ACTIVIDADES COTIDIANAS EN REDES SOCIALES. ESTUDIO DEL COMPORTAMIENTO HABITUAL Y LAS MEDIDAS DE PROTECCIÓN DE LOS USUARIOS DE FACEBOOK, INSTAGRAM Y TWITTER

Mariana N. Solari-Merlo

Universidad de Cádiz

Title: *Everyday activities in social networks. A study of usual behaviour and the mechanisms to protect Facebook, Instagram and Twitter users*

Resumen: El creciente uso de las redes sociales conlleva una exposición cada vez mayor de información personal susceptible de ser utilizada para la comisión de diversos delitos. Este nuevo espacio de criminalidad ha sido analizado en diversas ocasiones a la luz de la Teoría de las Actividades Cotidianas y de los estilos de vida, poniendo especial interés en las rutinas habituales de los usuarios de estas plataformas –estilos de vida online– y en las medidas de autoprotección que establecen –guardianes– para evitar convertirse en objetivos adecuados. Sobre la base de estos desarrollos, el presente trabajo analiza el comportamiento habitual de los usuarios de las principales redes sociales –Facebook, Instagram y Twitter– a efectos de determinar su grado de autoexposición, las medidas de autoprotección y las consecuencias negativas experimentadas con su uso.

Palabras clave: Teoría de las Actividades Cotidianas; Cibercriminalidad; Criminalidad en Redes Sociales; Cibercriminología; Autoexposición online.

Abstract: *The increasing use of social networks leads to an increasing exposure of personal information that can be used for the commission of various types of crimes. This new space of crime has been analysed on different occasions in light of the Routine Activity Theory and Lifestyles Theory, placing special interest in the habitual routines of users of these platforms - online lifestyles - and in the self-protection measures that they establish - guardians - to avoid becoming a suitable target. Based on these developments, this work analyses the habitual behaviour of the users of the main social networks –Facebook, Instagram and Twitter– in order to*

determine their degree of self-exposure, their self-protection measures and the negative consequences experienced with their use.

Keywords: *Routine Activity Theory; Cybercriminality; Social Media Crimes; Cybercriminology; Online Self-exposure.*

1. Introducción

La criminalidad que tienen lugar en el entorno virtual se ha ido expandiendo y encontrando nuevas oportunidades conforme el uso de internet se ha ido extendiendo[1]. En este sentido, podemos observar una incorporación masiva de internet en la vida diaria de los ciudadanos en todo el mundo. El crecimiento de los servicios virtualizados supone una mayor interacción y la extensión del espacio virtual a planos que permanecían ajenos a este ámbito. Así, junto al comercio y los medios de información, los ciudadanos tienen acceso a un conjunto cada vez más variado –y extenso– de servicios de la administración pública, la banca, sanidad, formación, entretenimiento, entre otros.

En el ámbito de la cibercriminalidad, esto supone la aparición de nuevas oportunidades delictivas –ya sean asociadas a nuevas formas de criminalidad o formas de criminalidad tradicionales adaptadas al entorno virtual (McGuire y Dowling, 2013)- toda vez que internet permite ahora el acceso a bienes jurídicos que hasta entonces permanecían ajenos a este ámbito. Esto es, cada interacción *online* supone la exposición de determinadas áreas, bienes, en los que se desarrolla la personalidad y que guardan relación, en cada caso, con dichas interacciones; la intensificación de esta actividad *online* –tanto por su frecuencia como por su extensión a nuevos espacios– supone una mayor exposición que, de no adoptarse las precauciones necesarias, conduce a una mayor vulnerabilidad.

En la actualidad, no obstante, es de destacar otro fenómeno añadido a esta situación y es que, junto a esta intensificación en su uso, los servicios

[1] Basta comprobar los estudios de cibercriminalidad que anualmente publica el Ministerio del Interior de España para comprobar este aumento constante. Especialmente desde los años 2016 hasta el 2019 –último informe disponible–, se constata un aumento de los delitos informáticos. En el estudio de 2020 se afirma que los ciberdelitos detectados crecieron un 35,8% respecto al año anterior. Cfr., Ministerio del Interior, 2020.

que ofrece internet y la web se han ido convirtiendo en canales multidireccionales y abiertos (PÉREZ SAN-JOSÉ, 2012, p. 5), donde los usuarios interactúan y se convierten en agentes activos del espacio, no meros receptores de información. A través de las redes sociales (en adelante, RRSS), foros, *blogs, webs* colaborativas, *microblogging*, *vlog*, videotutoriales, etc., el individuo se hace visible y se convierte en generador de contenido, de opinión, conocimiento. Eso es, pasa a un primer plano y se incrementa su exposición personal. Entre estos nuevos espacios surgidos en el ámbito virtual, destacan especialmente las RRSS. Surgidas como plataformas de encuentro e interconexión entre personas, su utilización masiva en todo el mundo las convierte en un medio especialmente propicio para la criminalidad toda vez que, como se verá, la propia finalidad y el modo de funcionar de las RRSS devienen elementos facilitadores del delito.

2. Marco teórico

Las aproximaciones criminológicas más actuales a la cibercriminalidad abordan el fenómeno desde el ámbito de las teorías de la oportunidad criminal. Centradas en el contexto criminal, estos enfoques toman como punto de partida la teoría de los estilos de vida (HINDELANG *et al.,* 1978) y la teoría de las actividades cotidianas (en adelante, TAC) (COHEN y FELSON, 1979) –posteriormente combinadas (COHEN *et al.,* 1981)-, adaptándolas al espacio virtual.

La teoría de los estilos de vida señala que las diferencias en las rutinas diarias –laboral, escolar y de ocio– inciden en la posibilidad de ser víctima de un delito. Cuanto mayor sea la exposición a determinados lugares, situaciones o personas –peligrosos–, mayor será el riesgo de victimización. Por su parte, la TAC señala que la oportunidad criminal tiene lugar cuando coinciden en un mismo espacio un agresor motivado y un objetivo adecuado, sin que existan guardianes capaces de evitar el evento. En su formulación original, COHEN y FELSON (1979) parten del análisis de los cambios sociales y tecnológico ocurridos durante los años 1947 y 1979, entendiendo que reflejan una transformación en los estilos de vida de los ciudadanos. Las personas pasan más tiempo realizando actividades fuera del hogar, lo que supone, por un lado, que entren en contacto con un mayor número de desconocidos –posibles delincuentes– y, por otro, que los hogares pasen más tiempo vacíos, desprotegidos (MEDINA ARIZA, 2013, p. 328). Como señala CHOI (2008, p. 311), podemos entender que la TAC es un desarrollo de la teoría de los estilos de vida; así, sin negar la importancia de la motivación del criminal (NGO y PATERNOSTER, 2011, p. 755), vienen a poner el acento en el estudio del comportamiento, las actividades y el contexto situacional de los delitos (PRATT *et al.,* 2010, p. 273)[2].

[2] Como señalaría posteriormente FELSON, cualquiera es capaz de cometer un delito, aunque, según su tipología, existen personas con mayores probabilidades (FELSON y ECKERT, 2018,

2.1. La TAC en el entorno virtual

El entorno virtual, no obstante, la TAC presenta determinadas peculiaridades que condicionan la interacción de los elementos clave de esta teoría. El espacio y el tiempo adquieren una significación diferente en el espacio virtual que supone, entre otras cosas, que agresor y víctima no tengan que confluir necesariamente en un mismo momento para que el delito tenga lugar (YAR, 2005). Es decir, mientras que, en su formulación inicial, la TAC se basa en la confluencia en un mismo lugar y tiempo de un agresor motivado, un objetivo adecuado y la ausencia de guardianes capaces, en un entorno virtual desaparece esa necesidad de reunión –es posible, pero no necesaria.

Como señala YAR (2005, pp. 418 y ss.), si algo caracteriza al espacio virtual es su extrema volatilidad y plasticidad. Los entornos virtuales cambian o, incluso, desaparecen con regularidad, así como también lo hacen sus actores, simplemente desconectándose de la red. El tiempo, por su parte, tiene una concepción diferente toda vez que en internet la actividad resulta ininterrumpida permitiendo la interacción de sujetos de diferentes partes y con distintas zonas horarias. En este sentido, resulta difícil realizar predicciones basándose en estos parámetros dado su carácter volátil, cambiante. Tiempo y espacio –elementos clave en la prevención situacional[3]- conllevan diferentes implicaciones en el ámbito virtual que van a condicionar la interacción de los sujetos –aquí, agresor, víctima y guardián– de un modo distinto a lo que lo hacen en el espacio físico. La volatilidad y el carácter atemporal, la desorganización (WILLIAM, 2016, p. 23), junto con las restantes características de internet[4], dificultan en gran medida la prevención del delito.

Centrándonos en el objeto de interés para el agresor –esto es, el objetivo adecuado–, es coincidente la doctrina[5] en señalar que, en el entorno

---

p.28). En el mismo sentido lo entienden ECK y CLARKE, quienes desarrollarían esta teoría añadiendo elementos preventivos que inciden en cada ámbito (ECK y CLARKE, 2003). La oportunidad es vista como causa de la victimización por lo que la introducción de medidas para reducir aquella conllevará la reducción de esta (WHITTY, 2019, p. 280).

[3] FELSON y CLARKE, 1998, pp. 14-15; COHEN, L.E. y FELSON, M., 1979, pp. 588-608. En profundidad, REDONDO ILLESCAS, S. y GARRIDO GENOVÉS, V., 2013, pp. 489-504, y MCLAUGHLIN, E., 2006, pp. 365-367.

De especial relevancia, LECLERC, B. y FELSON, M., 2016, pp. 116-131, y ECK, J. E. y CLARKE, R. V., 2003, pp. 7-39.

[4] En profundidad, MIRÓ LLINARES, F. 2011, pp. 5 y ss. quien apunta, junto a los citados caracteres –intrínsecos–, algunos caracteres extrínsecos del ciberespacio como son su deslocalización, transnacionalidad, neutralidad y descentralización o su carácter popularizado y anonimizado, entre otros. Newman y Clarke resumen estas características con el acrónimo SCAREM; *Stealth* (sigilo), *Challenge* (desafío), *Anonymity* (anonimato), *Reconnaisance* (reconocimiento), *Escape* (escape), y *Multiplied* (multiplicación), esto eso, los delitos pueden reproducirse fácilmente y dar lugar a nuevos delitos a través de la información obtenida. Confróntese NEWMAN, G. R y CLARKE, R. V., 2003, pp. 61 y ss.

[5] MIRÓ LLINARES, F. 2011, p. 11 y NEWMAN y CLARKE, 2003, p. 68, entre otros.

virtual, todo objetivo puede reducirse a la obtención de información, datos que dan acceso a otros bienes. Así, por ejemplo, la contraseña que da acceso a la cuenta bancaria, una base de datos con información sobre clientes, documentos confidenciales con información de inteligencia o secretos de empresa, entre otros.

Felson y Clarke (1998, pp. 5 y ss.) señalan las características que deben tener los objetivos para que puedan ser considerados adecuados[6], apetecibles para el agresor, resumiéndolos en el acrónimo VIVA (según su formulación original, *Value, Inertia, Visibility* y *Access*). En primer lugar, el objetivo debe ser valioso para el agresor, deseado, sin entrar a valorar los motivos de esa estimación o especial interés; en segundo lugar, la inercia hace referencia a la resistencia que ofrece el objeto en sí –por su gran tamaño y dificultad para el transporte, por ejemplo–; asimismo, el objeto debe ser visible para el agresor, debe presentar cierto grado de exposición que permita su percepción; y, finalmente, debe ser accesible, deben existir pocos obstáculos para el acceso del agresor al objetivo y posterior huida. Yar (2005, pp. 419 y ss.), al adaptar estas características al entorno virtual, señala que el valor del objeto tiene, por lo general, un carácter informacional; su inercia reside en el posible peso –virtual– que tenga el objeto a la hora de, por ejemplo, realizar una descarga de datos o copia ilícita; su visibilidad es consustancial al propio hecho de residir en el espacio virtual, esto es, toda vez que internet es un espacio público, todo objeto allí introducido se hace visible; y, por último, su accesibilidad hace referencia a las medidas de seguridad asociadas al objeto, tanto para dificultar el acceso como para identificar intrusiones.

Cabe hacer algunas precisiones respecto a esta adaptación. Coincidimos con Miró Llinares (2011, pp. 31 y ss.) cuando señala que es difícil hablar de inercia en el espacio virtual. Los caracteres intrínsecos en el espacio virtual apenas se diferencian y la evolución de las TICs proporciona los medios para salvar este obstáculo muy fácilmente. Por otra parte, la visibilidad no deriva de la introducción del objeto en el espacio virtual sino que requiere algo más, es necesaria cierta interacción para hacernos visibles *online*. Es a través de la participación activa en internet como somos percibidos por los demás y exponemos los bienes correspondientes a cada ámbito de interacción. Así, por ejemplo, al realizar una compra, utilizar los servicios de banca, escribir en un blog, participar en un foro o, especialmente, utilizar las RRSS. En lo que respecta a la accesibilidad, entendemos que los dispositivos informáticos descritos por Yar resultan más cercanos al concepto de guardián que al de accesibilidad. Antivirus, encriptadores, rastreadores, entre otros, constituyen medidas de seguridad introducidas por la propia víctima para prevenir los ataques o

[6] Clarke desarrollaría las características que tienen los objetos de interés (*hot products*) bajo el acrónimo CRAVED entendiendo que estos debían ser *Concealable, Removable, Aviable, Valuable, Enjoyable* y *Disponsable.* En profundidad, Clarke, 1999.

posibilitar la identificación el autor en caso de acceso ilícito al bien. Las medidas que dificultan el acceso al objetivo guardan relación con las actividades habituales, rutinarias, que las potenciales víctimas realizan en el espacio virtual, especialmente en los casos donde la información –esto es, el objetivo– es proporcionada por esta.

En este sentido, las RRSS se vuelven un objeto de especial interés para la cibercriminalidad desde el punto de vista de la TAC dado que la finalidad de estos nuevos espacios de interconexión entre personas y el modo de funcionamiento supone que sean los propios usuarios quienes de modo voluntario expongan información de carácter personal ante una audiencia que puede tener un carácter indeterminado. Es decir, son los propios usuarios, víctimas potenciales, quienes contribuyen a hacer los objetivos adecuados.

2.2. La TAC en el entorno de las RRSS

Como se ha anticipado, la finalidad y funcionamiento de las RRSS favorecen la aparición de objetivos adecuados. En este sentido, y obviando en un primer momento las diferencias específicas entre las distintas RRSS, podemos entender que la finalidad de todas ellas es la interacción de sus usuarios, el compartir información, gustos, debatir, opinar, etc. Así, son los propios usuarios quienes introducen los objetivos en el ciberespacio (Miró Llinares, 2011, pp. 27-28, y 2013) puesto que, a diferencia de lo que ocurre en el espacio físico, en el ámbito virtual los bienes expuestos en cada interacción serán únicamente aquellos que guarden relación con la finalidad de dicha interacción; ahora bien, una vez introducidos, el grado de accesibilidad es mayor. Podemos visualizar esto claramente con un ejemplo. Analizando una misma situación en el espacio virtual y en el físico, podemos pensar en un sujeto que se encuentra con un grupo de amigos o conocidos en una cafetería. Al igual que ocurre en el ámbito virtual, será dueño de decidir qué información comparte con el resto, siendo dichos amigos los únicos destinatarios de la información; en las RRSS, en cambio, de no adoptar las precauciones necesarias –sobre esto se volverá más adelante–, el número de sujetos que puede tener acceso a dicha información superará siempre a los partícipes en la conversación puesto que la información es visible para terceros. La víctima potencial tendrá cierto control de la audiencia únicamente si la charla tiene lugar en su página personal de la red social (esto es, en su muro) y tiene establecida alguna configuración de privacidad que reduzca el número de personas que puede tener acceso a la información, sea con carácter general (evitando RRSS abiertas, donde cualquier extraño al usuario puede acceder a su contenido), sea restringiendo entre sus contactos aquellos que tienen acceso a la misma (cuando la RRSS lo permite, como ocurre en Facebook, establecer subgrupos de privacidad evitando que todos los contactos puedan acceder a su información). En el caso de

que la conversación tenga lugar en otro muro ajeno a la víctima, se pierde control sobre la audiencia que puede leerla dado que, incluso cuando dicha publicación pueda ser borrada por el autor o la audiencia limitada por un administrador, no es posible controlar las capturas de pantalla de la misma que pudieran realizarse y sus posteriores remisiones.

Esto es, en el ciberespacio, la víctima decide qué información compartir en el transcurso de una conversación (y, hasta ahora, no hay diferencias con el espacio físico) pero, una vez compartida, la información es accesible a una audiencia mayor[7]. En el espacio físico, no obstante, cualquier encuentro conlleva la exposición de un número mayor de bienes, aquellos que podemos entender como personalísimos y que son inseparables del sujeto. Así, continuando con el ejemplo, nuestros sujetos estarán exponiendo su integridad física, patrimonial, libertad sexual, entre otros, toda vez que pueden ser objeto de ataques –agresiones físicas, sexuales, robos, etc.- durante el encuentro, con anterioridad y posterioridad al mismo. Esto no ocurre en el espacio virtual ya que los usuarios pueden decidir qué bienes hacer visibles frente a terceros. Así, por ejemplo, la información proporcionada *online* difícilmente facilitará la comisión de un robo o una agresión sexual (esto es, haga accesible el patrimonio o la libertad sexual de la víctima) si esta no guarda relación con dicho contenido[8].

Es en este sentido en el que apuntábamos que la razón de ser de las RRSS puede hacer a los objetivos especialmente adecuados. Señalábamos anteriormente que es la interacción de los sujetos –objetivo de las RRSS– lo que los hace visibles *online* y, en el transcurso de dicha interacción, son los propios sujetos quienes van introduciendo bienes valiosos en el ciberespacio y los hacen accesibles para un número indeterminado de personas. Partiendo de este presupuesto, cabe afirmar que la decisión de participar en RRSS conllevará en todos los casos algún tipo de exposición, y que serán las actividades rutinarias –y el estilo de vida *online*– de los usuarios y las medidas de protección que establezcan –guardianes– los elementos que pueden reducir la visibilidad o la accesibilidad a su información.

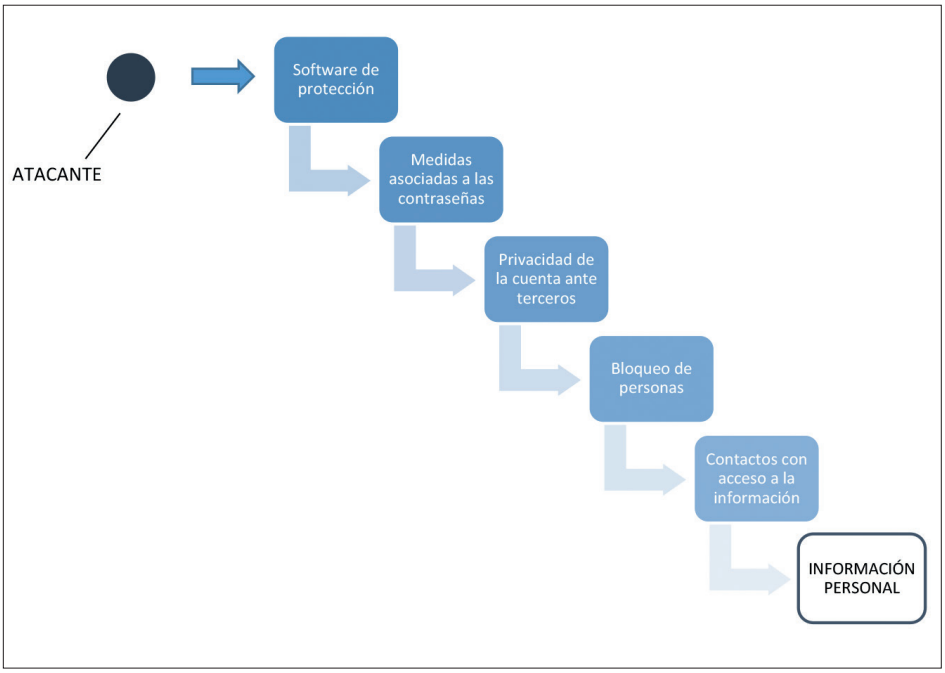
---

[7] Piénsese, además, que las conversaciones *online* quedan expuestas permanentemente en el correspondiente muro por lo que el acceso a la información puede tener lugar en cualquier momento, incluso uno muy posterior al día en que dicha charla tuvo lugar. Algunas RRSS –Facebook, por ejemplo– posibilitan el limitar la antigüedad de la información proporcionada a través de configuraciones que permiten limitar el visionado de publicaciones anteriores a determinada fecha, pero, una vez más, esta posibilidad dependerá de que la conversación haya tenido lugar en el muro de la víctima y de que esta, efectivamente, habilite dicha configuración.

[8] Cabe señalar que se hace referencia tanto a delitos que tienen lugar en el espacio virtual como a los que tienen lugar en el espacio físico. En relación con estos últimos, los usuarios de RRSS pueden compartir información sobre su lugar de residencia, de trabajo, zonas habituales de ocio o, incluso, planes de futuro, entre otros, que posibiliten la localización física de los sujetos.

En relación con este último elemento, la siguiente ilustración resume los mecanismos de protección con los que cuenta la víctima a efectos de preservar información. Lógicamente, la forma más efectiva de hacerlo es evitar compartir información personal –si no hay objeto de interés, no habrá ataques– pero, entendemos, esto resulta opuesto a la propia finalidad de las RRSS y, por ende, de sus usuarios.

Ilustración 1. Guardianes en RRSS[9]



Así, algunas medidas (guardianes) que los usuarios adoptan para evitar el acceso de terceros a sus sistemas informáticos o cuentas personales pueden ser calificadas como guardianes técnicos (Choi, 2008, Holt y Bossler, 2009, Ngo y Paternoster, 2011, y van Wilsem, 2013), tales como la utilización de *softwares* de protección –antivirus, anti-intrusiones, *firewall*, etc.-, mientras que otras, más sencillas de implementar, guardan relación con las contraseñas[10] y han sido calificadas como guardianes personales, guardián social o autoguardián (Miró Llinares, 2013, p. 11). El empleo de estas medidas suele guardar relación con la prevención de conductas de *hacking* y acceso informático no consentido por parte de personas extrañas a los usuarios.

[9] Elaboración propia.

[10] Tales como la dureza de la misma, el cambiarla frecuentemente, no compartirla con terceros, no dejarla almacenada en sitios públicos, etc.

Entre los guardianes personales, y en el ámbito específico de las RRSS, los usuarios pueden también adoptar otras medidas a efectos de limitar la aproximación del potencial atacante al objeto de interés. Así, es posible configurar la privacidad de la cuenta para que la información publicada sólo sea visible para los contactos de su titular, excluyendo el acceso de terceros. Incluso –y avanzando un paso en la protección de la privacidad– las principales RRSS (Facebook, Instagram y Twitter, entre otras) permiten limitar las posibilidades de contacto con otros sujetos a través del sistema de bloqueos. Esto es, bloqueado un usuario, entre dichas cuentas no se podrá establecer ningún contacto, siquiera visualizar la propia existencia de la cuenta salvo que se recurra a la cuenta de un tercero y, a través de esta, visualizar la cuenta bloqueada. Asimismo, y como último recurso a destacar, algunas RRSS como Facebook cuentan con la posibilidad de crear subgrupos entre los contactos, permitiendo al usuario decidir qué información comparte con unos u otros sin que en ningún caso los destinatarios se enteren a qué grupo pertenecen. Como se representa en la ilustración, la distancia la distancia entre el atacante y el objetivo se reduce conforme se supera alguna medida de protección.

En última instancia, los usuarios pueden controlar la información que ellos mismos hacen pública, omitiendo datos que puedan dar acceso a otros bienes protegidos. Entendemos que este tipo de medidas, no obstante, resultan más cercanas a las precauciones a adoptar en el desenvolvimiento habitual en las RRSS –esto es, a las actividades cotidianas– que a la noción de guardián y, en ese sentido, el estudio llevado a cabo distingue el análisis de las acciones de los usuarios que consideramos contribuyen a hacer los objetivos más atractivos, de aquellas otras implementadas para dificultar el ataque. Esta información será expuesta en la metodología, pero, con carácter previo, es conveniente conocer los antecedentes empíricos que han analizado diversas formas de cibercriminalidad desde el punto de vista de la TAC.

2.3. Antecedentes empíricos

Existen diversos estudios que han testado la adecuación del modelo planteado por la TAC para explicar la cibercriminalidad. Así, en lo que respecta a las actividades habituales de las víctimas, se ha señalado la relación entre el tiempo pasado *online* y, en particular, el tipo de actividad realizada en el ciberespacio, por un lado, y el ser objeto de victimización, por otro, Holt y Bossler (2009) encontraron que el número de horas pasadas en salas de chat o utilizando mensajería instantánea guarda correlación con el riesgo de sufrir ciberacoso. En el mismo sentido, Marcum *et al.* (2010) destacan esta relación para ciberabuso añadiendo a las anteriores variables la frecuencia e intensidad del uso de RRSS y el envío de email. Ngo y Paternoster (2011) precisan que no cabría hablar tanto de la relevancia del tiempo pasado en el espacio

virtual, sino sólo del tiempo pasado realizando actividades que impliquen interacción con terceros; esto es, no sería relevante, por ejemplo, ver vídeos en *YouTube* sino participar en activamente en las RRSS. Así, entre las distintas conductas *online*, REYNS (2015) encontró relevante el realizar reservas de servicios, participar en RRSS y publicar información personal toda vez que aumentan el riesgo de sufrir *phishing*, *hacking* o ataques con *malware*. Similares conclusiones hallaron los trabajos de PRATT *et al.* (2010) en relación a las compras *online* y el riesgo de ser víctima de estafas; MIRÓ LLINARES (2013) para el acoso; CHOI *et al.* (2017) para acoso sexual; y VAKHITOVA *et al.* (2019) para ciberabuso y *ciberstalking*.

La conducta de la víctima no sólo es relevante por cuanto puede suponer una mayor exposición sino porque puede hacer más atractivos los objetivos. Cuanta más información se comparta, mayor será el riesgo de victimización dada la mayor exposición personal en diversas áreas de su vida. Así, se ha de considerar especialmente el realizar periódicas actualizaciones en las RRSS, subir fotos personales y trasmitir contenido puesto que aumenta el riesgo de ser víctima de *ciberstalking* (REYNS *et al.,* 2011); en el mismo sentido, NGO y PATERNOSTER (2011) para diversos delitos –ataques con virus informáticos, acoso, recibir pornografía no deseada, solicitudes de sexo no deseadas, ataques de *phishing* y difamación–; CHOI *et al.* (2019) sobre los hábitos en RRSS y la victimización por *ciberbullying*; y WHITTY (2019) quien incluye el estudio de variables de la personalidad de las víctimas de ciberfraudes. Es relevante también la audiencia que tiene acceso a dicha información; tener un número elevado de contactos en RRSS, agregar a extraños a la red de contactos y utilizar webs que ofrecen servicios de amistad aumentan el riesgo de victimización para *ciberstalking* (REYNS *et al.,* 2011)[11]. En el mismo sentido, el trabajo de MIRÓ LLINARES (2013) señala que una mayor visibilidad *online* supone un mayor riesgo de victimización, entendiendo por tal el introducir mayor cantidad de objetivos en el espacio virtual y tener un mayor número de interacciones, especialmente con personas desconocidas.

En algunos casos se ha estudiado otra clase de comportamientos de riesgo por parte de las víctimas que, podríamos entender, se acercan a la noción de desviados. Así, realizar conductas de *hacking* aumenta el riesgo de ciberacoso (HOLT y BOSSLER, 2009); hacer o proporcionar copias falsas de *software* u objetos de propiedad intelectual (música, películas y series de televisión), proporcionar acceso ilegítimo a información, introducirse sin permiso en un ordenador ajeno o ver contenido obsceno o pornográfico aumenta el riesgo de sufrir estos delitos (NGO y PATERNOSTER, 2011); y acosar o molestar a alguien, solicitar favores

[11] De modo adicional, sobre la victimización a través de las RRSS, confróntese, en el mismo sentido, YBARRA y MITCHELL (2008); NAVARRO y JASINSKI (2012); y BOSSLER *et al.* (2016).

sexuales sabiendo que no son deseados, hablar repetidamente a alguien de modo agresivo o amenazarlo con causarle daño físico, hackear una cuenta de RRSS, descargar música ilegal y el envío de imágenes sexuales no deseadas aumenta el riesgo de ser víctima de *ciberstalking* (Reyns *et al.*, 2011).

En relación con los guardianes, existen pocos estudios al respecto y los realizados, de modo mayoritario, se centran en los mecanismos físicos de protección; esto es, disponer de medios informáticos tales como programas antivirus, de detección de intrusos, *firewall*, etc. En este sentido, Holt y Bossler (2009) y van Wilsem (2013) encontraron que la instalación estos programas no tiene efectos preventivos para los delitos de ciberacoso y *hacking*, mientras que Choi (2008), en cambio, señala su utilidad. Destaca especialmente el trabajo de Ngo y Paternoster (2011) quienes hallaron que la instalación de estos programas se relacionan del modo significativo con los ataques mediante virus y el acoso pero no lo hacen en la dirección esperada, es decir, para reducir las posibilidades de victimización; en su estudio, quienes disponían de estos medios señalaron que habían sido víctimas de estas conductas en más de un 100% y 70% respectivamente[12]; de modo similar, Hutchings y Hayes (2009) en relación a los ataques *phishing*. Otros trabajos han estudiado la efectividad de las habilidades informáticas de los usuarios o las advertencias de los propios sitios *webs* –tales como alertas de fraude o similar–, sin que encontraran relación significativa en ningún caso (Leukfeldt y Yar, 2016; y Whitty, 2019, respectivamente). En este sentido, el trabajo de Baillon *et al.* (2019) señala que la experiencia en sí no es relevante para reducir el riesgo de recibir ataques de *phishing*, debe estar acompañada de información específica sobre el tema.

3. Objetivos

El objetivo de este trabajo es analizar el comportamiento de los usuarios en las RRSS en aspectos que puedan conllevar una posible victimización. No se trata de un estudio de victimización puesto que lo que se pretende comprobar es, por un lado, si los estilos de vida habituales en RRSS suponen un alto grado de exposición personal y, por otro, si los usuarios adoptan algún tipo de medidas preventivas para paliar dicha exposición[13].

[12] Apuntan los autores que, quizás, este fenómeno se deba a que quienes poseen estos softwares de protección navegan *online* con una falsa sensación de seguridad que los lleva a ser más imprudentes en sus acciones cotidianas. Ngo y Paternoster, 2011, p. 786.

[13] Cabe señalar que actualmente hay publicado un estudio de la autora derivado de las presentes encuestas donde se analizan las medias de autoprotección asociadas a las contraseñas de las cuentas y las victimizaciones por accesos ilícitos en dichas cuentas. Cfr. Solari Merlo, 2021.

En este sentido, se pondrá el foco de atención en tres áreas principales: el tipo de actividad realizada en las RRSS, las medidas adoptadas en relación a la privacidad y los problemas personales percibidos por el uso de las RRSS. La elección de las RRSS a analizar se hizo teniendo en cuenta su popularidad[14] –el número de usuarios–, su carácter genérico –no específico– y el tipo de interacción más habitual entre sus usuarios. Así, las RRSS que se analizarán serán Facebook, Instagram y Twitter[15].

4. Metodología

4.1. Muestra

La encuesta, diseñada específicamente para este trabajo, fue autoadministrada por los participantes a través de internet (técnica CAWI, *Computer Assisted Web Interviewing*)[16] y estuvo abierta a respuestas durante el mes de abril de 2020. Para esto, se consideró adecuado compartir la encuesta entre las propias RRSS analizadas a efectos de llegar directamente a sus usuarios, solicitándoles, a su vez, que la volviesen a compartir en sus propios muros o grupos. En este sentido, se trata de un muestreo no probabilístico.

La plataforma donde se realizaron las encuestas fue *Google Forms* dado su carácter gratuito –esta investigación no cuenta con financiación de ningún tipo–, las diversas posibilidades que ofrece en la formulación de preguntas y la familiaridad –es habitual responder encuestas en esta plataforma por lo que los usuarios serán menos reticentes a la hora de hacerlo, evitando la desconfianza que puede suponer proporcionar información en un sitio desconocido– e facilidad para los partícipes a la hora de responder. El tamaño de la muestra es de 384 individuos[17] que

[14] Para determinar la popularidad de las RRSS se tomaron las estadísticas que analizan estos datos a nivel global (Kemp, 2020) y en España (IAB, 2020).

[15] Cada una de estas tres RRSS funciona de modo similar pero no coincidente. En todas, los usuarios deben registrarse proporcionando ciertos datos personales, un nombre de usuario –en Facebook será el nombre proporcionado en los datos personales– e introduciendo una imagen. Estos dos últimos elementos serán los que identifiquen el perfil –la cuenta– de dicho usuario ante el resto de la comunidad. A continuación, es necesario que los usuarios añadan contactos para poder interactuar introduciendo en las opciones de búsqueda de la red el nombre de otros usuarios y enviándoles la correspondiente solicitud de establecer contacto –amistad, en Facebook– o añadiéndolos cuando la red lo permite –seguimiento o *follower* en Twitter e Instagram. El funcionamiento concreto de cada red es diferente; a lo largo de este trabajo se irán exponiendo las diferencias más destacadas conforme se vaya requiriendo para exponer los resultados obtenidos en las encuestas.

[16] Sobre las ventajas de este método de entrevista, confróntese Vakhitova, 2019, p. 227, quien destaca especialmente la reducción de los errores inducidos por el entrevistador y de la deseabilidad social

[17] Para un nivel de confianza del 95% y un error muestral del 5%, n= $(1{,}96^2*0{,}5*0{,}5) / (0{,}05*0{,}05) = 0{,}9604 / 0{,}0025 = 384{,}16$. Dado que el número de respuestas obtenidas fue

se distribuyen de forma similar entre mujeres (51%, N = 194) y hombres (48%, N = 185)[18].

4.2. Variables y tratamiento de datos

Las encuestas proporcionan información sobre 28 variables, de las cuales 27 son categóricas (C) y 1 numérica (N).

4.2.1. Actividades en RRSS

Las siguientes variables recogidas en la Tabla 1 fueron realizadas con el objetivo de determinar la visibilidad del comportamiento habitual de los usuarios.

Con base a la información de la V8, se procedió a configurar la V9 clasificando las opciones proporcionadas de respuesta en 3 grupos en función del tipo de información proporcionada y su incidencia en la privacidad y/o intimidad de los sujetos. Así, de menor a mayor exposición personal, se constituye un primer grupo (GI 1 –grupo de información 1–) con la *información básica necesaria para crear la cuenta*, el *nombre y apellido*, la *ciudad de residencia* y el *estado civil o situación sentimental*. Un segundo grupo (GI 2) que incide más en la privacidad o intimidad de los sujetos es el relativo al lugar de estudio o trabajo, la *orientación sexual* y los *lugares de ocio frecuentados*, ya que se trata de información especialmente protegida y/o que permite localizar físicamente a los sujetos. Y, finalmente, la información sobre el *barrio o calle donde viven* o la *información sobre los hijos* entendemos que constituirían un tercer grupo (GI 3) donde el nivel de exposición pública –y, por consiguiente, posible vulnerabilidad– es mayor.

Los sujetos que señalaron proporcionar información exclusivamente sobre una de las variables del GI 1, se los asignó a este grupo; entre los restantes, si señalaron una opción del GI 1 y al menos una del GI 2, fueron asignados al GI 2; y quienes señalaron al menos una variable del GI 2 y otra del GI 3, fueron asignados al GI 3; fuera de esta clasificación quedan tres personas que afirmaron no compartir ningún tipo de información (GI 0).

mayor, se procedió, por orden de respuesta, a comprobar que las encuestas se habían completado de modo adecuado, eliminando aquellas que no cumplían esta condición y tomando una nueva, también por orden de respuestas, entre las disponibles.

[18] 5 sujetos prefirieron no revelar su sexo.

Tabla 1. Variables relativas a las actividades rutinarias[19]

Variable	Tipo	Respuesta
Uso de RRSS		
RRSS utilizadas *(Facebook, Instagram, Twitter, Otros)*	V1, C	Múltiples respuestas
Antigüedad en cada RRSS *(Menos de 3 años, de 3 a 6 años, de 7 a 10 años, Más de 10 años)*	V2, C	Una respuesta por red social
Conexión desde *app (Sí, No)*	V3, C	Dicotómica
Antigüedad máxima en RRSS[20] *(Menos de 3 años, De 3 a 6 años, De 7 a 10 años, Más de 10 años)*	V4, C	Configurada
Multiplicidad de RRSS[21] *(1, 2, 3, Más de 3)*	V5, C	Configurada
Actividad en RRSS		
Tiempo pasado en RRSS *(Más de una hora al día, Menos de una hora al día, Más de 4 días a la semana, Menos de 4 días a la semana, Algunos días al mes, Nunca o casi nunca)*	V6, C	Una respuesta por red social
Tipo de actividad realizada *(Interactuar con terceros* –dar "*like*", comentar publicaciones de otros, etc.-, *Publicar fotos, Publicar contenido de otro tipo)*	V7, C	Una respuesta por actividad
Información personal compartida *(Información básica necesaria para crear la cuenta, Nombre y apellido, Ciudad de residencia, Estado civil, Situación sentimental, Orientación sexual, Lugares de ocio frecuentados, Barrio o calle de residencia, Información sobre los hijos)*	V8, C	Múltiples respuestas
Grupos de información *(0, 1, 2, 3)*	V9, C	Configurada

[19] Elaboración propia.

[20] Con la información relativa a la antigüedad en cada red social, se creó la variable de antigüedad máxima en RRSS, tomando la fecha más antigua proporcionada para alguna de las 3.

[21] Con los datos de la V1 se configuró la variable relativa al uso de múltiples RRSS.

4.2.2. Guardianes: protección de la privacidad

Las siguientes variables se realizaron para conocer la autoprotección de la privacidad de los usuarios.

Tabla 2. Variables relativas a los guardianes[22]

Variable	Tipo	Respuesta
Número de contactos *(menos de 100, 101-200, 201-300, 301-400, 401-500* y *más de 500)*	V10, C	Una respuesta por red social
Percepción de control de privacidad *(Sí, No)*	V11, C	Dicotómica
Configuración de la privacidad[23] *(Configuro la privacidad según la publicación, Personas concretas que yo decido, Todos mis amigos/ seguidores, Amigos y amigos de amigos, Cualquiera, aunque no sea mi amigo o seguidor)*	V12, C	Una respuesta por red social
Bloqueos *(No; Sí, porque he tenido un problema o discusión con esa persona; Sí, porque me siento acosado o vigilado por esa persona; Sí, no he tenido ningún problema concreto, pero no quiero que sepa nada de mí)*	V13, C	Múltiples respuestas

4.2.3. Consecuencias negativas experimentadas

En la sección relativa a las consecuencias negativas se trataron las siguientes cuestiones a efectos de conocer si el uso de las RRSS podía

[22] Elaboración propia.

[23] La configuración funciona de modo distinto en cada red social. Las opciones más básicas –Instagram y Twitter– suponen elegir entre tener una cuenta pública, donde cualquiera puede ver las publicaciones, o privada, donde sólo aquellos que siguen al titular de la cuenta pueden verlas; en dichas RRSS, al crear una cuenta, la configuración por defecto es la de cuenta pública. El sistema de Facebook, en cambio, establece diversos filtros de privacidad y, en atención a esa especificidad, este fue el modelo que se siguió en el diseño de la encuesta, ofreciendo opciones de respuesta similares. Esto supone que, al optar por ofrecer unas mismas respuestas para todas las RRSS –para simplificar la labor de los encuestados–, diversas opciones no serán válidas, *a priori*, para usuarios de Instagram y Twitter. La interpretación de estos datos, no obstante, salvará este inconveniente puesto que las respuestas ofrecidas pueden, a la postre, simplificarse en cuenta privada o cuenta pública. Para realizar este análisis en Instagram y Twitter, se han recodificado las variables atendiendo a que en dichas RRSS, las cuentas y las publicaciones únicamente pueden ser públicas o privadas. Así, quienes señalaron que cualquiera, aunque no sea amigo o seguidor, puede ver las publicaciones fueron incluidos en el grupo de cuenta pública; los restantes, en el grupo de cuenta privada –con excepción de quienes señalaron no saber dicha información, que se mantuvieron en el GP 0.

resultar negativo para los usuarios y, en ese caso, si las consecuencias se limitaban a la actividad *online* o trascendían a los aspectos no virtuales de la vida de los sujetos.

Tabla 3. Variables relativas a las consecuencias negativas[24]

Variable	Tipo	Respuesta
Problemas tras realizar publicación *(No; Sí, con mis padres; Sí, con mi pareja; Sí, con mis amigos; Sí, en el trabajo; Sí, otros)*	V14, C	Múltiples respuestas
Persona con la que se ha tenido problemas *(Padres, Pareja, Amigos, Trabajo, Otros)*	V15, C	Configurada
Agravios recibidos por parte de otros usuarios *(Sí, No)*	V16, C	Dicotómica
Red social de los agravios *(Facebook, Instagram, Twitter)*	V17, C	Una respuesta por red social
Frecuencia de agravios *(1 o 2 veces, 3 a 10 veces, M*ás de 10 veces*)*	V18, C	Múltiples respuestas
Modo de producirse los agravios *(Muro propio, Muro de quien agravia, Muro de un tercero o grupo, Mensaje privado* –MP-*)*	V19, C	Múltiples respuestas
Conocimiento del usuario que agravia *(No; Sí, de las RRSS; Sí, de fuera de las RRSS)*	V20, C	Múltiples respuestas
Denuncia de hechos ante las autoridades de la red social *(No; Sí, denuncia de 1 o más personas; Sí, denuncia de 1 o más grupos)*	V21, C	Múltiples respuestas
Red social de denuncia de hechos y motivos	V22, C	Respuesta abierta
Denuncia de hechos ante las autoridades de la policía *(Sí, No)*	V23, C	Dicotómica
Red social donde tuvieron lugar los hechos y motivos	V24, C	Respuesta abierta

4.2.4 Variables de control y análisis de datos

Como variable de control se introdujo el sexo (V25, C), la edad (V26, N) y el nivel de estudios máximo alcanzado (V27, C). La variable relativa

[24] Elaboración propia.

a la edad fue categorizada posteriormente (V28, C) para facilitar el cruce con otras variables.

Una vez depurados los datos, se procedió a su tratamiento con el programa estadístico *Statgraphics Centurion* versión 17.2.07. En el cruce de variables, algunas fueron consideradas ordinales; así, V2, relativa a la antigüedad (valor mín. para la menor antigüedad), V4, relativa a la multiplicidad de redes (valor mín. para el menor número de RRSS usado), V6, relativa al tiempo pasado en las RRSS (valor mín. para conexiones esporádicas e incrementándose conforme se intensifica su uso), V9, relativa al tipo de información personal compartida –grupos de información– (valor mín. para quienes menos información comparten), V10, relativa al número de contactos (valor mín. para quienes menos contactos tienen), V18, relativa a las veces que se recibieron insultos o agravios en RRSS (valor mínimo para la menor frecuencia), y V28 relativa a los intervalos de edad (valor mín. para la menor edad). Una vez creadas estas variables y recodificados los datos, se ejecutó el análisis estadístico.

5. Principales resultados

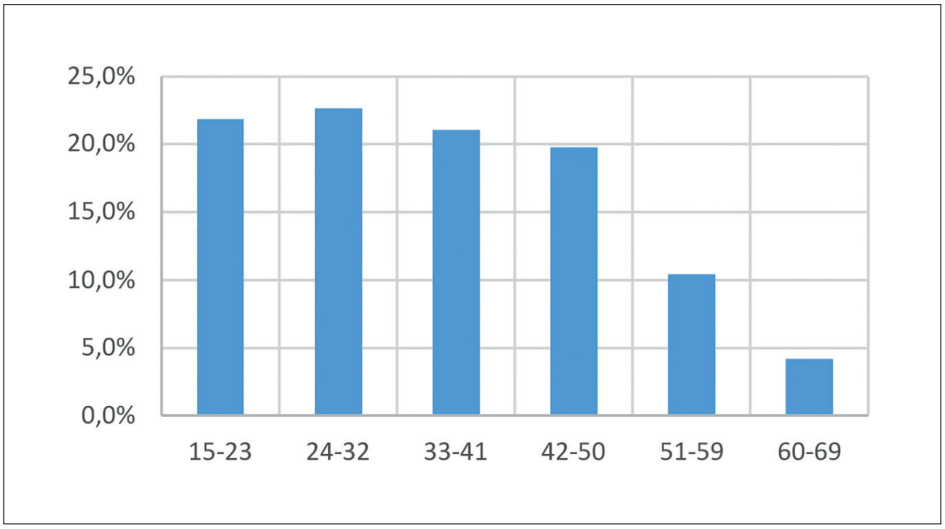
5.1. Características comunes

Los usuarios de RRSS estudiados (51% mujeres y 48% hombres) tienen mayoritariamente una edad comprendida entre los 24 y 45 años, con una mayor representación para el intervalo de edad comprendido entre los 24 y 32 años y una edad media de 36 años. El 59,6% (N = 229) cuenta con titulación universitaria, el 29,4% (N = 113) tiene un nivel preuniversitario y un 9,4% (N = 36) cuenta con doctorado[25] (Gráfica 1).

Es difícil comparar estos datos a nivel global puesto que no existe una institución que mida las variables aquí analizadas. Como aproximación, podemos señalar que según el último estudio de IAB (2020) las características de esta población en España son el ser principalmente mujeres (51%), con una edad media de 40 años, con mayor representación para el intervalo de edad comprendido entre los 25 y 54 años (y especialmente entre los 41 y 54), y mayoritariamente titulados universitarios (48%), seguidos de preuniversitarios (36%). Como puede comprobarse, aunque estos dos últimos valores se asemejan, el presente trabajo presenta una representación mayor de personas jóvenes y tituladas de lo que respecta al total de la población –a su aproximación en España.

[25] Un 1,6%, N = 6, no respondieron a esta pregunta.

Gráfica 1. Edad de la muestra. Intervalos[26]



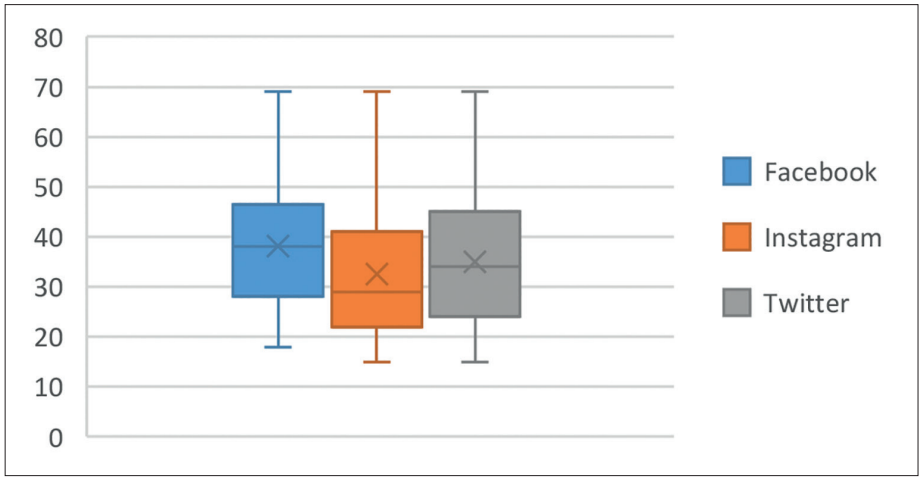
Como se puede ver en las Gráficas 2 y 3, cada red social presenta perfiles distintos[27] en lo que respecta a los intervalos de edad. Así, en Facebook, la media de edad se sitúa en los 38,2 años (DE = 11,9; Mo = 25; Mín. = 18; Máx. = 69), con una mayor representación para las edades comprendidas entre los 28 a 46 años (cuartil inferior y superior). En Instagram, hallamos un marco de edad inferior, con una media en los 32,5 años (DE = 11,9; Mo = 22; Mín. = 15; Máx. = 69) y una mayor representación para las edades de 22 a 41 años. Twitter, por su parte, se sitúa en un punto intermedio, con una edad media de 35 años (DE = 12,8; Mo = 20; Mín. = 15; Máx. = 69) y un intervalo de edad más habitual entre los 24 y 45 años.

Estos resultados fueron comparados con el test ANOVA encontrando diferencias en términos estadísticamente significativos –si bien con un efecto pequeño– $F_{(2;\ 845)} = 14{,}11$; $p < 0{,}001$; $\eta^2 = 0{,}03$. Estas diferencias se dan en todos los grupos (test Tukey).

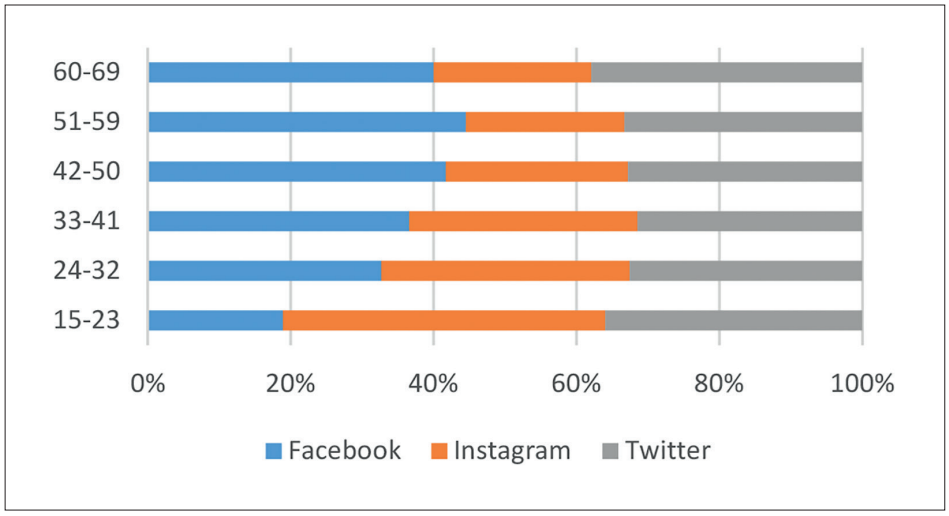
[26] Elaboración propia.

[27] En este caso, el test ANOVA fue corregido con el estadístico F de Welch, dado que no se cumplía con el supuesto de homocedasticidad o igualdad de las varianzas, encontrando diferencias en términos estadísticamente significativos –si bien con un efecto medio– $F_{(5;\ 376{,}13)} = 9{,}2154$; $p < 0{,}001$; $\eta^2 = 0{,}05$. Estas diferencias se dan en todos los grupos (test Games-Howell).

Gráfica 2. Perfil de edad por RRSS[28]



Gráfica 3. Perfil de edad por RRSS. Intervalos[29]

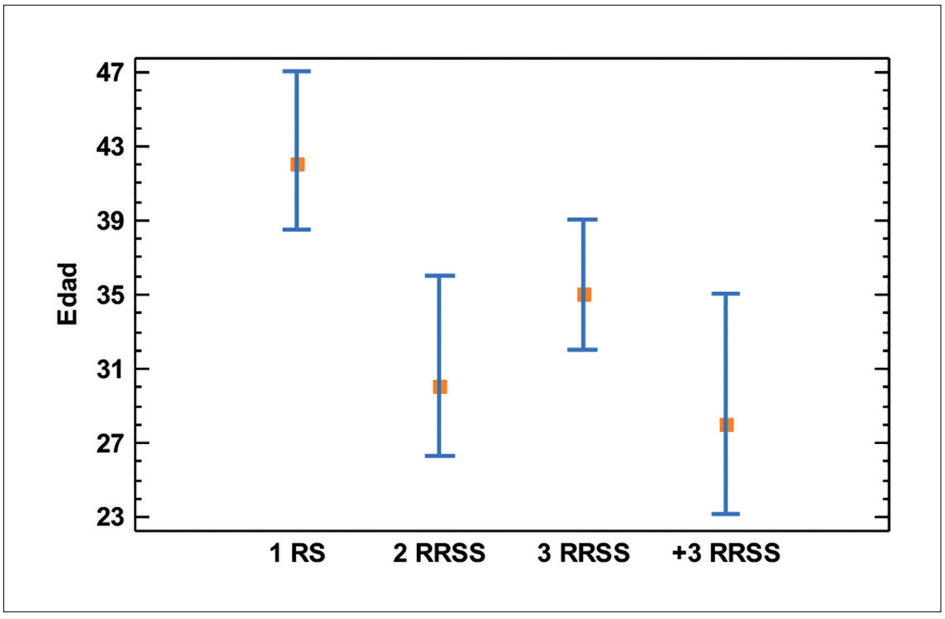


En cuanto a las RRSS utilizadas, los usuarios totales de cada red social son 257 en Facebook, 259 en Instagram y 332 en Twitter. Ahora bien, dado que los encuestados señalaron múltiples respuestas, fue posible extraer información sobre el uso simultáneo de diversas RRSS, esto

[28] Elaboración propia.
[29] Elaboración propia.

es, multiplicidad de RRSS. En este sentido, un 19,5% que afirmó utilizar sólo una, un 34,4% utiliza 2, el 39,6% usa 3, y el 6,5% (N = 25) utiliza más de 3. Esta variable fue examinada con mayor detenimiento analizando su posible relación con la variable de la edad de los sujetos. Tras realizar el test ANOVA con la corrección de Welch, se observó un efecto significativo medio $F_{(3; 380)} = 7,93$; $p = 0,0001$; $\eta^2 = 0,06$. Estas diferencias se dan entre quienes tienen 1 RS y cada uno de los restantes grupos, pero no entre estos grupos entre sí (test Tukey).

Gráfica 4. Multiplicidad de RRSS y edad de usuarios[30]

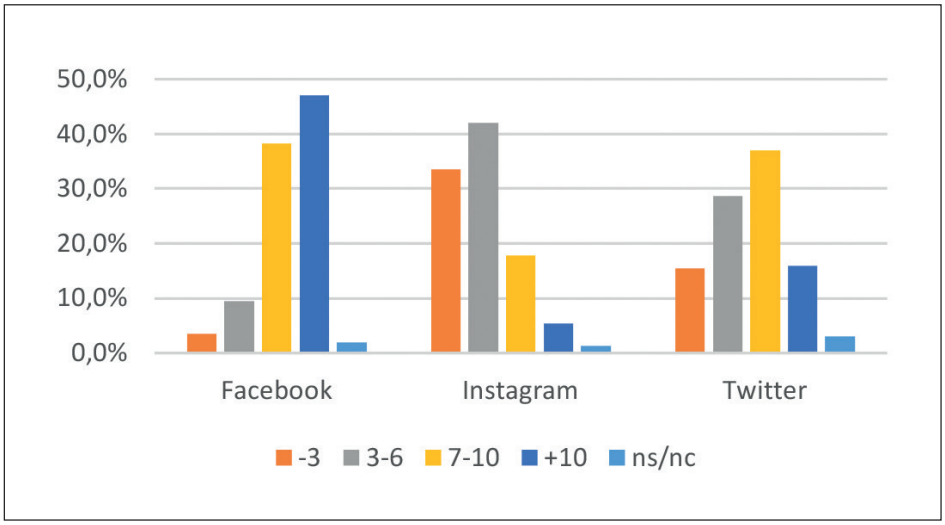


En cuanto a la antigüedad de la cuenta[31], puede observarse cierta correspondencia entre la antigüedad señalada por los usuarios y la de las propias RRSS. Así, Facebook es la red social más antigua –fundada en 2004–, seguida por Twitter -2006– e Instagram -2010–, por lo que resulta coherente encontrar una mayor representación de cuentas antiguas en la primera y de cuentas más recientes en las últimas.

[30] Elaboración propia.

[31] Cabe destacar, existe una discrepancia respecto a la cifra de usuarios de cada red social según la respuesta señalada anteriormente (V1). Así, mientras que los sujetos que afirmaron poseer cuenta fueron 257 en Facebook, 259 en Instagram y 332 en Twitter, respondieron a la presente pregunta, respectivamente, 319, 298 y 363 personas. Esto se debe a que la anterior pregunta se refería a las redes usadas en la actualidad y en esta se pregunta por la antigüedad de la primera cuenta, que puede ser que no se siga utilizando actualmente.

Gráfica 5. Antigüedad en las RRSS[32]



5.1.1. Actividad en RRSS

El módulo de la actividad en las RRSS está centrado en comprobar aspectos que inciden en la visibilidad de los sujetos que, como se verá en el próximo módulo, guardan relación con su privacidad. En este sentido, los usuarios que han respondido a la encuesta suelen hacer un uso intensivo de las RRSS, con conexiones diarias (73%) durante varias horas al día (68,5% del total de conexiones diarias). Estas conexiones se realizan frecuentemente desde el móvil (70,5% de usuarios de Facebook, 88,9% de Instagram y 88,4% de Twitter) y, en este sentido, cabe destacar que se observa una diferencia significativa puesto que los usuarios que no cuentan con la *app* en el móvil pasan menos horas en las RRSS[33]. Prácticamente en todas las conexiones los usuarios interactúan –es decir, tienen una participación activa, no son meros espectadores–, lo cual va en consonancia con la finalidad de las RRSS. La publicación de fotos, no obstante, es la actividad menos realizada.

Destaca especialmente el tipo de información compartida por los usuarios en sus diferentes interacciones puesto que, como señalábamos anteriormente, supone la introducción de bienes valiosos en el espacio virtual.

[32] Elaboración propia.

[33] Cabe destacar que, a efectos de facilitar el manejo estadístico y visionado de datos, se agruparon las categorías de la variable 6 relativa al tiempo pasado en la red social en *diario* (sin distinguir el número de horas al día), *semanal* (sin distinguir el número de días a la semana), *mensual* (algunos días al mes) y *esporádico* (nunca o casi nunca).

Tabla 4. Información que los usuarios comparten en RRSS[34]

	Mujeres		Hombres		Total	
	f	*%*	*f*	*%*	*f*[35]	% del total de respuestas
La ciudad donde vivo	145	*50,9*	137	*48,1*	285	*21,1*
Nombre y apellido	127	*54,5*	102	*43,8*	233	*17,2*
Estado civil o situación sentimental	98	*55,1*	78	*43,8*	178	*13,2*
Información básica	86	*50,0*	82	*47,7*	172	*12,7*
Lugar donde estudio o trabajo	90	*52,6*	77	*45,0*	171	*12,7*
Orientación sexual	62	*54,9*	51	*45,1*	113	*8,4*
Lugares de ocio frecuentados	53	*54,6*	42	*43,3*	97	*7,2*
Barrio o calle donde vivo	21	*43,8*	26	*54,2*	48	*3,6*
Conocimiento sobre hijos	12	*46,2*	14	*53,8*	26	*1,9*
Otros	6	*24,0*	19	*76,0*	25	*1,9*
Nada[36]	1	*33,3*	2	*66,7*	3	*0,2*

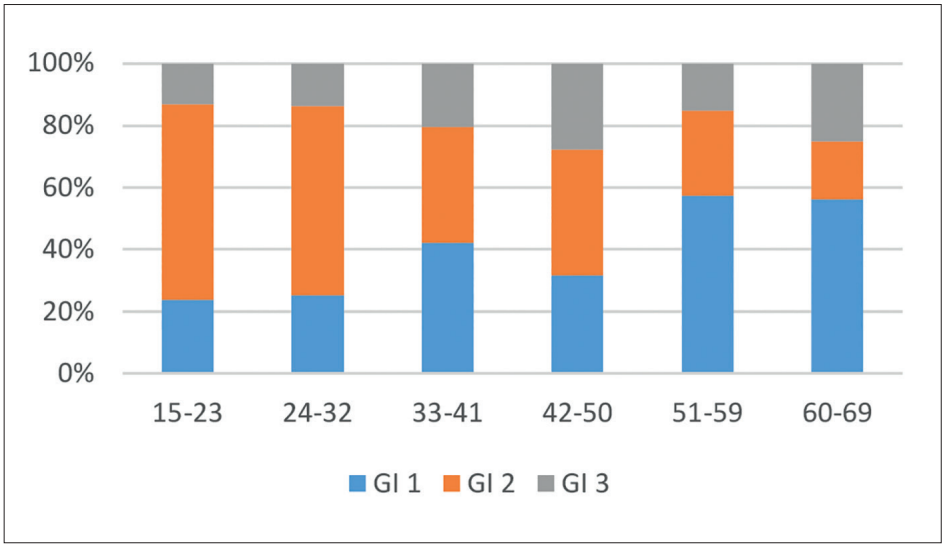
Así, la opción más señalada (46,9%) es la que ha sido clasificada como pertenencia al GI 2; esto es, usuarios que, al menos, han publicado datos sobre su orientación sexual o lugar de estudio, trabajo u ocio frecuentes –es decir, una localización física habitual. El GI 3 –usuarios que, junto a las anteriores, comparten información sobre su domicilio o datos de sus hijos– tiene la representación más reducida pero que, en cualquier caso, alcanza el 18,2% de la muestra. El cruce de variables no arroja valores significativos a nivel estadístico para ninguna de las analizadas. No obstante, cabe hacer algunas apreciaciones. Así, según la antigüedad en las RRSS, el grupo que tiene una proporción más alta entre los que menos información comparten –aquí, GI 1–, es el de los más novatos en las RRSS, con una antigüedad inferior a los 3 años, que ofrece un porcentaje

[34] Elaboración propia.
[35] Incluye encuestados que no revelaron su sexo.
[36] Cabe destacar que quienes señalaron la opción "nada", no marcaron ninguna otra, ni siquiera la relativa a información básica para la creación de la cuenta, lo que bien puede interpretarse como una percepción subjetiva de que se tiene un nivel máximo de privacidad, bien como que todos los datos proporcionados para la creación de la cuenta son falsos por lo que, efectivamente, sus contactos no conocen nada sobre estas personas.

del 40,6% para el total de su grupo[37], por lo que se sitúa por encima de la media del GI 1 situada en 34,1%. Las personas con la máxima antigüedad considerada tienen una proporción baja de pertenencia al GI 3 –los que más información comparten– que se sitúa en el 10,3%, por debajo de la media del total de la muestra situado en 18,2%.

Los usuarios más jóvenes pertenecen en mayor medida al GI 2; conforme aumenta la edad, esta representación disminuye y se incrementa la pertenencia al GI 1 –quienes menos información comparten. Asimismo, quienes utilizan sólo una red social suelen compartir menos información (47,2% para el GI 1 y 12,5% para el GI 3).

Gráfica 6. Grupos según tipo de información compartida e intervalos de edad[38]



En este sentido, podemos señalar que los usuarios de RRSS tienen una exposición personal elevada, tanto por el uso de múltiples RRSS, como por el tiempo pasado en la red social, por su participación activa en la misma y, de modo especial, por el tipo de información personal compartida con su audiencia.

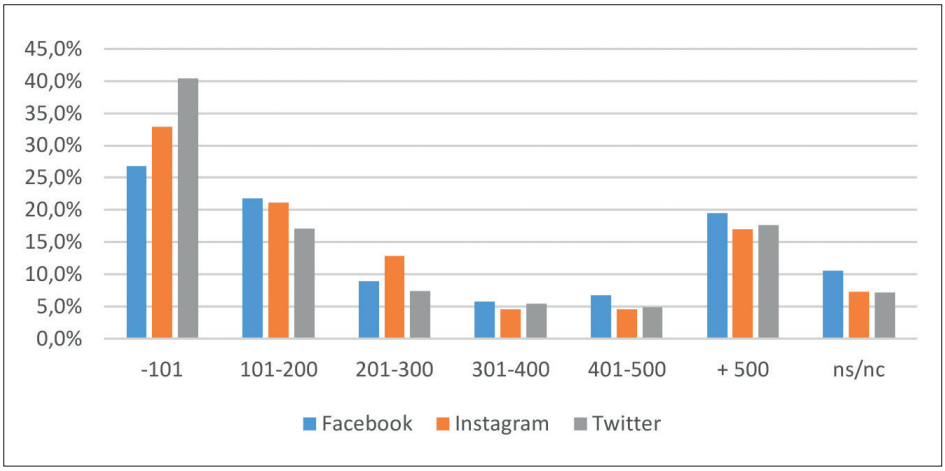
[37] Cabe destacar que entre las personas que tienen esta antigüedad se igualan los porcentajes para el GI 1 y GI 2, 40,6% en cada caso.

[38] Elaboración propia.

5.1.2. Protección de la privacidad

Al margen de las diferenciaciones que se establecerán en cada red social, podemos observar que el número de contactos en RRSS nos remite a dos tipos de usuarios: uno con una cifra relativamente reducida –hasta 100, principalmente, o hasta 200– y otro con una elevada cifra que supera los 500. Las categorías intermedias tienen una menor representación.

Gráfica 7. Número de contactos según RRSS[39]



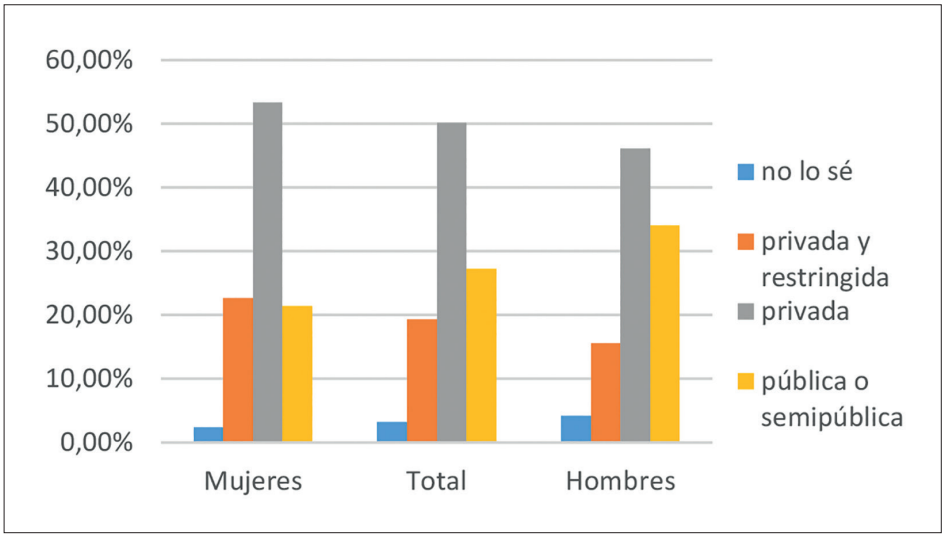
En el cruce de variables destaca especialmente la relación entre el número de contactos y el tipo de información compartida. Así, quienes menos información comparten –GI 1– tienen de modo mayoritario pocos contactos (hasta 100). A partir de los 200 contactos, se incrementa la pertenencia al GI 2 y, en menor medida, al GI 3. Esto es, esa alta exposición personal señalada anteriormente se da con mayor frecuencia con una audiencia que, al menos, está en torno a los 200 contactos, existiendo un grupo significativo cuyos contactos superan los 500 usuarios.

Asimismo, los usuarios señalan mayoritariamente ser conscientes de la configuración de privacidad de sus RRSS (83,9%) y, ante las diferentes medidas a adoptar se puede ver que, también de modo mayoritario, prefieren no alterar la configuración que establece cada red social por defecto. Entre quienes realizan modificaciones en esta configuración, se observa que las mujeres tienen una tenencia a incrementar la privacidad –restringiendo la audiencia que puede ver sus publicaciones–, mientras que los hombres presentan la tendencia opuesta, a

[39] Elaboración propia.

incrementar la exposición [$X^2_{(2)}$ = 7,122; p = 0,0284][40]. En este sentido, podemos entender que se ejerce un mayor grado de autoprotección –autoguardián, según se denominaba anteriormente– entre las mujeres.

Gráfica 8. Configuración de privacidad de la cuenta y sexo[41]



En relación con los bloqueos –cabe recordar que se trata de una medida de autoprotección de la privacidad drástica respecto a un usuario concreto–, el 75,5% de los encuestados señaló haber bloqueado a otro usuario. Resulta significativa la relación entre esta variable y la relativa al sexo [$X^2_{(3)}$ = 16,264; p = 0,0010][42], siendo la causa más habitual del bloqueo el preservar la privacidad, es decir, sin que esté motivado en un hecho concreto pero, mientras que para las mujeres esta opción supone el 52,9% del total de respuestas, para los hombres este porcentaje se reduce al 38%, teniendo similar representación el haber tenido un problema o discusión con esa persona (37,5%). Sentirse acosado o vigilado por el otro usuario tienen para ambos la menor representación, en torno al 15%. Cabe apuntar así que, si bien todos los usuarios utilizan en gran medida esta forma de autoprotección, las mujeres parecen tener una mayor precaución al respecto, estableciendo esta medida con anterioridad al surgimiento de un problema, esto es, con carácter preventivo.

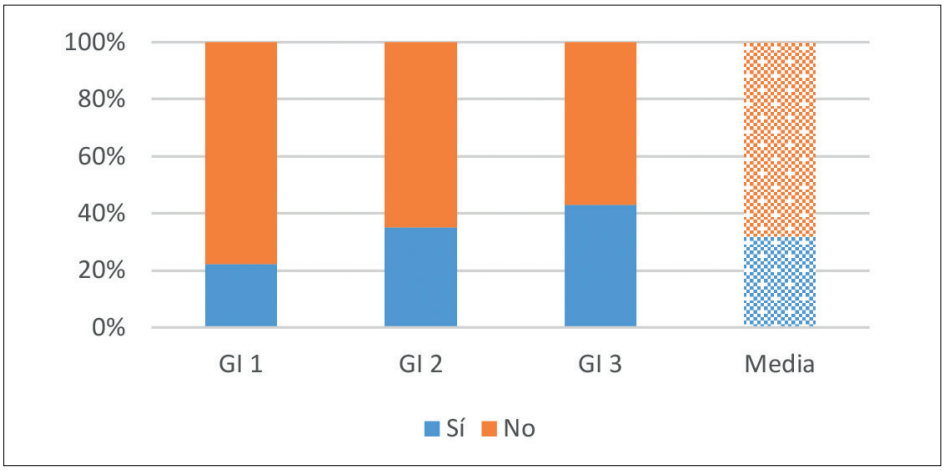
[40] Para la variable "sexo", se ha excluido a quienes no señalaron ninguno y para la variable "configuración de la privacidad" a aquellos que dijeron no saber este dato.
[41] Elaboración propia.
[42] Para la variable "sexo", se ha excluido a quienes no señalaron ninguno.

Quienes adoptan en mayor medida esta acción preventiva [$X^2_{(3)}$ = 11,339; p = 0,0010] son los usuarios que más RRSS utilizan (con más de 3 RRSS, el porcentaje de bloqueos asciende al 92% y, con 1 red social, disminuye hasta el 64%), las personas más jóvenes (hasta 32 años) y los usuarios con una antigüedad media de 3 a 10 años.

5.1.3. Consecuencias negativas experimentadas

Un 31,8% de los sujetos señaló haber tenido problemas tras realizar alguna publicación, destacando especialmente quienes más RRSS utilizan (los porcentajes se incrementan conforme lo hace el número de RRSS utilizadas con una significación estadísticamente relevante [$X^2_{(3)}$ = 23,509; p < 0,0001]), quienes más información comparten (conforme se incrementa la información compartida, mayor número de problemas se ha señalado tener [$X^2_{(2)}$ = 10,389; p = 0,0055]), los más veteranos en el uso de las RRSS (más de 10 años), y de una edad comprendida entre los 33 y 59 años; en sentido contrario, los usuarios que no han realizado bloqueos y los que tiene poca antigüedad en RRSS (hasta 3 años) señalan en mayor medida no haber tenido problemas en este sentido.

Gráfica 9. Problemas en RRSS según grupos de información compartida[43]



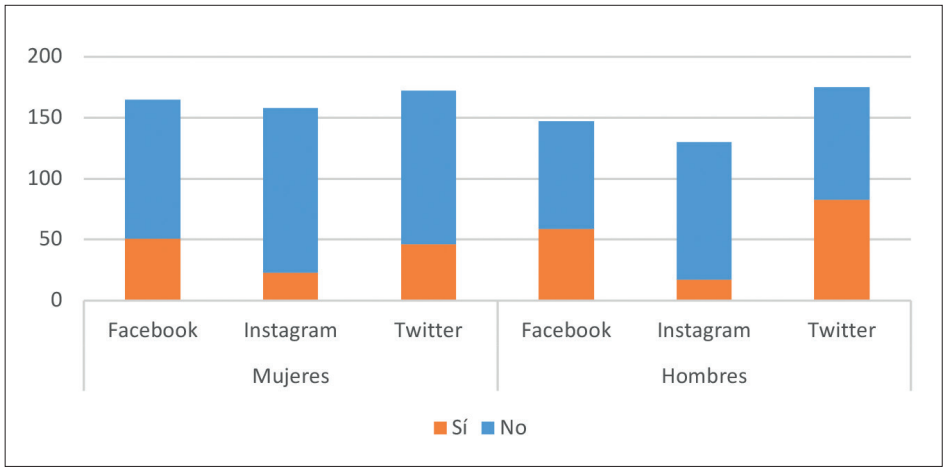
En la distinción por sexos se observan diferencias significativas en relación a la persona con la que han tenido problemas [$X^2_{(4)}$ = 11,295; p = 0,0234]; así, mientras que las mujeres han tenido problemas principalmente

[43] Elaboración propia.

con su pareja (opción de respuesta del 32,5%, frente al 16,7% para hombres) y los hombres los han tenido con amigos (43,1%, frente al 31,3% para mujeres). Entre quienes tuvieron problemas con otros, lo más habitual fue tenerlos con desconocidos.

La mayoría de los usuarios (51%) señaló haber sufrido insultos o faltas de respeto en las RRSS una vez, observando diferencias significativas [$X_{y\ (1)}^2$ = 5,888; p = 0,0152] entre hombres (57,8%) y mujeres (44,9%). En este sentido, destacan especialmente los usuarios de múltiples RRSS [$X^2_{(3)}$ = 12,106; p = 0,0070] –al igual que en la variable relativa a los problemas, conforme aumenta el número de RRSS, se incrementan las respuestas afirmativas al haber recibido insultos–, quienes más información comparten [$X^2_{(2)}$ = 8,625; p = 0,0134] –GI 3, un 16% de respuestas afirmativas por encima de la media–, y, en sentido opuesto, quienes no bloquean [$X_{y\ (1)}^2$ = 27,807; p < 0,0001] que, mayoritariamente (72,5%), afirman no haber sido víctimas de agravios. En la distinción por RRSS, destaca Twitter con un porcentaje más alto de respuestas afirmativas (37,4%, N = 131), seguido de Facebook (35%, N = 111); en Instagram el valor es de 13,8% [$X^2_{(2)}$ = 50,005; p < 0,0001].

Gráfica 10. Agravios recibidos en RRSS según sexo[44]



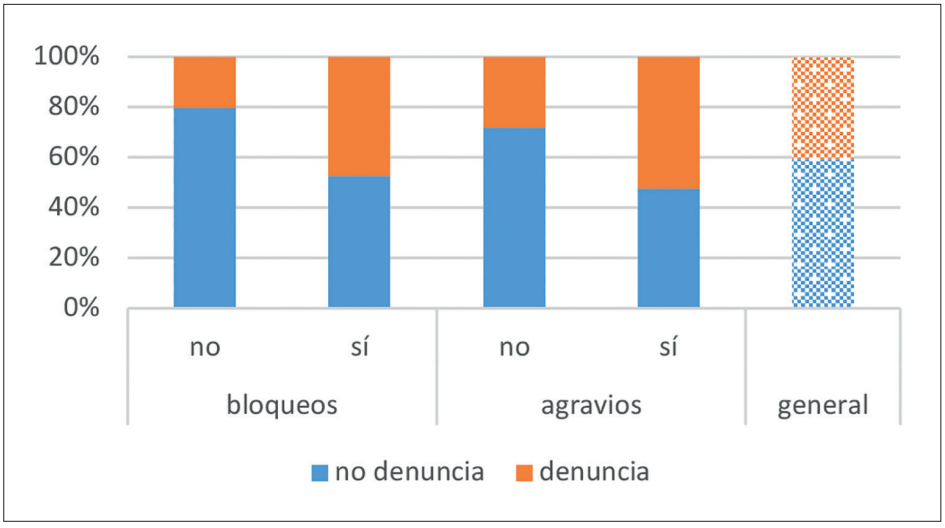
Entre las mujeres lo habitual es que conocieran al usuario que las insultó (55,3%), mientras que entre los hombres lo habitual es que no lo hicieran (61,7%). Cuando se conoce al otro usuario, las mujeres lo hacen principalmente fuera de las RRSS y los hombres tienen el contacto únicamente en el espacio virtual, sin que trascienda la relación al espacio físico. Aunque esta información no nos remite, en principio, a

[44] Elaboración propia.

un entorno delictivo –con estos datos no es posible hablar de delitos de injurias o similar–, podemos afirmar que se trata de hechos vividos como conflictivos, ofensivos, y que han sido experimentados por la mayoría de los usuarios. Resulta estadísticamente significativo [$X_y^2{}_{(1)} = 6{,}748$; $p = 0{,}0094$] que, en el caso de las mujeres, el usuario agresor es principalmente alguien conocido fuera de las RRSS, esto es, en el espacio no virtual, mientras que para los hombres los agresores son principalmente desconocidos o personas conocidas únicamente de las RRSS.

Por otra parte, los usuarios no suelen denunciar hechos ante las RRSS (59,4%); entre los que lo hacen, destacan especialmente los que han realizado bloqueos –quienes no bloquean tienen unos valores más altos hacia la no denuncia (79,6%) y quienes bloquean, unos más elevados en la denuncia (47,6%) [$X_y^2{}_{(1)} = 21{,}185$; $p < 0{,}0001$]- y quienes sufrieron insultos o faltas de respeto (52,6%); en este último caso [$X_y^2{}_{(1)} = 22{,}607$; $p < 0{,}0001$] el valor de denuncia se vuelve la opción mayoritaria (52,6%) y, en el caso de no haberlos sufrido, el valor de no denuncia se incrementa hasta el 71,8%, sin que sea posible afirmar que los hechos guarden relación entre sí. Podemos apuntar, no obstante, que quienes toman más precauciones o han vivido situaciones conflictivas, recurren a los medios de protección de la propias RRSSS con mayor frecuencia.

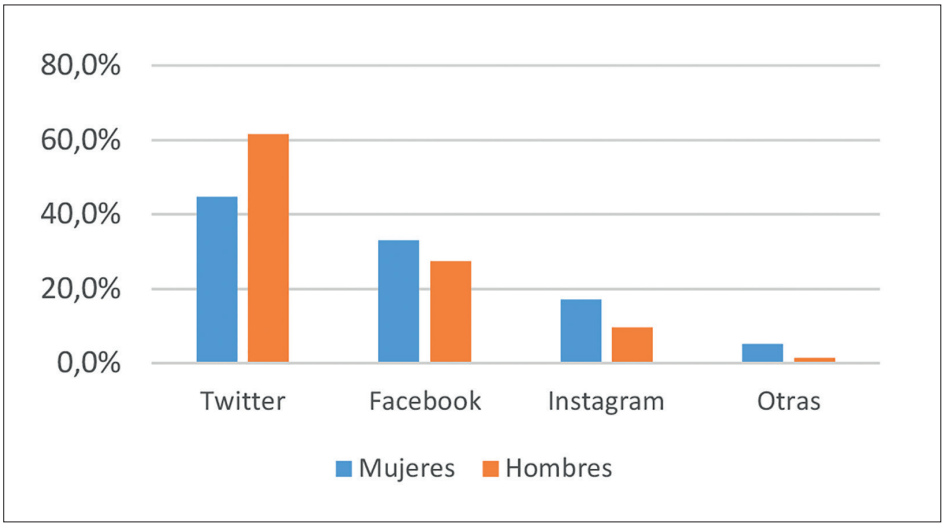
Gráfica 11. Denuncias, bloqueos y agravios recibidos[45]



[45] Elaboración propia.

Mayoritariamente, las denuncias tienen lugar en una sola red social (64,1%) y, entre las distintas RRSS, principalmente se denuncia en Twitter (53%), seguido de Facebook (30,2%) e Instagram (13,4%)[46].

Gráfica 12. Denuncias según RRSS y sexo[47]



Así, los motivos de las denuncias son variados y se diferencian según sexo. En el caso de las mujeres, encontramos entre las principales causas el contenido relacionado con odio -40,6%-, (entre otros, relacionados con machismo, género, maltrato, misoginia, racismo, xenofobia y LGTB), inapropiado (no se describe su contenido) -9,9%-, e información falsa o *fake news* y otros (sin especificar) con un 7,9% cada uno. Entre los hombres, los motivos más frecuentes son el contenido de odio (27%), información falsa o *fake news* (13,5%), insultos (12,6%), y acoso (8,1%).

Un dato destacable en el que no ha sido posible profundizar es que, de modo espontáneo, diversos encuestados señalaron no ser víctimas de los hechos denunciados, sino que, ante agravios, insultos o discriminación a terceros, denunciaron los hechos ante la red social. Esto podría ser indicativo de la presencia de un elemento protector que opera como guardián informal en el ámbito de las RRSS. Su estudio, no obstante, requiere una mayor profundización.

[46] Se excluyen del cálculo quienes señalaron haber denunciado pero no respondieron a esta pregunta.
[47] Elaboración propia.

Finalmente, cabe destacar que existe un porcentaje muy bajo denuncia hechos ante la policía (8,3%, 53,1% de los cuales son mujeres, 40,6% hombres y 6,3 de sexo indeterminado). Las principales causas de denuncia entre las mujeres son las amenazas (27,8%), el contenido pedófilo (22,2%), y las injurias y contenido de odio (11,1% en cada caso). Entre los hombres, las principales causas son el acoso (37,5%) y contenido pedófilo (25%). Entendemos, no obstante, que la baja proporción de denuncias ante la policía no permite hacer generalizaciones respecto a esta información.

5.2. Facebook

Los usuarios de Facebook son mayoritariamente mujeres (52,5%, frente al 45,5% de hombres) con una edad principalmente comprendida entre los 33 y 41 años; las mujeres, no obstante, tienen una edad media de 36,5 años mientras que en los hombres supera los 40 años.

En relación con las *actividades cotidianas*, cabe destacar, respecto a la tendencia general expuesta anteriormente, que los usuarios de esta red social se conectan con menor frecuencia a la red, aumentando especialmente los valores de conexiones esporádicas (nunca o casi nunca) del 13,4% –media de RRSS– al 22,9%. En congruencia con estos datos, los usuarios de Facebook son quienes menos conexiones realizan a través de la *app* del móvil. En este apartado destaca también que es en Facebook donde encontramos las cuentas más antiguas, con una respuesta mayoritaria para una antigüedad superior a 10 años.

En relación con la *protección de la privacidad*, se observa una tendencia general a no alterar la configuración básica de la red social, esto es, que las publicaciones sean vistas por todos los contactos (57,1% de mujeres y 47,0% de hombres). Cuando se altera, las mujeres tienden a aumentar la privacidad (22,6% para cuentas privadas y restringidas), mientras que los hombres tienden a reducirla (35,9% para cuentas públicas o semi públicas).

Finalmente, en relación con las *consecuencias negativas* del uso de la red, los hombres son insultados con mayor frecuencia que las mujeres, pero Facebook es la red social donde las mujeres reciben más insultos (42,5% de respuestas afirmativas, relevancia significativa [$X^2_{(2)} = 12,650$; $p = 0,0018$] respecto de las usuarias de las otras RRSS). El medio concreto de hacerlo es en el muro de un tercer usuario o grupo, o, de modo secundario, en el muro del propio agraviado, y la frecuencia de los hechos es reducida, entre 1 y 2 veces.

5.3. *Instagram*

Al igual que en Facebook, encontramos también una mayoría de mujeres entre los usuarios de Instagram (55,2% frente al 44,8% de hombres), con una edad media menor para ambos supuestos (31,4% para mujeres y 33,8% para hombres) y una mayor presentación para el intervalo de edad de los 24 a 32 años para las primeras y de 33 a 41 años para los segundos. Se trata de usuarios con poca antigüedad en la red social, principalmente de 3 y 6 años (41,9%), seguido de menos de 3 años (33,6%), aunque en las mujeres tienen cuentas con una antigüedad ligeramente superior pero que alcanza un valor estadísticamente significativo [$X^2_{(3)}$ = 8,792; p = 0,0322].

En cuanto a las *actividades habituales*, destaca especialmente respecto a la media el elevado número de conexiones móviles (88,9%), que se conectan con mayor frecuencia que los usuarios de Facebook y que, entre las actividades más frecuentes en la red, presentan valores más elevados para la publicación de fotografías.

En la *privacidad de la cuenta*, las usuarias con más de 500 contactos superan considerablemente a los hombres que exceden dicha cifra (23,4% frente al 9,1% de los hombres, diferencia estadísticamente significativa [$X^2_{(6)}$ = 13,038; p = 0,0424]). Asimismo, las cuentas son mayoritariamente privadas (67,8%).

En lo que respecta a los *problemas*, es de destacar que Instagram es la única red social donde las mujeres son insultadas en mayor medida que los hombres (14,6% y 13,1%, respectivamente), siendo habitual que los agravios se hayan producido entre 3 y 10 veces y que hayan tenido lugar a través de mensajes privados, no de modo público. Asimismo, la proporción de sujetos que señalan haber recibido insultos o faltas de respeto desciende conforme aumenta su edad [$X^2_{(5)}$ = 23,281; p = 0,0003].

5.4. *Twitter*

A diferencia de las RRSS anteriormente comentadas, en Twitter encontramos una mayor representación de hombres (52,9%) con una edad media superior a la de las mujeres –en esto no hay diferencias con otras RRSS– que alcanza los 36,8 años para hombres y 32,8 años para mujeres. En relación con la antigüedad de la cuenta, se observan valores intermedios respecto a las RRSS analizadas (7 a 10 años -36,9%-, seguido de 3 a 6 años -28,7%-); sin que resulte estadísticamente significativo, los hombres tienen mayor antigüedad en la red social que las mujeres.

En cuanto a la *actividad*, Twitter destaca especialmente por ser la red social que mayores conexiones diarias tiene (82,9%), siendo 81,7% de las cuales de modo intensivo (más de una hora diaria). Asimismo, presenta altos valores para conexiones móviles (88,4%).

En relación con la *protección de la privacidad*, destaca principalmente el número de cuentas con más de 500 contactos y con un carácter público –configuración por defecto de la red. Al igual que ocurre en Facebook, las mujeres presentan una mayor configuración de cuentas privadas (45,9%), mientras que en los hombres se observa la tendencia opuesta (un 78,2% señaló tener una cuenta pública), lo cual resulta estadísticamente significativo [$X^2_{y\ (1)} = 20{,}254$; $p < 0{,}0001$]. Conforme los usuarios son más antiguos en la red social, la proporción de cuentas públicas crece, pasando de representar un 52,2% –usuarios de menos de 3 años– hasta alcanzar el 75,9% para usuarios de más de 10 años en la red social [$X^2_{(3)} = 9{,}11$; $p = 0{,}0279$].

Por último, en relación con los *problemas derivados del uso*, los usuarios de Twitter son quienes más insultos reciben -37,4%- proporción que se eleva especialmente en el caso de los hombres, hasta alcanzar el 52,2%. Twitter es, así, la única red social donde la distinción por sexos resulta estadísticamente significativa (del total de insultados de Twitter, los hombres representan el 64,3%. [$X^2_{y\ (1)} = 15{,}017$; $p = 0{,}0001$]). Conforme los usuarios proporcionan más información de carácter personal (V9), la proporción de respuestas afirmativas ante insultos se incrementa. En cuanto a la frecuencia, al igual que en Instagram, lo más habitual es haber recibido agravios entre 3 y 10 veces, pero, a diferencia de la anterior, hay una tendencia hacia una frecuencia mayor (por encima de 10 veces), siendo lo habitual que los hechos tengan lugar en el muro del agraviado.

6. Conclusiones

Se señalaba anteriormente que el principal objetivo de este trabajo era el estudio de las características de los usuarios de RRSS en los aspectos que, según ha señalado la doctrina, hacen los objetivos más atractivos en el espacio virtual a la luz de la TAC.

En este sentido, este trabajo supone una primera aproximación para el análisis del nivel de exposición de los usuarios de las tres RRSS más populares y que mayores interacciones entre desconocidos permiten. Tanto la frecuencia, como la intensidad, la participación activa, la utilización simultánea de múltiples RRSS y el tipo de información compartida, nos apuntan a niveles especialmente altos de exposición personal, con usuarios con interacciones diarias de más de una hora y que introducen bienes protegidos en el espacio virtual que, en muchos casos, además de revelar información íntima o que guarda relación con los hijos, permitiendo su localización física en el espacio no virtual.

Esta alta exposición es, a su vez, accesible para todos los contactos de su red social –que oscilan entre los 100 y 200, o más de 500– puesto que los usuarios no suelen modificar la configuración de privacidad de la cuenta. Como contrapeso encontramos que es frecuente la adopción de ciertas medidas de seguridad, esto es, autoguardianes. Así, los usuarios

mayoritariamente utilizan el bloqueo con carácter preventivo y, en el caso de las mujeres que modifican la configuración de privacidad de la red social, lo hacen para incrementarla. Por el contrario, es de destacar que los hombres habitualmente disminuyen la privacidad de sus cuentas, permitiendo a desconocidos acceder a su información personal.

Asimismo, la mayoría de los usuarios ha experimentado consecuencias negativas con el uso de las RRSS, ya sea porque sus propias publicaciones les ocasionaron problemas con su pareja o amigos –entre otros–, porque otro usuario los ha insultado o faltado el respeto, o porque han presenciado un hecho que consideraron con la gravedad suficiente como para motivar una denuncia ante la red social. En este último caso, cabe destacar especialmente la necesidad de profundizar en el papel de los usuarios como guardianes –informales– de otros usuarios.

Esta información, entendemos, resulta de utilidad a la hora de diseñar medidas de prevención –tales como campañas, por ejemplo– que vengan a incidir en las prácticas de autoexposición que, según se ha visto, son más frecuentes en las RRSS, así como también en el fomento del empleo de las medidas de autoprotección proporcionando la orientación adecuada en función de los perfiles de usuarios de cada red social. Como se ha señalado anteriormente, la reducción de la oportunidad criminal pasa por evitar la confluencia del agresor con el objetivo adecuado en ausencia de guardianes efectivos, por lo que reducir el atractivo del objeto y potenciar el papel de los guardianes y gestores puede tener efectos preventivos.

7. Limitaciones

La principal limitación de este trabajo consideramos que guarda relación con el método no probabilístico de obtención de la muestra. Revisiones futuras de este trabajo deberían obtener una muestra con una mayor representación de todos los intervalos de edad considerados. Asimismo, una ampliación de la muestra permitiría también incluir variables victimológicas que permitirían comparar las características de al TAC aquí analizadas entre los sujetos que han sido víctimas de un delito en las RRSS y las de aquellos que no lo han sido.

Bibliografía

BAILLON, A. *et al.,* "Informing, simulating experience, or both: A field experiment on *phishing* risks", *PLoS ONE* 14(12): e0224216, 2019.

BOSSLER, A. M. *et al.,* "Predicting *online* harassment victimization among a juvenile population", *Youth & Society*, 44 (4), 2012, 500–523.

CHOI, K. S., "Computer Crime Victimization and Integrated Theory: An Empirical Assessment", *International Journal of Cyber Criminology*, 2 (1), 2008, 308–333.

CHOI, K. S. *et al.,* "Mobile Phone Technology and *Online* Sexual Harassment among Juveniles in South Korea: Effects of Self-control and Social Learning", *International Journal of Cyber Criminology*, 11 (1), 2017, 110–127.

CHOI, K. S. *et al.,* "Impacts of *online* risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis", *Computers in Human Behavior,* 100, 2019, 1-10.

CLARKE, R. V., "Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods", *Police Research Series*, Paper 112, Policing and Reducing Crime Unit, Research Development and Statistics Directorate. Home Office, 1999.

COHEN, L. E. Y FELSON, M., "Social change and crime rate trends: A routine activity approach", *American Sociological Review*, 44, 1979, 588-608.

COHEN, L. E. *et al.,* "Social inequality and predatory criminal victimization: An exposition and test of a formal theory", *American Sociological Review*, 46, 1981, 505-524.

ECK, J. E. Y CLARKE, R. V., "Classifying Common Police Problems: A Routine Activity Theory Approach", en M. J. SMITH y D. B. CORNISH (eds.), *Theory and Practice in Situational Crime Prevention. Crime Prevention Studies*, vol. 16, Criminal Justice Press, Nueva York, 2003, 7-39.

FELSON, M. Y CLARKE, R. V., "Opportunity makes the thief: practical theory for crime prevention", *Police Research Series*, Paper 98, Policing and Reducing Crime Unit, Research Development and Statistics Directorate. Home Office, 1998.

FELSON, M. Y ECKERT, M. A., *Crime and Everyday Life A Brief Introduction,* 6ª ed., SAGE Publications, California, 2018.

HINDELANG, M. J. *et al., Victims of personal crime: An empirical foundation for a theory of personal victimization*, Ballinger, Cambridge, 1978.

HOLT, T. J. Y BOSSLER, A. M., "Examining the applicability of lifestyle-routine activities theory for cyber crime victimization", *Deviant Behavior*, 30, 2009, 1-25.

HUTCHINGS, A. y HAYES, H., "Routine Activity Theory and *Phishing* Victimisation: Who Gets Caught in the 'Net'?", *Current Issues in Criminal Justice*, 20 (3), 2009, 433-451.

IAB, ESPAÑA, *Estudio de Redes Sociales 2020*. Accesible en https://iabspain.es/estudio/estudio-redes-sociales-2020/ [Fecha de consulta: 21/07/2020].

KEMP, S., *Digital 2020: Global Digital Overview*. Accesible en https://datareportal.com/reports/digital-2020-global-digital-overview [Fecha de consulta: 21/07/2020]

LECLERC, B. Y FELSON, M., "Routine Activities Preceding Adolescent Sexual Abuse of Younger Children", *Sexual Abuse: A Journal of Research and Treatment*, 28 (2), 2016, 116-131.

LEUKFELDT, E. R. Y YAR, M., "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis", *Deviant Behavior*, 37 (3), 2016, 263-280.

MARCUM, C. D. *et al.,* "Potential factors of *online* victimization of youth: An examination of adolescent *online* behaviors utilizing routine activity theory", *Deviant Behavior*, 31 (5), 2010, 381-410.

MCGUIRE, M. y DOWLING, S., "Chapter 2: Cyber-enabled crimes fraud and theft", *Research Report 75*, Home Office, 2013.

MCLAUGHLIN, E., "Routine Activities Theory", en E. MCLAUGHLIN y J. MUNICE (eds.), *The Sage Dictionary of Criminology,* SAGE Publications, Londres, 2006, 365-367.

MEDINA ARIZA, J., *Políticas y estrategias de prevención del delito y seguridad ciudadana*, Edisofer, Madrid, 2013.

MINISTERIO DEL INTERIOR, *ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA*, 2020.

MIRÓ LLINARES, F., "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", *RECPC,* 13-07, 2011.

MIRÓ LLINARES, F., "La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio", *REIC*, 5 (11), págs. 1-35.

NAVARRO, J. N. Y JASINSKI, J. N., "Going cyber: Using routine activities theory to predict cyberbullying experiences". *Sociological Spectrum*, 32 (1), 2012, 81–94.

NEWMAN, G. R. Y CLARKE, R. V., *Superhighway Robbery: Crime Prevention and E-commerce Crime (Crime Science Series),* Willan, Cullompton, 2003.

NGO, F. T. y PATERNOSTER, R., "Cybercrime Victimization: An examination of Individual and Situational level factors", *International Journal of Cyber Criminology*, 5 (1), 2011, 773–793.

PÉREZ SAN-JOSÉ, P. (dir.), *Guía para usuarios: identidad digital y reputación online*, Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2012.

PRATT, T. C. *et al.,* "Routine *Online* Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory", *Journal of Research in Crime and Delinquency*, 47 (3), 2010, 267-296.

REDONDO ILLESCAS, S. Y GARRIDO GENOVÉS, V., *Principios de Criminología,* 4ª ed., Tirant lo Blanch, Valencia, 2013.

REYNS, B. W., "A routine activity perspective on *online* victimisation", *Journal of Financial Crime*, 22 (4), 2015, 396 – 411.

REYNS, B. W. *et al.,* "Being Pursued *Online*: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization", *Criminal Justice and Behavior*, 38 (11), 2011, 1149-1169.

SOLARI MERLO, M. N., "Medidas de autoprotección en redes sociales", *Archivos de Criminología, Seguridad Privada y Criminalística,* 27, 2021, 91-117.

VAKHITOVA, Z. I. *et al.,* "Lifestyles and routine activities: Do they enable different types of cyber abuse?", *Computers in Human Behavior*, 101, 2019, 225–237.

VAN WILSEM, J., "'Bought it, but never got it': Assessing risk factors for *online* consumer fraud victimization", *European Sociological Review*, 29 (2), 2013, 168-178.

WHITTY, M. T., "Predicting susceptibility to cyber-fraud victimhood", *Journal of Financial Crime*, 26 (1), 2019, 277-292.

YAR, M., "The novelty of 'cybercrime': An assessment in light of routine activity theory", *European Journal of Criminology*, 2, 2005, 407-427.

YBARRA, M. L. Y MITCHELL, K. J., "How risky are social networking sites? A comparison of places *online* where youth sexual solicitation and harassment occurs", *Pediatrics*, 121 (2), 2008, 350-357.