríamos a esa norma una parte del proyecto 2.722, que establece que la asunción de identidad ajena tiene que ser utilizando su nombre, su apellido, su imagen o algo que indefectiblemente lo vincule con esa persona, para darle mayor precisión a la norma.

Los proyectos también tienen varias definiciones acerca del entorno en el

cual esto debe decidirse: tecnologías de comunicación y de información –las TICs–, las redes sociales, Internet.

Hay una definición que ya está en el Código Penal: en el delito de *grooming* se define como comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos. También se podría usar una norma similar para que el Código tenga las mismas definiciones y tenga cierta sistematicidad.

Finalmente –esto también nos parece muy adecuado destacar–, sigo un poco los lineamientos del doctor de Carril en cuanto a que en el tema de estas normas hay que tener mucho cuidado con no afectar determinadas cuestiones que tienen que ver con la libertad de expresión. La creación de perfiles de identidades ajenas, en determinados momentos, puede estar asociada a las cuentas de parodia, como ya se ha mencionado, y también a las cuentas de ensalsamiento: las cuentas de Google de fans, donde se usa la identidad de la persona a la que se quiere ensalsar. Entonces, si uno hace una lectura fría de la norma, quien crea una cuenta de club de fans para alentar a determinado personaje, puede llegar a estar gobernado por la norma.

Además, acerca de la idea de personaje público, tendríamos que discutir cuándo uno adquiere el rol de personaje público y cuándo lo deja, más allá de los funcionarios públicos que tenemos un principio y un fin determinado por las leyes. Pero respecto de los personajes públicos que no son funcionarios públicos, cuándo son públicos y cuándo dejan de serlo es bastante complicado. Preferiríamos dejar una norma que no englobe esas circunstancias; pero sí, tal vez, habría que tratar de definir este concepto de qué casos no se van a considerar delictivos, en la medida en que la intención no sea cometer un delito o perjudicar a una persona –como dice uno de los mensajes– sino que tenga otra opción que sea la crítica política, la sátira política, como pasa con los imitadores en la televisión. Es la versión de redes sociales de los imitadores, de la sátira. Entonces, en ese sentido, tendría que estar cubierto.

Más allá de eso, desde el punto de vista técnico del dolo, cuando uno advierte que la cuenta es de sátira, no estaría englobada por la norma por esta falta de intención.

Algunas iniciativas, como la de la Cámara Nacional Electoral de crear un registro de cuentas originales van a permitir mitigar esto; pero es algo muy aleatorio. También, que haya plataformas de redes sociales que tengan un control bastante estricto: que traten de verificar cuentas, de establecer la verdadera identidad de una persona, depende de la plataforma concreta. Mañana puede aparecer una plataforma nueva a la que eso no le importe; y, de hecho, las hay. Hay plataformas que no tienen esos controles, que no guardan registro, cuyas políticas comunitarias son tres renglones. Entonces, tenemos que pensar en escenarios diferentes.

Esos son los aportes que queremos hacer.

Nos parecen muy auspiciosos los proyectos y les agradecemos mucho que nos hayan invitado.

Sr. Presidente (Luenzo).- Doctor, muchas gracias.

¿Alguna consulta los senadores?

– No se producen manifestaciones.

Sr. Presidente (Luenzo).- Bueno, muchas gracias; seguiremos charlando, muy amable.

De esta manera damos por concluido este plenario de comisiones.

Vamos a seguir trabajando y apuntando a ver si podemos, con esta síntesis,

llegar a un proyecto final; muchas gracias.

– Son las 16.06.