Seguridad y privacidad en redes sociales virtuales: tipologías y perfiles actitudinales.

Luis Eduardo Ruano[1], Ernesto Congote[2]

[1] Profesor Investigador. Programa de Psicología, Universidad Cooperativa de Colombia, Sede Popayán, luiseruano@gmail.com
[1] Investigador Programa de Psicología, Universidad Cooperativa de Colombia, Sede Popayán, ernesto.congote@hotmail.com

Resumen. El artículo reflexiona en torno a la percepción y manejo de la seguridad y privacidad en redes sociales virtuales (Facebook, Instagram, WhatsApp). Empleando la técnica cualitativa de los grupos de discusión y el análisis sociológico del sistema de discursos, se identifican cuatro tipologías de usuarios de redes sociales (Observador, Discreto, Abierto y Avatar), que dan cuenta de la relación entre las categorías de análisis (percepción, usos, administración de la información, comunicación, identidad virtual), y el uso de redes sociales. Partiendo de una perspectiva general sobre el manejo de la información online, se identifican posiciones estructurales, migraciones discursivas, y perfiles actitudinales específicos relativos a cada usuario; finalmente, se realizan algunas consideraciones sobre el rol que desempeñan las tipologías en el escenario virtual.

Palabras clave: redes sociales virtuales, privacidad, seguridad, identidad, tipología de usuarios de redes sociales, perfiles actitudinales.

Security and privacy in virtual social networks: typologies and attitudinal profiles

Abstract: This article reflects on the perception and management of security and privacy in virtual social networks (Facebook, Instagram, WhatsApp). By using the qualitative technique of discussion groups and the sociological analysis of the speech system, four typologies of social network users are identified (Observer, Discreet, Open and Avatar), which account for the relationship between the categories of analysis , Uses, information management, communication, virtual identity), and the use of social networks. Starting from a general perspective on the management of online information, structural positions, discursive migrations, and specific attitudinal profiles related to each user are identified; Finally, some considerations are made about the role played by typologies in the virtual scenario.

Key Words: Virtual Social Networks, privacy, Security, Identity, Social Network User Typologies, Attitudinal profiles. 1 Introducción

1 Introducción

Las redes sociales virtuales y sus contenidos asumen progresivamente mayor relevancia, dentro del objeto de análisis de las ciencias sociales (Borgatti, 2009). Su operación en espacios profesionales, lúdicos y educativos es cada día más constante, y su integración con sitios web y dispositivos tecnológicos que se adecúan a sus requerimientos, las hacen prácticas para la comunicación y un objetivo deseado para el marketing y el minado de datos (Castells, 2006, 2009).
Desde las redes sociales, grandes compañías y hasta gobiernos pretenden impulsar la economía, generar interrelación y dinamizar la participación política, es por ello, que, en su ejercicio, se hace necesario que las mismas repiensen constantemente los conceptos de seguridad y privacidad, que permitan mayor comodidad para sus usuarios. Surgen así, conceptos como la "e-confianza", que no es más que "la actitud de aceptación, familiaridad y seguridad que los ciudadanos muestran hacia el uso de servicios a través de medios electrónicos" (San José, 2012, 41). Es importante reflexionar al

respecto, pues “la seguridad representa una limitación importante de cara a la utilización de nuevos servicios online” (San José, 2012, 40).

La carencia de privacidad e intimidad, unida a posibles suplantaciones de identidad, aparecen entre los temas más preocupantes para los usuarios. Aunque las Redes sociales, se preocupan por blindarse, “no están exentas de riesgos, especialmente aquellos relacionados con la seguridad de la información, la privacidad, la intimidad, la protección de sectores vulnerables de la población o la propiedad intelectual” (García, 2011. 98).

En el marco de una sociedad que se comunica ampliamente a partir de la internet, la sencillez para acceder a datos personales aumenta. Esto se apoya en “la dificultad para desaparecer información de la red, la viralidad de difusión de noticias o imágenes y la credibilidad que tanto los ciudadanos como los medios otorgan a esta información (positiva o negativa) y su efecto en la opinión pública” (San José, 2012, 44).

Entre tanto, aunque parecieran positivos los flujos de información, las redes afectan de manera violenta valores como – el honor, intimidad, propia imagen o a la protección de datos – de millones de usuarios, pues las mismas, no se comunican de manera directa con las legislaciones particulares de los países, o la información de la web resulta confusa, dificultando la comprensión de amplios sectores de la población, que no disponen de conocimientos jurídicos y tecnológicos.

De esta manera, derechos antes considerados como fundamentales y de difícil vulneración (privacidad e intimidad), se supeditan ante la necesidad de registrarse en las diferentes redes sociales, que, como requisito de acceso, demandan que los nuevos usuarios además de sus datos sociodemográficos “voluntariamente consignen su ideología política, su orientación sexual o sus preferencias religiosas. Toda esta información no solo será visible para todos los amigos o contactos del usuario, sino que, dependiendo de la configuración del perfil (más o menos pública), incluso sería accesible para todos los usuarios de la plataforma” (San José, 2012).

Pareciera que más que de la Red, depende de los usuarios, su propio manejo de la seguridad, en el sentido de que los mismos están en la obligación de decidir que tanto revelan o comparten, con los demás. Así, “El perfil de un usuario en una red social suele contener información personal, comentarios, fotografías y cualquier otro contenido que desee compartir. Dependiendo de quién tenga acceso a estos datos, su exposición a riesgo y la posibilidad de que su privacidad esté comprometida será mayor” (Monsalve & Granada, 2013. 134).

Para este trabajo, basado fundamentalmente en la Red Social Facebook, se puede observar “que el perfil del usuario está configurado por defecto como totalmente abierto al público, lo que obliga al usuario a tener que reconfigurarlo para limitar la visibilidad de sus datos” (San José, 2012), este proceso resulta incierto si atendemos que en su mayoría, los usuarios de la actualidad militan en tipologías de usuarios que migraron al uso de redes sociales con posterioridad a su aparición, tuvieron que redefinir su identidad y prácticas al uso de las mismas, como un fenómeno que no les es natural y que por lo tanto no comprenden de manera integral (Ruano, Congote & Torres. 2016). Así, abundan en las redes, perfiles de fácil acceso para otros, que pueden estar o no entre los contactos del usuario. Favorece la inestabilidad de la privacidad, los cambios y actualizaciones en el software, condiciones de uso y el hecho de que tras cada actualización haya que volver a configurar las opciones de privacidad y a la dificultad para frenar la difusión de datos que se registran. Lo que pone en peligro a los usuarios, especialmente en manos de personas malintencionadas (Rheingold, 2002). Además, la mayoría de redes, permite la identificación automática de perfiles por medio de buscadores, “recogiéndose como mínimo los datos básicos del usuario y su lista de contactos, cuando no imágenes y comentarios, permitiendo que cualquiera pueda acceder a ellos, pertenezca o no a la red social” (Asís, 2010. 78).

Son muchas las formas de exponer la privacidad y seguridad, los datos no sólo son usados con fines criminales. “Entre las formas más habituales de recopilación de direcciones para posteriormente realizar envíos masivos destacan: la creación de un perfil falso de algún personaje famoso para atraer

la atención de otros miembros, la creación de grupos o comunidades sobre determinada temática, o el desarrollo de aplicaciones que acceden a la libreta de contactos del perfil del usuario o incluso a la de su cuenta de correo electrónico o al listín telefónico de su móvil" (Christakis & Fowler, 2010. 18).
Las consecuencias de los problemas de seguridad pueden ser variadas, van desde la creación de mensajes Spam, que los ciberdelincuentes estructuran a partir de información recogida en los perfiles (edad, sexo, escolaridad), la suplantación de personas, el *phishing* y el *pharming*, suplantaciones de personas jurídicas (Mitjans, 2009), para obtener datos personales y claves de acceso al perfil del usuario, así como números de tarjetas de crédito, contraseñas, código PIN, etc. (Martínez, Sendín & García, 2013). Las situaciones que han sido descritas no definen una realidad estática; de hecho, es previsible que las amenazas evolucionen empujadas por las nuevas posibilidades técnicas que surgen constantemente.

2 Metodología

Se presenta un estudio de corte cualitativo, desarrollado a partir del Análisis Sociológico del Sistema de Discursos (Gutiérrez del Álamo, 2010). El corpus de análisis, se compone de cinco grupos de discusión mixtos (usuarios y abandonistas de las redes Facebook, Instagram y WhatsApp) con moderación no directiva, donde participaron sujetos entre los 16 y 45 años de edad, provenientes de diferentes sectores de la ciudad de Popayán - Colombia.
Después de realizar la transcripción textual de los grupos de discusión, se realizó la lectura y codificación de cada uno haciendo uso del programa Atlas.ti7; así, cada cita se vincula en el texto con uno o varios códigos deductivos. Seguido a la codificación abierta, se planteó la codificación axial que enlaza categorías en cuanto a sus propiedades y dimensiones (Strauss & Corbin, 2002), de este modo, se busca que los datos obtenidos en la codificación inicial puedan ser reagrupados, analizados y relacionados en busca de la relación entre categorías (percepción, usos, administración de la información, comunicación, identidad virtual).
Aplicando la técnica de análisis línea por línea, se generaron categorías iniciales (con sus propiedades y dimensiones) para identificar relaciones entre códigos (deductivos e inductivos); estas relaciones, se estructuraron a través del software de análisis como redes semánticas de sentido, para ser sustentadas teóricamente como categorías tipológicas. La identificación de tipologías que responden a perfiles actitudinales de usuarios de redes sociales virtuales, posibilita la obtención de una muestra de tipo estructural que representa posiciones discursivas asociadas a cada tipo.
Considerando que este análisis parte desde unos niveles más básicos de interpretación hasta unos niveles más complejos de reconstrucción del sentido de los discursos, se parte de un modelo central que considera ejes y perfiles, continuando con un análisis semiótico-estructuralista, que luego se complementa en una dimensión más bien pragmática o interpretativa del contexto, condensada en una matriz de relaciones estructurantes. El estudio, constituye una representatividad estructural que no tiene como propósito la generalización de resultados, pero si la aplicabilidad de los mismos.

3 Modelo de Análisis

El modelo de análisis constituye el componente central que orienta los resultados de la investigación. Se presentan cuatro tipologías de usuarios: observador, discreto, abierto y avatar; estas describen posiciones discursivas y actitudes asociadas con el manejo de la privacidad y la seguridad en redes sociales virtuales.

En la parte superior del esquema se sitúan los usuarios observadores y discretos, caracterizados por verificar la identidad de los usuarios con los que interactúan, controlar el tipo de información que comparten y evitar acciones que pongan en riesgo su privacidad. En la parte inferior, se ubican los usuarios abiertos y avatar, caracterizados por ser fácilmente accesibles, poseer una lista extensa de contactos y exhibir abiertamente su privacidad.

Fig. 1. *Tipología de usuarios de redes sociales virtuales, cada tipo se correlaciona con uno o más ejes. El eje X representa la seguridad, el eje Y la privacidad. De acuerdo con el esquema de análisis, el usuario observador concede mayor importancia a su seguridad que a su privacidad, el usuario avatar confiere mayor importancia a su seguridad que a su privacidad, el usuario discreto le da mucha importancia a su privacidad y seguridad y el usuario abierto asigna poca importancia a su privacidad y seguridad.*

.

Seguidamente, se plantea una Matriz de Pares sémicos y Ejes estructurantes. Esta parte del análisis, tiene como propósito obtener algunas distinciones claves como base para los análisis que se llevan a cabo más adelante. Las mismas permiten identificar aquellos pares sémicos que incorporan de mejor forma al resto de los códigos de oposición. Se ubicó en la primera parte de la lista a modo de referencia, el Usuario Discreto – Usuario Abierto, por ser estos perfiles los que se contraponen de forma más tajante en el modelo de análisis, a diferencia de los perfiles Observador y Avatar que pueden ser considerados como de transición.

Tabla 1. Pares Sémicos y Ejes Estructurantes

Ejes	Usuario Discreto	Usuario Abierto
Percepción	Piensa que las redes sociales son inseguras. Desconfía del uso que personas malintencionadas puedan hacer de su información personal.	No le preocupa la seguridad de su cuenta.
Usos	Aprendizaje, comunicación, mantenimiento de relaciones.	Establecimiento de relaciones, difusión, comunicación, ocio.
Administración de la información	Comparte contenidos para sí mismo, como una forma de almacenar en su perfil la información que le parece interesante.	Comparte información privada como estados de ánimo, logros, opiniones, así como las relaciones que posee con otros usuarios.
Comunicación	Sólo se comunica por medio del chat. La comunicación privada se	Comunica aspectos privados de su vida a través del muro y el chat.

	reserva para el contacto personal o cara a cara.	
Identidad virtual	Se representa por medio de imágenes o símbolos que dificultan su identificación fuera de la red.	Se muestra tal como es en las redes sociales.

Para dar continuidad al análisis, se plantea de manera conjunta un análisis comparativo de las categorías para cada perfil, a través de una Matriz de Oposiciones Estructurantes, donde se extraen aquellas unidades de sentido que representan los discursos predominantes de cada categoría.

Tabla 2. Oposiciones estructurantes.

Ejes	Observador	Discreto	Abierto	Avatar
Percepción	Se siente cómodo con la seguridad de su cuenta. Considera que tiene el control total de su información en las redes.	Piensa que las redes sociales son inseguras. Desconfía del uso que personas malintencionadas puedan hacer de su información personal.	No le preocupa la seguridad de su cuenta.	Sólo le preocupa su seguridad ante la posibilidad de ser descubierto.
Usos	Comunicación, difusión, entretenimiento, contacto con usuarios que le parecen interesantes.	Aprendizaje, comunicación, mantenimiento de relaciones.	Establecimiento de relaciones, difusión, comunicación, ocio.	Acceso a perfiles de interés, recolección de información sobre otros usuarios, manipulación de la información para beneficio propio.
Administración de la información	Comparte información superficial que no guarda relación profunda con su vida privada.	Comparte contenidos para sí mismo, como una forma de almacenar en su perfil la información que le parece interesante.	Comparte información privada como estados de ánimo, logros, opiniones, así como las relaciones que posee con otros usuarios.	Comparte información falsa que resulta atractiva para otros usuarios.
Comunicación	Comunica información general a través del muro e información privada por medio del chat.	Sólo se comunica por medio del chat. La comunicación privada se reserva para el contacto personal o cara a cara.	Comunica aspectos privados de su vida a través del muro y el chat.	Se comunica abiertamente sin profundizar en los detalles para no caer en la contradicción.
Identidad virtual	Expone algunas características superficiales de su identidad (no virtual) fuera de la red.	Se representa por medio de imágenes o símbolos que dificultan su identificación fuera de la red.	Se muestra tal como es en las redes sociales.	No representa ninguna de sus características reales en la red.

Finalmente, la Matriz de Relaciones Estructurantes, constituye el esquema que permite dar cuenta, de la capacidad explicativa que tienen las categorías de análisis, las cuales permiten acoplar de forma coherente el sistema de relaciones discursivas observadas.

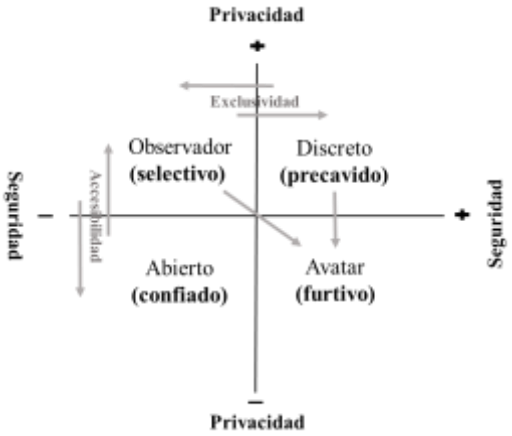

Fig. 2. *El esquema presenta las posiciones discursivas que identifican a los sujetos al interior de las tipologías.*

En la migración discursiva, el sujeto *observador* que revela un discurso de selectividad, puede tornarse *abierto* si incrementa su accesibilidad y comienza a compartir su información personal con todo tipo de público, en el sentido opuesto, el sujeto *observador* puede tornarse *discreto* si incrementa su exclusividad y comienza a interactuar en redes exclusivamente con personas que conoce fuera de la red; el sujeto *discreto* que se muestra precavido, puede volverse *observador* si pierde exclusividad y comienza a compartir su información personal con usuarios desconocidos fuera de la red; el sujeto *abierto*, que se representa por medio de un discurso de confianza, puede convertirse en sujeto *observador* si comienza a compartir su información sólo con usuarios conocidos o desconocidos que superan sus filtros de aceptación. Los sujetos observadores y discretos pueden migrar hacia la posición *avatar*, e incluso asumir esta postura sin dejar de pertenecer a sus respectivas tipologías en cualquier momento.

4 Hipótesis

De la revisión de los conceptos de privacidad y seguridad, se desprenden algunas hipótesis importantes que podrían aportar una base para el estudio de la interacción en redes sociales virtuales, esto en términos de supuestos y no en el sentido estadístico de aceptar o rechazar una prueba. Al respecto se plantean cuatro supuestos:

i. Los usuarios observadores, comparten su privacidad con personas desconocidas que les inspiran confianza.
ii. Los usuarios discretos, siempre controlan la información que comparten con otros, aun cuando su lista de contactos se compone sólo de personas que conoce fuera de la red.
iii. Los usuarios abiertos, sacrifican su privacidad por incrementar su lista de contactos.
iv. Los usuarios avatar, asumen la identidad de otros para proteger su privacidad mientras navegan.

5 Análisis

El análisis parte desde una aproximación o retrato sociológico de cada uno de los perfiles, como una forma de ofrecer los primeros antecedentes contextuales y personales de los sujetos que representan las tipologías. Los datos que aquí se presentan, corresponden a la información recabada por medio de la técnica de grupos de discusión.

El usuario *observador*, controla cuidadosamente la información que publica, la confiabilidad de los contactos con los que interactúa, las herramientas de privacidad y seguridad de las que dispone y los riesgos asociados a sus acciones; se siente cómodo compartiendo su intimidad en las redes, en la medida en que sólo comparte las cosas que desea. Generalmente utiliza su intuición y experiencia personal al momento de entablar nuevas relaciones interpersonales, por lo que su lista de contactos se compone de personas conocidas o desconocidas fuera de la red que generan confianza.

El fragmento que mejor representa la tipología se obtiene del sujeto 7 y sujeto 3, respectivamente, participantes del tercer grupo de discusión. *"Yo soy un poco más privado, la verdad o sea a mí me gusta como clasificar cada red social: lo que es WhatsApp, siento que es como para el vínculo que yo me desenvuelvo diariamente. No tengo personas desconocidas ni nada de eso, ni personas de otras ciudades, bueno de otras ciudades (sólo) si somos conocidos desde antes. Facebook ya está un poquito, un poco más abierto; o sea, busco personas de otras ciudades, sean nacionales (o) internacionales, pero digamos que por una u otra razón ya he tenido como un contacto anteriormente. Ya lo que es Instagram ya es totalmente desconocido, en relación con mis seguidores y con las personas que yo estoy siguiendo, porque en Instagram sólo me guío por lo que a mí más me gusta, nada más; igualmente, siento que las cosas que coloco ahí --o sea aparte de que son personales-- no son como tan que me describan a mí, sino como que es algo muy llano, algo muy superficial".*

"Por experiencia y de cosas malas que pasan uno ya comienza como filtrar a la gente, entonces pues yo que hago ehh entonces, por ejemplo, si me envían una solicitud veo que, más que la imagen sea bonita o algo así, que tenga como congruencia la imagen del perfil como con la descripción que te dicen, por ejemplo si tienen una imagen de una fotografía así espectacular, dice que le gusta la fotografía, dice que estudia en una universidad… pues ya digo "no… este man como que si tiene algo" o sea, no es cualquiera, si tiene congruencia la imagen con lo que dice en su perfil, entonces si es eso lo que uno busca… es que haya congruencia, que uno se puede sentir identificado con algo para ya después poder entablar una amistad".

El usuario *discreto*, controla cuidadosamente el tipo de información que comparte, se abstiene de opinar abiertamente sobre temas específicos y abandona la red cuando percibe que vulneran su intimidad o seguridad; le preocupa que utilicen su imagen o información personal sin su consentimiento, desconfía de las intenciones de determinados usuarios y prefiere pasar desapercibido. Su lista de contactos se limita a personas conocidas, con las cuales mantiene algún grado de proximidad fuera de la red.

El fragmento que mejor representa la tipología se obtiene del sujeto 5, del tercer grupo de discusión. *"Yo no tengo Facebook hace 3 años, pues a mí no me gustaba que la gente me mirara o me buscara, entonces yo por ejemplo en el chat siempre ponía "desconectado" o simplemente la persona, o la privacidad siempre la tenía para mí; porque yo resultaba viendo el contenido de otras personas o cosas así, entonces eso es lo que no me gusta a mí. Otras personas deberían interesarse al menos en tener su propia privacidad".*

El usuario *abierto*, expone su intimidad sin mayor reserva, posee una lista extensa de contactos, que incluyen personas desconocidas fuera de la red o con las que mantiene interacciones pobres al interior de la misma; debido a las pocas restricciones de privacidad, prácticamente cualquier usuario tiene acceso a su información personal, fotografías, publicaciones e incluso números y direcciones de contacto. Considera que el objetivo de las redes sociales es compartir con cualquier persona, por lo

que se siente cómodo opinando abiertamente sobre todo tipo de temas, referenciando las actividades que realiza, compartiendo sus estados de ánimo y visualizando los lugares en los que se encuentra.
Los fragmentos que mejor representan la tipología se obtienen del sujeto 1 y sujeto 5 respectivamente, del tercer grupo de discusión. "*Siempre me ha gustado lo que es la libertad y las relaciones libres, nunca bloqueo a nadie, nunca dejo de seguir, es más, si (alguien) le da "seguir" sigue así, nunca lo cambio, porque manejo la libertad en cada uno de los vínculos que yo manejo con las personas; es más, no tengo que ocultar nada, soy lo que soy y lo muestro tal y como es en mi Facebook; y al igual en ninguna parte del Facebook dice que si tú no eres así y así no puedes abrir tu página" (…)* "*No manejo filtros para bloquear nada, porque la idea de mantener las redes sociales es como digamos estar uno abierto a todo el mundo; si yo comparto una publicación en mi muro y yo bloqueo que cualquier otra persona lo pueda ver, entonces básicamente no estoy cumpliendo un el fin que es compartir con quien sea".*
El usuario *avatar*, adecúa la información de su cuenta de acuerdo a sus intereses y objetivos particulares, diseña una imagen idealizada o atractiva de sí mismo, interactúa con muchos usuarios y se preocupa por parecer auténtico. Puede adoptar la imagen de alguien distinto para expresar características de sí mismo que no se sentiría incomodo expresando desde su cuenta personal, asumir identidades completamente diferentes a la suya, o utilizar varias cuentas para lograr diferentes propósitos, como observar sin ser observado y recolectar información de su interés; generalmente posee un gran número de contactos y controla su seguridad evitando situaciones que lo pongan en descubierto.
Los fragmentos que mejor representan las tipologías se obtienen del sujeto 3 del quinto grupo de discusión, el sujeto 1 del quinto grupo de discusión, el sujeto 5 del grupo piloto y el sujeto 5 del cuarto grupo de discusión, respectivamente. *"La mayoría de redes sociales de la red son muy vulnerables ya que piden un email y password los cuales son muy inseguros, por ejemplo, el Outlook actual es muy vulnerable uno se puede meter y ya tiene la contraseña de todas las redes sociales" (…) "Yo hackeo Face (refiriéndose al Facebook), desde varias cuentas y monitores para hackear, lo que pasa es que lo descubren rápido" (…) "Yo diseñé un scribd y hay gente, amigos que se conectan, se despiertan y leen Facebook y se acuestan, y antes de dormir revisan sus últimas actualizaciones; pude ver los patrones de sueño de las personas, obviamente eso es ilegal ¿no? pero uno emplea rutas hasta llegar a eso" (…)* "*Yo tengo dos Facebook; uno como más privado que es para estar en comunicación con la familia, los amigos, mirar cosas, pasar el tiempo (y) otro, que es más general, como para que las personas te miren".*
Por un fenómeno de deseabilidad social y censura, los usuarios avatar en los grupos de discusión evitaron profundizar en la descripción de sus actividades.

6 Consideraciones Finales

Las redes sociales virtuales, representan un escenario de interacción, caracterizado por la inmediatez, la multipresencia, el gigantesco flujo de información, el anonimato y la posibilidad de establecer contacto prácticamente con cualquier otro usuario en la red. Debido a esto, en el escenario virtual, conviven diferentes tipos de usuarios, con posiciones discursivas y perfiles actitudinales estructuralmente distintos entre sí, lo que genera dinámicas y flujos particulares, donde la única regulación posible es la que cada usuario realiza desde su cuenta.
Los usuarios observadores, son selectivos, tienen filtros subjetivos para evaluar a las personas que intentan contactarlos, sustentados en sus conocimientos y experiencias previas; de este modo, identifican y evitan a los usuarios indeseados (incluido el avatar). Algunos de estos filtros incluyen hablar a través del chat o mensajería interna/privada, solicitar identificación por videollamada, recurrir a los amigos en común para indagar sobre la identidad de la persona o simplemente mirar el contenido

de la cuenta para decidir si el usuario que envía una solicitud de amistad o contacto es lo suficientemente interesante como para aceptarlo. Aunque son exclusivos, su lista de contactos no se limita a personas conocidas, sino también a aquellos desconocidos que se ganan su confianza o le parecen interesantes.

Los usuarios abiertos, son accesibles y tienden a ser exhibicionistas. Los perfiles abiertos corresponden a modelos, artistas o personas reconocidas que se benefician económica (accediendo a nuevas ofertas laborales) o psicológicamente (alcanzando reconocimiento social) de la visualización y difusión de los contenidos de su cuenta, sin que esto signifique desconocer la existencia de perfiles de personas comunes que exponen su vida privada para alcanzar popularidad entre los usuarios o mantener un nivel elevado de interactividad (representado en alcanzar gran número de seguidores, Likes, comentarios y solicitudes de amistad). Otro tipo de usuarios abiertos, son aquellos que comparten públicamente el contenido de su cuenta, porque desconocen cómo configurar la privacidad y seguridad de la misma.

Los usuarios discretos, son desconfiados y su interacción se limita a revisar y compartir contenidos sin involucrar aspectos privados de su vida fuera de la red. Generalmente, el miedo a que suplanten su identidad, utilicen su información personal para cometer actos delictivos o puedan ser contactados por personas malintencionadas, conlleva que se abstengan de subir fotografías de sí mismos o de su entorno social; en lugar de ello, emplean imágenes que los representan o fotografías en las que se dificulta su reconocimiento, de manera similar, no escriben su nombre completo, colocan un seudónimo o las iniciales pretendiendo ser identificados sólo por aquellos que los conocen realmente. Desconfían de los sitios que solicitan información personal (como su número telefónico, lugar de residencia o trabajo) como requisito para registrarse.

Finalmente, los usuarios avatar, diseñan perfiles con contenido llamativo (imágenes de mujeres u hombres físicamente atractivos, personas famosas, e incluso un perfil de fans o seguidores). El avatar nunca expone su privacidad, porque asume la identidad de otros; evita dar demasiados detalles sobre sí mismo para no caer en la contradicción, inventa excusas para no ser contactado por videollamada, dilata la posibilidad de un encuentro cara a cara y abandona la interacción cuando se siente inseguro o piensa que puede ser descubierto.

7 Conclusión

A través de la técnica cualitativa de los grupos de discusión, fue posible indagar en las percepciones, representaciones y comportamientos de los sujetos, respecto al manejo de la privacidad y seguridad en redes sociales; evidenciando, una relación entre la percepción subjetiva --asociada a la experiencia personal, el conocimiento de las redes y el aprendizaje social-- y las representaciones sociales intersubjetivas, como un factor significativo en la adopción de una actitud de accesibilidad o exclusividad, que se manifiesta en el tipo de información personal que los usuarios comparten según la seguridad que perciben en las redes. De manera similar, el análisis sociológico del sistema de discursos, evidenció diferentes maneras de representar la accesibilidad y exclusividad en cada sujeto, encontrando, criterios y métodos subjetivos más o menos generalizados, que les permiten identificar a otros, establecer límites, definir juicios para la aceptación o rechazo, y sentirse seguros en la interacción.

Agradecimientos. Al grupo de Investigación PSIEDU del programa de psicología de la Universidad Cooperativa de Colombia, sede Popayán. Por su apoyo y gestión para la realización, presentación y publicación de este trabajo.

Referencias

Asís, Agustín (2010). *'Redes sociales y protección de datos. Redes Sociales e interpretación en Red: una perspectiva técnica-jurídica*', curso de verano, 26 al 30 de julio, Santander, Universidad de Cantabria.

Borgatti, S. (2009). *Network Analysis in the Social Sciences.* Boyd, D. y Ellison, N. (2008). Social Network Sites: Definition, History, and Scholarship.

Castells, M. (2006). *La era de la información. Economía, sociedad y cultura.* La sociedad red. México: Siglo XXI.

Castells, M. (2008). *The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance*. The Annals of the American Academy of Political and Social Science.

Castells, M. (2009). *Comunicación y poder.* Madrid: Alianza Editorial.

Christakis, Nicholas A. & James H. Fowler (2010). *Conectados. El sorprendente poder de las redes sociales y cómo nos afectan.* Madrid, Taurus.

Del Álamo, F, C. (2009). Análisis sociológico del sistema de discursos, Madrid: Centro de Investigaciones Sociológicas.

García Jiménez, A. (2011). *Una perspectiva sobre los riesgos y usos de internet en la adolescencia. Icono 14*, 9(3), 396-411. doi: 10.7195/ri14.v9i3.62.

Martínez, E., Sendín, J.C., & García Jiménez, A. (2013). *Percepción de los riesgos en la red por los adolescentes en España: usos problemáticos y formas de control. Anàlisi: Quaderns de comunicació i cultura*, (48), 111-130.

Monsalve, J & Granada, L. (2013). *Redes sociales: aproximación a un estado del arte. Revista Digital Lámpsakos, (9),* 34-41.

Rheingold, H. (2002). *Smart Mobs: the Next Social Revolution.* Cambridge, Massachusetts: Perseus San José, Pablo. Seguridad y privacidad en Redes Sociales. Investigación y marketin. Aedemo N. 124.

Strauss, A., & Corbin, J. (2002). Bases de la investigación cualitativa. Técnicas y procedimientos para desarrollar la teoría fundamentada. Bogotá: CONTUS---Editorial universidad de Antioquia.

Wassermann, S., Faust, K. (1995). *Social Network Analysis.* New York: Cambridge University Press Mitjans Perelló, E. (2009). Impacto de las redes sociales en el Derecho a la protección de datos personales. *Anuario de la Facultad de Derecho (Universidad de Alcalá)*, (2), 107-129.