Revista Electrónica de Estudios Penales y de la Seguridad
ISSN: 2531-1565

VICTIMIZACIÓN DE LOS USUARIOS DE LAS APLICACIONES AFECTIVO-SEXUALES Y CULTURA DE COMPLIANCE

VICTIMIZATION OF USERS OF AFFECTIVE-SEXUAL APPLICATIONS AND THE CULTURE OF COMPLIANCE

David Pavón Herradón[1]
Profesor de Derecho
Universidad Europea de Madrid (UEM) (España)

Antonio Silva Esquinas
Profesor de Criminología
Universidad Europea de Madrid (UEM) (España)

Jorge Ramiro Pérez Suárez
Profesor de Criminología
Universidad Europea de Madrid (UEM) (España)

R. Rebeca Cordero Verdugo
Profesora Titular en Sociología Aplicada
Universidad Europea de Madrid (UEM) (España)

Aída Fonseca Díaz
Profesora de Derecho
Universidad Europea de Madrid (UEM) (España)

Fecha de recepción: 9 de enero de 2022.

Fecha de aceptación: 25 mayo de 2022.

RESUMEN

Los Proyectos *"Enrolla2 Generación X Percepciones de Seguridad y Actitudes de Riesgo en individuos pertenecientes a la Generación X vinculadas al uso de aplicaciones informáticas afectivo-sexuales (CIPI/20/091)"* y *"La gestión del deseo en tiempos del*

[1] Todos los autores forman parte del Grupo de Conocimiento-Investigación en Problemáticas Sociales Universidad Europea de Madrid y del Departamento de Ciencias Jurídicas y Políticas de la Facultad de Ciencias Sociales y de la Comunicación UEM.

COVID (CIPI/20/159)" tenían como respectivos objetivos, estudiar la percepción de la seguridad, su incidencia en el nivel de victimización y los riesgos para la salud de los individuos en las aplicaciones afectivo-sexuales; y conocer las motivaciones que han llevado a los mismos a usar *apps* afectivo-sexuales durante el confinamiento. Se observaron diferentes niveles de seguridad en las *apps*, dependiendo del tratamiento de los datos de los usuarios, la existencia de actitudes de hostigamiento y la emergencia de un mercado de droga digital. Jurídicamente, se presume necesario mejorar la protección de los usuarios, potenciales víctimas de delitos -singularmente identificados- y, asimismo, incentivar la cultura de la prevención o *compliance* con respecto a las entidades propietarias de dichas plataformas.

ABSTRACT

The Projects "Enrolla2 Generation X Security Perceptions and Risk Attitudes in individuals belonging to the Generation X linked to the use of affective-sexual computer applications (CIPI / 20/091)" and "The management of desire in times of COVID (CIPI / 20/159) "had as their respective objectives, to study the perception of security, its incidence in the level of victimization and the risks to the health of individuals in affective-sexual applications; and to know the motivations that have led them to use affective-sexual apps during lockdown. Different levels of security were observed in the apps, depending on the treatment of user data, the existence of harassing attitudes and the emergence of a digital drug market. Legally, it is understood as necessary to improve the protection of users, potential victims of crime - individually identified - and, likewise, encourage the culture of prevention or compliance with respect to the companies that own said platforms.

PALABRAS CLAVE

Etnografía digital, Criminología, sexualidad, delitos, *compliance*.

KEYWORDS

Digital ethnography, Criminology, sexuality, crimes, compliance.

ÍNDICE

SUMMARY

1. INTRODUCCIÓN.

Como se ha tenido ocasión de exponer[2], también en estudios previos al presente[3], en los últimos años se ha venido produciendo una proliferación y expansión de las redes sociales, de las llamadas *apps* y, concretamente, de forma especial, aunque no única, de las *apps* informáticas afectivo-sexuales que, al margen de conformar una forma de intercomunicación e interacción entre individuos, se han convertido en un nuevo contexto o nicho de riesgo de producción de determinados comportamientos delictivos.

A este respecto, como se dice, ya se tuvo oportunidad de hacer un primer análisis jurídico de los principales riesgos que existen para determinados usuarios de estas plataformas de contacto y de los principales delitos que emergen en algunas de las mencionadas redes sociales, todo ello fruto de la observación y análisis llevados a cabo en el proyecto "*Enrolla2. Percepciones de seguridad y actitudes de riesgo en "millennials" vinculadas al uso de apps informáticas afectivo-sexuales*", del Grupo de Conocimiento-Investigación en Problemáticas Sociales de la Universidad Europea en

[2] En este artículo se amplía el contenido de la ponencia presentada en el II Congreso Iberoamericano "Política Criminal de Excepción durante la Emergencia Sanitaria y su Impacto en los Derechos Humanos" organizado por la Red Iberoamericana de Investigadores en Política Criminal e Instituciones de la Seguridad, entre otras instituciones.

[3] Vid. SILVA ESQUINAS, A., FONSECA DÍAZ, A.R., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R.R. Y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia violeta. Análisis jurídico con perspectiva de género en base a la etnografía del Proyecto Enrolla2", en *Revista Internacional de Derecho Contemporáneo, vol. 74*, Legis Editores, Colombia, 2021, pp. 5-40.

Madrid (con el código Enrolla2 2018/UEM34, financiado por la Universidad Europea)[4], estudio circunscrito hasta usuarios de edad no superior a los 35 años (desde los 18).

Pues bien, dando continuidad a dicho estudio en torno a los riesgos y posibles ilícitos en el contexto de estas *apps*, por el mismo Grupo de Conocimiento-Investigación en Problemáticas Sociales se ha abordado en esta ocasión un nuevo análisis de otras redes sociales del carácter indicado, esta vez en el ámbito del proyecto "*Enrolla2. Percepciones de seguridad y actitudes de riesgo en individuos pertenecientes a la Generación X vinculadas al uso de aplicaciones informáticas afectivo-sexuales* (CIPI/20/091)", (con el código Enrolla2 2020/UEM19, financiado por la Universidad Europea)[5], referido en esta oportunidad a usuarios con edades superiores a los 36 años y hasta los 50. Dicho estudio se complementa con el denominado "*La gestión del deseo en tiempos del COVID* (CIPI/20/159)"[6], también del Grupo de Conocimiento-Investigación en Problemáticas Sociales, centrado en conocer las motivaciones que han llevado a los individuos a usar *apps* afectivo-sexuales durante el confinamiento. Ambos estudios se retroalimentan metodológicamente, a través de un diseño de métodos mixtos: etnografía digital abierta multisituada en estas *apps*, entrevistas a usuarios, micro-encuestas en redes sociales y encuestas a personas que usaron estas *apps* en el confinamiento.

Sin perjuicio del estudio de los riesgos existentes para estos usuarios y de los singulares comportamientos delictivos observados con respecto a los mismos, en el proyecto "*Enrolla2. Percepciones de seguridad y actitudes de riesgo en individuos pertenecientes a la Generación X vinculadas al uso de aplicaciones informáticas afectivo-sexuales* (CIPI/20/091)", se pone también especial énfasis en el estudio de la seguridad de las *apps*, aspecto no abordado en el trabajo referido a la "*Generación Millennials*", tan solo apuntado, pero igualmente aplicable al mismo, entendido precisamente como uno de los principales agentes generadores de la puesta en riesgo o lesión de bienes jurídicos titularidad de los usuarios de las aplicaciones e, incluso, de titularidad o interés general o carácter supraindividual.

En este sentido, como se manifestó en este primer estudio jurídico, debe partirse ahora nuevamente de la premisa de que en el medio digital se producen iguales comportamientos delictivos que en el ámbito o medio analógico; iguales ilícitos que acontecen, sin embargo, incluso con mayor facilidad en el mundo digital, en atención al anonimato o falsa sensación de seguridad que la víctima percibe como consecuencia de los filtros que en apariencia tienen las mentadas aplicaciones[7].

De la observación de los delitos que habitualmente se producen con respecto a los "*Millennials*" en estas aplicaciones informáticas afectivo-sexuales, se dedujeron[8],

[4] En concreto, se analizaron seis *apps* afectivo-sexuales: *Tinder, Grindr, Badoo, Lovoo, Wapa y Wapa* (Silva *et al*, 2018). Este análisis jurídico culminó en la publicación reseñada en la nota al pie que precede.
[5] En concreto se analizaron cinco *apps* afectivo-sexuales: *Meetic, Pof, Lumen, Wapa y Wapo* (Silva "*et al*", 2020).
[6] Vid. CORDERO VERDUGO, R.R., PÉREZ SUÁREZ, J.R. Y SILVA ESQUINAS, A., "La gestión del deseo afectivo-sexual en la crisis de la Covid-19", en *La vida cotidiana en tiempos de la COVID. Una antropología de la pandemia*, Del Campo Tejedor, A., (coord.) y AA.VV., Los Libros de la Catarata, Madrid, 2021, pp. 201-225.
[7] SILVA ESQUINAS, A., FONSECA DÍAZ, A.R., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R.R. Y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia… cit., p. 6.
[8] Ibidem, pp. 9 y ss.

como principales, los que tienen que ver con la personalidad, la intimidad personal, la libertad y la libertad e indemnidad sexuales, como pueden ser, entre otros, los siguientes: recepción no solicitada de materiales sexualmente explícitos y la pornografía de venganza (*revenge porn*), *creepshots, upskirting, digital voyeurism, doxing o doxxing, cyber stalking, cyber bullying, s*uplantación de identidad (*impersonation*), *hacking, cracking* o *amenazas de violencia (threats of violence)*. Algunos de ellos presentan un encaje más o menos sencillo desde el punto de vista de la dogmática penal y el Derecho positivo, al identificarse el respectivo comportamiento con alguna de las figuras delictivas descritas en el Código Penal español, no obstante lo cual, otros tantos, como el caso, por citar algún ejemplo, del primero de los señalados, la recepción no solicitada de materiales sexualmente explícitos y la pornografía de venganza (*revenge porn*), no tienen una fácil identificación en la norma penal sustantiva española, debiendo acudirse a figuras tradicionales de aplicación subsidiaria a falta de un tipo penal concreto, como ocurre paradigmáticamente con el delito de coacciones, ya asumido doctrinalmente como un tipo de recogida[9].

Incluso, se ha llegado a comprender a tenor de los anteriores comportamientos, de la existencia de una nueva forma de violencia de género, llevada a cabo a través del medio tecnológico en general[10] y, en particular, de estas *apps* afectivo-sexuales, ya denominadas por organismos internacionales como el Parlamento Europeo "*Cyber violence and hate speech online against women*"[11].

Por su parte, de la más reciente observación realizada de las aplicaciones informáticas afectivo-sexuales, como se dice, esta vez con respecto a la llamada "*Generación X*", al margen de reproducirse en mayor o menor medida delitos como los acabados de enumerar y que, por ello, no serán objeto de análisis en esta ocasión, parece que se identificaron algunos otros muy concretos, como lo serían el uso indebido de datos que conforman la intimidad del usuario, el trabajo sexual, la corrupción de menores, el tráfico de drogas o, en el contexto patrimonial, las estafas; delitos cuya comisión también se vería facilitada por el medio digital a través de las *apps*.

Para la evitación de comportamientos delictivos como los señalados tanto en uno como en otro estudio, resulta trascendental el papel de las personas jurídicas responsables de las aplicaciones, sobre la base, por una parte, de la llamada ética corporativa y, por otra parte, de la responsabilidad penal en la que las mismas podrían incurrir como consecuencia de los delitos que puedan producirse o facilitarse a través de la red o aplicación de la que resultan titulares.

[9] Por todos, PAVÓN HERRADÓN, D., "Amenazas y coacciones", en Armendáriz León, C. (dir.), Bustos Rubio, M. (coord.) y AA.VV., *Parte Especial del Derecho Penal a través del sistema de casos*, Tirant lo Blanch, Valencia, 2020, p. 100.

[10] Sobre los delitos de violencia de género en el contexto tecnológico, Vid. MÉNDEZ HERNÁNDEZ, M., "Los delitos de violencia de género a través de medios telemáticos", en Ortega Burgos, E., (dir.), Andújar, J., Imbroda B.J., Tuero, J.A., Frago Amada, J.A. (coords.) y AA.VV., *Actualidad Penal 2019*, Tirant lo Blanch, Valencia, 2019, pp. 471-488.

[11] Así se denomina el estudio publicado por Van Der Wilk para el Parlamento Europeo en junio de 2018. Accesible en (último acceso 29-11-2021):
https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

En este sentido, con respecto a este último aspecto, ya es sabido que la norma penal sustantiva[12] introdujo en el año 2010, a través de la reforma operada por la LO 5/2010[13], la responsabilidad penal de las personas jurídicas, la cual fue objeto de posterior modificación a través de la LO 1/2015[14]. Precisamente, para la evitación en la medida de lo posible de estos riesgos para los bienes jurídicos más importantes en el ámbito o contexto de la actividad empresarial, se adoptó este nuevo sistema de responsabilidad, fruto del cual ha emergido, como instrumento al servicio de tal finalidad, el llamado "*Corporate Compliance*", entendido como un conjunto de buenas prácticas y procedimientos ideados para la localización de riesgos de producción de ilícitos en el seno o en el contexto de la persona jurídica, ya a nivel interno, por su personal, ya por terceros ajenos a la misma, y para la generación de mecanismos de alerta, prevención, gestión, control y respuesta frente a tales riesgos o comportamientos. Sistemas de prevención de riesgos penales que, además, han generado el surgimiento y auge de la primeramente mencionada ética corporativa, encaminada a la generación de una cultura de valores y principios que informen favorablemente de la reputación de la empresa y de su compromiso para con los derechos individuales y colectivos.

No en vano, a nivel internacional han surgido normas de estandarización y normativización en torno a la conformación de los llamados *Sistemas de Gestión de Compliance*, concretamente, a través de la norma ISO 19600, sustituida en 2021 por la ISO 37301, e igualmente, de estandarización y normativización de sistemas del *Compliance Penal*, a través de la ISO 19601, desarrollada en España a través de la correspondiente UNE[15].

Expuesto lo anterior, en las siguientes líneas se tratará de hacer una aproximación, fundamentalmente a partir del reporte etnográfico "*Enrolla2 Generación X*", además de las nuevas formas delictivas que parecen haberse hallado en el contexto de las aplicaciones informáticas afectivo-sexuales analizadas, las debilidades observadas en materia de seguridad que las mismas presentan, así como la importancia de una adecuada planificación y ejecución del "*Corporate Compliance*" para la lucha contra estas formas de criminalidad y, por ende, como forma de dotar verdadera protección a los usuarios de estas *apps*, y no como una mera forma de evitación de consecuencias jurídicas para las empresas responsables o titulares de las mismas.

Debe, pues, preguntarse de nuevo, si acaso son estos nuevos escenarios los que están provocando o favoreciendo la comisión de delitos como los señalados, favorecido por la deficiente o insuficiente seguridad de estas redes y plataformas, o bien, si son los propios usuarios, a través de sus comportamientos, los que lo estarían permitiendo e incluso, paradójicamente, fomentando la proliferación de estos hechos delictivos mediante acciones de autopuesta en peligro.

---

[12] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE núm. 281, de 25 de noviembre de 1995.

[13] Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE núm. 152, de 23 de junio de 2010.

[14] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE núm. 77, de 31 de marzo de 2015.

[15] GÓMEZ-JARA DÍEZ, C., *Compliance penal y responsabilidad penal de las personas jurídicas. A propósito de la UNE 19601. Sistemas de Gestión de Compliance Penal*, Aranzadi, Cizur Menor (Navarra), 2020.

2. BREVE REFERENCIA A ALGUNA DE LAS NUEVAS TIPOLOGÍAS DELICTIVAS OBSERVADAS EN LA CIBERESFERA DE LAS *APPS* AFECTIVO-SEXUALES CONFORME A LA REGULACIÓN JURÍDICO PENAL ACTUAL EN ESPAÑA

Como se ha apuntado en líneas anteriores, del estudio etnográfico "*Enrolla2 Generación X*", se ha comprobado la aparente existencia de nuevos tipos delictivos, que se sumarían a los ya observados en el reporte etnográfico "*Enrolla2 Millenials*". Sucintamente y a título ejemplificativo, a continuación, se hará referencia a alguno de estos nuevos comportamientos, así como a su identificación en la norma penal de entre los delitos contenidos en su Libro II (Delitos y sus penas).

La identificación de los citados comportamientos que parece tienen lugar en las *apps* objeto de observación y estudio, y su contraste en la norma penal, permitirá verificar tanto el tipo penal que resultaría en cada caso de aplicación y, por tanto, cuál sería su regulación positiva, como la respuesta punitiva que se podría derivar de tales acciones o, en su caso, omisiones. Ello permitirá conocer de qué manera y con qué alcance tiene lugar la acción protectora de los intereses en juego por parte de la legislación punitiva, todo ello, prescindiendo en este momento del tratamiento jurídico-penal que pudiera darse a una posible autopuesta en peligro por parte del propio titular del bien jurídico y que pudiera haber coadyuvado al surgimiento del comportamiento reprochable que, en todo caso, no resultaría por ello justificado.

No obstante, los siguientes fenómenos delictivos, como se dice, parece que no serían los únicos observados, quedando para un posterior análisis y estudio algunos otros, relacionados con el trabajo sexual, la corrupción de menores o la distribución de drogas.

2.1. *Catfish*.

El fenómeno del *catfish* consiste en una forma de usurpación de la personalidad (*impersonation*), la cual tiene lugar en el ámbito de las redes sociales, especialmente en las relacionadas con las *apps* afectivo-sexuales, creando una cuenta falsa o un perfil falso, incluso con una identidad de género diferente o simulando una edad determinada, circunstancias de las que incluso puede depender la posibilidad de participar en las *apps*.

Al *catfish* ya se hizo concreta (pero breve) referencia en el estudio dedicado a los usuarios de la "*Generación Millennials*"[16], pero de nuevo resulta obligada su mención y análisis, esta vez más profundo que entonces, habida cuenta del protagonismo que alcanza con respecto a los usuarios de la *Generación X* este fenómeno.

La conducta[17] parece, en apariencia, que se produce en dos principales modalidades, a saber: una, consistente en conformar una personalidad irreal, un perfil, manera de ser, carácter concreto…, que sin embargo son mera invención, haciendo creer a un tercero que tal persona realmente existe, con la cual cree estar

[16] SILVA ESQUINAS, A., FONSECA DÍAZ, A., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R. y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia… cit., p. 22.
[17] Sobre el delito de usurpación de estado civil, Vid. por todos, DÍAZ LÓPEZ, J.A., *El delito de usurpación del estado civil*, Dykinson, Madrid, 2010.

relacionándose; y otra, consistente en tomar la imagen y/o personalidad de un tercero (o algún aspecto de la misma), a fin de hacerse pasar por tal persona, bien en forma absoluta, bien con respecto a la imagen o ciertos aspectos de su perfil, manera de ser o carácter.

De ambas modalidades, como se expondrá y justificará a continuación, esta última es la única que en sentido estricto se podría identificar con la usurpación de la personalidad desde el prisma técnico-legal, lo que impediría, por tanto, hablar de usurpación como forma delictual en ambos supuestos. En este sentido y, concretamente, desde el punto de vista del Ordenamiento penal, debe partirse de que la usurpación de la personalidad se halla recogida en el artículo 401 del Código Penal español, ubicado en el Capítulo IV (De la usurpación del estado civil), del Título XVIII (De las falsedades), siendo una suerte de suplantación de identidad penada con prisión de entre seis meses y tres años.

El comportamiento descrito en la mencionada norma es completamente abierto, pues la dicción típica únicamente refiere como tal *"el que usurpare el estado civil de otra persona"*, admitiéndose, en consecuencia, cualquier forma de usurpación o de apoderamiento de la personalidad. Sin embargo, a este respecto y teniendo en cuenta lo dicho en líneas anteriores, debe interpretarse que el tipo penal deviene limitando en realidad a la usurpación en los casos en los que se estuviera tomando la imagen y/o rasgos de la personalidad de otra persona, a fin de hacerse el autor pasar por la misma y, por tanto, que no estaríamos ante supuestos de usurpación cuando el sujeto activo se presentara como una persona cuyos rasgos de la personalidad son inventados, no tomados de otro o, al menos, con suficiente consistencia como para en un momento dado poder identificar a ese tercero. Debe tenerse en cuenta a favor de esta interpretación estricta, que cuando la norma penal sustantiva alude a *"otra persona"*, parece que lo está refiriendo a alguien que en verdad existe, persona de la cual se toma la imagen y/o rasgos de la personalidad, y por la que quien actúa pretende pasarse.

Consecuentemente, la usurpación de identidad se refiere exclusivamente a los casos en los que se pretende la suplantación de la identidad de otro, y no a la invención de una identidad que no supone la suplantación de identidad de un tercero. Nos hallamos, pues, en presencia de un delito de naturaleza falsaria, tanto porque así puede deducirse del propio comportamiento, marcado por su alejamiento de la realidad e, igualmente, porque parece coherente si se atiende a la sistemática del legislador, que resolvió incluir el delito de usurpación de estado civil en el Título referido a las falsedades.

Y es precisamente de su naturaleza falsaria de la que se derivan una serie de consideraciones que no pueden dejar de atenderse, por las implicaciones jurídico-penales que las mismas conllevan. De este modo, la primera consideración que ha de extraerse de la citada naturaleza, es que la usurpación de la personalidad trae su *ratio legis* en el hecho mismo de la falsedad que tal comportamiento supone, esto es, en el hecho mismo de hacer creer a terceros que quien actúa es otra persona. Se trata, por tanto, de una circunstancia por sí sola se hace merecedora del reproche jurídico-penal, sin que sea preciso para su sanción que de la usurpación realizada se deriven nuevos riesgos o lesiones para otros bienes jurídicos, más allá, pues, del consisten en la seguridad del tráfico jurídico, que es el que se daña cuando se suplanta a otra persona.

La segunda consideración tiene que ver con el caso de la personalidad falsa pero inventada, esto es, aquella que se ha indicado no podría subsumirse en las previsiones del artículo 401 del Código Penal. Pues bien, habida cuenta de la naturaleza falsaria del delito, pese a las dificultades señaladas para comprenderse ese perfil falso como una suplantación de identidad, podría sin embargo tener encaje como delito de falsedad documental *ex* artículo 395 de la norma penal sustantiva, esto es, entender que nos hallamos simplemente ante una falsedad documental a la relacionado con la creación de un perfil falso, circunstancia que debe ser igualmente objeto de comprobación[18].

El artículo 395 del Código Penal recoge el delito de falsedad en documento privado, cometido por persona particular, al señalar que *"El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390"*, previéndose una pena de prisión de seis meses a dos años. Relacionado, pues, con el mismo, habrá de atenderse a las modalidades comisivas[19] recogidas en el artículo 390.1.1º, 2º y 3º, esto es, la falsedad en documento privado del particular deberá producirse, ya alterando un documento en alguno de sus elementos o requisitos de carácter esencial, ya simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad, o ya suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes a las que hubieran hecho (*sic*).

Como puede deducirse de las anteriores líneas, para que la creación de un perfil falso e inventado en una *app*, pudiera comprenderse como el delito de falsedad documental, toda vez que no puede serlo de usurpación, se requeriría, en primer término, admitir que la generación del perfil mismo se trata de una falsedad en documento privado, de tal forma que debe asimilarse el apartado de la aplicación para el registro y alta de usuario como un documento de naturaleza privado, lo que no parece conllevar excesivas dificultades, no tratándose de un documento ni oficial, ni público, ni mercantil; en segundo lugar, que la falsedad descrita sea llevada a cabo con el objeto o finalidad de perjudicar a un tercero, lo que igualmente no parece de complicada comprensión, en tanto que la creación de una personalidad falsa parece llevar inherente la idea de perjuicio al que deposita en dicha información que se facilita una legítima expectativa de veracidad. En este sentido, debe tenerse en cuenta que el bien jurídico protegido en los delitos de falsedad documental viene conformado por la función del documento que se altera, es decir, lo que pretende dotarse de protección es la función que presenta el documento que es objeto de falsificación, en este caso, el perfil del usuario, cuya función es conocer al sujeto con el que puede llegar a interactuarse, de tal suerte que con la falsedad de la personalidad reflejada en el formulario de alta de la aplicación de que se trate, se daña la función que tiene tal documento en orden a dar a conocer al nuevo usuario frente al resto de personas que igualmente participan en la *app*.

[18] Sobre las falsedades documentales, Vid. NIETO MARTÍN, A., "Falsedades en la empresa", en De la Mata Barranco, N., Dopico Gómez-Aller, J., Lascuraín Sánchez, J.A. y Nieto Martín, A., *Derecho Penal Económico y de la Empresa*, Dykinson, Madrid, 2018, pp. 685-726.

[19] PAVÓN HERRADÓN, D., *El delito de falsedad documental societaria*, Bosch-Wolters Kluwer, Madrid, 2016, pp. 102-112.

Finalmente, para poder considerar que estos comportamientos relativos a la creación de un perfil irreal, encajan en el delito de falsedad en documento privado, como alternativa de naturaleza falsaria al de usurpación de estado civil, se hace necesario que la falsedad en sí misma cometida haya tenido lugar en laguna de las formas descritas en el apartado 1, números 1º a 3º, del artículo 390 del Código Penal. Sin embargo, de la lectura sosegada de dichas modalidades comisivas y de su interpretación técnica, no parece posible que la creación del perfil falso en las aplicaciones objeto de estudio venga a producirse en alguna de esas tres maneras, pues ni se altera un documento en alguno de sus elementos o requisitos de carácter esencial, toda vez que el documento es de nueva creación, ni se simula un documento en todo o en parte, pues el formulario no se reproduce ni total ni parcialmente, sino que se emplea el original, ni se hace suponer la intervención de personas o la atribución a las mismas de determinadas afirmaciones en un concreto acto que en verdad no tiene lugar en el caso concreto.

Más bien puede afirmarse que el comportamiento que realiza el sujeto que crea una identidad o perfil falso no empleando la imagen o datos de la personalidad de un tercero, consistiría en una mera forma de falsedad ideológica, esto es, en hacer constar, simple y llanamente, unos datos inciertos en el formulario de registro y alta de usuario de la *app*, acción que encaja en la descripción del número 4º del mismo artículo 390.1 (*"faltando a la verdad en la narración de los hechos"*) y que, sin embargo, cuando es cometido por un particular y en documento privado, resulta atípico, tal y como se deduce de la redacción del artículo 395 del Código Penal, que sólo contempla como posibles formas comisivas las previstas en el artículo 390.1.1º, 2º y 3º.

De cuanto precede puede concluirse, en lo que se refiere al fenómeno del *catfish*, que el mismo sólo tendría encaje o reflejo en una de las figuras contempladas en el Código Penal español, en concreto, en la usurpación de estado civil, cuando el comportamiento consistiere en emplear la imagen y/o datos de la personalidad de un tercero, haciendo creer que esa persona es la que interactúa, pero no en el supuesto de la invención de un perfil inventado, acción que, como se ha indicado, sería atípica, puesto que ni cumple con los elementos típicos propios del delito de usurpación, ni alternativamente los del delito de falsedad en documento privado. Ello conduce a la consideración de que este último caso resulta alejado de los delitos de naturaleza falsaria, por lo que podría estar más cercano a los de naturaleza defraudatoria, en concreto, a la estafa, la cual abordaremos en las siguientes líneas, castigando, en su caso, la forma del engaño bastante, pero no conformando un tipo penal autónomo.

2.2. Timos.

Como se desprende del estudio realizado con respecto a la llamada *"Generación X"*, en ocasiones se solicita a los usuarios excesiva información acerca de las circunstancias familiares y económicas, al menos así lo parece en orden al establecimiento de afinidades, extremo que puede favorecer o incentivar comportamientos de naturaleza defraudatoria, como pueden ser los timos, estafas desde un punto de vista técnico-jurídico. Efectivamente, como consta en el varias veces mencionado estudio etnográfico que precede al presente trabajo y que sirve de base al mismo, algunas *apps* solicitan a los usuarios un elevadísimo número de datos de carácter

personal, que alcanzan incluso el conocimiento sobre los ingresos que perciben regularmente por razón del trabajo, así como otras circunstancias que pueden delatar, directa o indirectamente, estados sociales o económicos concretos de la persona, como por ejemplo, entre otros, el estado civil del usuario o sus familiares, el orden de nacimiento cuando el usuario tiene hermanos, si se poseen vehículos o si se consumen drogas.

Con respecto a estas posibles conductas defraudatorias, es indudable que el patrimonio se erige como interés objeto de protección, siendo objeto material del delito los bienes que integran el patrimonio, esto es, dinero, inmuebles, joyas, derechos patrimoniales, etcétera [20], y que en el caso concreto se verían afectados.

Los conocidos como timos en el contexto de las *apps*, encuentran su acomodo normativo en los artículos 248 y siguientes de la norma penal sustantiva, donde se regula el delito de estafa. Básicamente se producen, conforme al Código Penal español, cuando, a través de un engaño, se logra provocar un error en un tercero, a consecuencia del cual éste lleva a cabo una disposición patrimonial, dañando dicho patrimonio. Para que este engaño tenga relevancia desde la perspectiva penal, debe presentarse como bastante, es decir, como una maniobra no burda o absurda, o fácilmente apreciable como falsa, sino con la entidad suficiente como para provocar en un sujeto medio la creencia de su veracidad o verosimilitud, siendo la consecuencia directa de ello ese actuar bajo engaño, esto es, bajo error.

De este modo, como se dice, quedarían fuera del engaño relevante a los efectos de la estafa, aquellos que se fundan en un error burdo o evidente. En conexión con ello, como nos recuerda DOPICO GÓMEZ-ALLER, *"Por llamativo que parezca, existen mentiras permitidas, afirmaciones falsas que se toleran en el tráfico, como el llamado dolus bonus o la exagerada ponderación de las virtudes de la cosa por parte del vendedor. Se trata de actos socialmente adecuados, de riesgos permitidos en el tráfico"*[21]. Trasladada la cuestión al campo objeto de estudio, podrían llegar a comprenderse que determinadas exageraciones que se producen por algunos usuarios en el contexto de las apps afectivo-sexuales, podrían considerarse como admisibles si, con una valoración imparcial y ponderada, pudiera llegar a comprenderse una limitada capacidad de afectación patrimonial en el engañado.

Así, por ejemplo, podría carecer de trascendencia jurídico-penal, un comentario efectuado por un usuario que consistiera en explicar a otro usuario que cada sábado cena en un lujoso restaurante, con el objetivo de presentarse a sí mismo con una imagen exagerada en lo que se refiere a su calidad de vida y nivel patrimonial, circunstancia que a su vez podría poner en riesgo el patrimonio del receptor de tal mensaje, al descuidar

[20] En referencia a la estafa, LIÑÁN LAFUENTE, A., "Capítulo III. Estafas y otras defraudaciones", en Liñán Lafuente, A. (coord.) y VV.AA., *Delitos económicos y empresariales*, Dykinson, Madrid, 2020, p. 109. Vid. también FERNÁNDEZ SALINERO SAN MARTÍN, M.A., "Tema práctico I: Estafa (arts. 248-251 bis CP)", en Abadías Selma, A., Bustos Rubio, M. (dirs.) y AA.VV., *Temas prácticos para el estudio del Derecho Penal Económico*, Colex, A Coruña, 2020, pp. 21-33; o NÚÑEZ CASTAÑO, E., "Los delitos patrimoniales de defraudación (I): estafa, apropiación indebida y administración desleal", en Galán Muñoz, A. y Núñez Castaño, E., Manual de Derecho penal Económico y de la Empresa, 2ª edición, Tirant lo Blanch, Valencia, 2018, pp. 51-73.

[21] DOPICO GÓMEZ-ALLER, J., "Estafa y otros fraudes en el ámbito empresarial", en De la Mata Barranco, N., Dopico Gómez-Aller, J., Lascuraín Sánchez, J.A. y Nieto Martín, A., *Derecho Penal Económico y de la Empresa*, Dykinson, Madrid, 2018, p. 176.

el nivel de protección de sus propios bienes constante su relación con aquél. En este sentido, para que pudiera apreciarse el engaño bastante, debería existir el llamado dolo antecedente por parte del que emite la información falsa, esto es, dicho de otra manera, quien aparenta un nivel económico alto debería trasmitir esta información al otro usuario con el ánimo inicial de llevar a cabo un timo, y no por razón de lograr una relación más estrecha con la otra persona, sin perjuicio de lo cual, esta última, a la vista del comentario, podría llegar a realizar un acto de disposición patrimonial bajo engaño, como por ejemplo, hacerle llegar un regalo de cumpleaños más caro de lo que pudiera considerarse razonable para un usuario carente de altos recursos.

Por lo tanto, para que pueda apreciarse que el engaño puede conducir a una estafa, se requiere que el mismo sea antecedente, bastante y causal de la disposición patrimonial[22]. Y, consecuentemente, sólo en los casos señalados podrá comprenderse producido un timo, debiendo descartarse los casos en los que el engaño no tiene como objetivo previamente ideado el desembolso patrimonial injusto de otro usuario, siendo esta la razón en sí del engaño, ni el mismo puede considerarse como desencadenante lógico que conduzca a la disposición económica ulteriormente hecha.

De este modo, en los timos o estafas, así en las que tienen lugar a través o en el contexto de las *apps* afectivo-sexuales, como en cualquier otro ámbito, el engaño causador del daño patrimonial es el elemento sobre el que pivota el reproche penal, de tal suerte que, a falta de tal engaño, no puede hablarse de defraudación; el engaño, pues, hace creer en el tercero que algo que es cierto no lo es, o a la inversa, lo que tendrá lugar por medio de cualquier ardid, maquinación, fabulación o artificio[23]. Posibles ilícitos en cuya concurrencia puede resultar decisiva la excesiva e innecesaria información que algunas aplicaciones requieren del usuario que se registra, al socaire o con el supuesto objetivo de la búsqueda de afinidades con otros consumidores de las *apps*.

2.3. Revelación de la intimidad.

De nuevo como se desprende del estudio realizado de las apps afectivo-sexuales con respecto a la llamada *"Generación X"*, el exceso de información que se solicita a los usuarios, especialmente en algunas *apps*, acerca de sus circunstancias personales, familiares e, incluso, económicas, en principio, para el establecimiento de afinidades entre usuarios, puede favorecer o incentivar sin embargo comportamientos atentatorios contra la intimidad y la normativa general sobre protección de datos, lo que se desdobla, por una parte, en un riesgo de eventuales comportamientos vinculados a utilización indebida de información en masa de los usuarios o *big data* y, por otra parte, aunque de manera menos compleja, el simple riesgo de una eventual comunicación indebida a terceros de los datos que forman parte de la intimidad de un usuario en particular; posibles comportamientos que nos sitúan más bien en el plano de la revelación de los secretos que afectan a la vida personal o familiar de los usuarios, y no tanto en el plano del descubrimiento en sí de dichos datos.

La intimidad se erige como un derecho fundamental de rango constitucional. El artículo 18.1 garantiza *"el derecho al honor, a la intimidad personal y familiar y el*

[22] Así LIÑÁN LAFUENTE, A., "Capítulo… cit., p. 110.
[23] Ibidem, p. 110.

derecho a la propia imagen", mientras que el apartado 4 previene cómo *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. Pues bien, la transgresión de este derecho fundamental se produce con cierta facilidad en el entorno digital ya que, junto con la evidente autopuesta en peligro del propio usuario como primera posible fuente facilitadora de datos que compromete su intimidad, se produce indefectiblemente un escenario de riesgo extraordinario, marcado por la necesidad de un tratamiento masivo de los datos personales recabados por las *apps*, con y sin constancia o consciencia del propio usuario, datos a partir de los cuales se le puede medir, perfilar, clasificar y predecir, lo que, como se decía en el análisis jurídico de los principales riesgos que existen para usuarios de las apps afectivo-sexuales de la "*Generación Millenials*", supone estar en presencia de *"una autentica copia digital de la persona, un holograma mercantilizado creado a la medida de otros"*[24], en torno a la cual es más que evidente el riesgo de utilización indebida por parte del tenedor de los datos o por parte de terceros que puedan llegar a tener acceso legal o ilegal a los mismos.

Como ya se dijera en líneas anteriores, del estudio etnográfico elaborado con respecto a usuarios de las *apps* afectivo-sexuales de usuarios pertenecientes a la llamada "*Generación X*", se comprueba que algunas de estas aplicaciones solicitan a los usuarios un elevadísimo número de datos de carácter personal que, se insiste, alcanzan incluso datos de carácter económico, ya obtenidos de forma directa, al requerirse información sobre los ingresos salariales del usuario que se registra o concreta su perfil, ya logrados de forma indirecta, a través de preguntas que pueden igualmente reflejar, en cierta medida, la capacidad económica del usuario, bien por su lugar de residencia o de trabajo, sus hábitos, el uso del tiempo libre, el estado civil y la familia, etcétera.

El uso de información personal de manera indebida puede suponer una infracción extrapenal basada en normas tales como la que concierne a la protección de datos de carácter personal, regulada de forma primaria a nivel europeo en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y a nivel nacional, esto es, en el Ordenamiento español, a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Dichas normas, así como las concordantes, establecen sistemas sancionadores a las transgresiones producidas por los encargados de la custodia o tratamiento de los datos y, por tanto, el mal tratamiento o uso de la información obtenida o recibida, puede sancionarse en el plano Administrativo.

Junto con este sistema sancionador extrapenal, sin embargo, también puede tener cabida la sanción penal, básicamente cuando se produce, más allá del uso o custodia indebida de la información, una afectación a la intimidad de las personas que se ven afectadas por las mencionadas conductas. Efectivamente, prescindiendo en este momento de lo relativo a la normativa de protección de datos, nos centraremos en los posibles reproches jurídico-penales frente a los comportamientos invasores de la

[24] SILVA ESQUINAS, A., FONSECA DÍAZ, A., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R. y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia… p. 31.

intimidad, como consecuencia de un mal uso de los datos facilitados por los propios usuarios de las *apps* al tiempo de su registro o concreción y mejora de su perfil en las aplicaciones, pudiendo anticiparse cómo, entre otros posibles comportamientos, hay dos de fácil identificación que se concretan en el eventual uso inadecuado de los datos: uno, el posible uso indebido de la información para fines de *big data*; otro, a menor escala, la posible revelación de datos que afectan a la intimidad de un usuario concreto.

Las anteriores acciones pueden identificarse en el Código Penal español en los apartados 4 a 6 del artículo 197, precepto contenido en el Capítulo I (*"Del descubrimiento y revelación de secretos"*), del Título X (*"Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio"*), dentro del Libro II (*"Delitos y sus formas"*). Por lo que se refiere a la intimidad como interés jurídico digno de protección, simplemente señalar, además de su condición como derecho fundamental, que presenta dos caras o vertientes, una positiva y otra negativa; la positiva hace alusión al derecho de cada persona a conocer y llevar a cabo el control los datos que afectan a la personalidad y al ámbito familiar que se hallen en poder de terceras personas, y la negativa, referida al derecho de excluir a terceras personas del conocimiento del ámbito personal[25].

El artículo 197.4 de la norma penal sustantiva, consiste en un tipo agravado de acceso y revelación de la información que atañe a la intimidad de la persona, sancionándose con mayor pena que el tipo básico de acceso a información secreta, cuando el mismo se lleva a cabo *"…por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros…"*, o cuando se hace en orden a una utilización de la información *"…no autorizada de datos personales de la víctima"*. Dicho agravamiento en el acceso a los datos que conforman la intimidad de los usuarios, viene marcado, por tanto, bien por razón del sujeto activo, bien por el uso no autorizado de la información. Por su parte, por lo que se refiere a la transmisión de la información obtenida o que se posee, el precepto prevé igualmente una forma agravada con respecto al tipo básico de revelación de secretos cuando efectivamente tienen lugar igualmente actos de difusión, cesión o revelación a terceros, por quienes resultan ser los encargados o responsables de la información o cuando por los mismos se hace un uso no autorizado de la misma.

Trasladada la cuestión al ámbito de las *apps* afectivo-sexuales, nos situaríamos, pues, en el plano de la entrega de datos por parte de los usuarios de las mismas, con la apriorística finalidad de ser empleados en la búsqueda de afinidades con otros usuarios; datos o información con respecto a los cuales se genera un riesgo de una eventual indebida utilización de los mismos sin consentimiento de su titular, precisamente por quien es responsable de su custodia. Ilícito penal con respecto al cual se ha previsto una

[25] Así lo expone GORJÓN BARRANCO, Mª.C., "Descubrimiento y revelación de secretos", en Armendáriz León, C. (dir.), Bustos Rubio, M. (coord.) y VV.AA., *Parte Especial del Derecho Penal a través del sistema de casos*, Tirant lo Blanch, Valencia, 2020, p. 211. Vid. también JORGE BARREIRO, A., "El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP", en *Revista Jurídica Universidad Autónoma de Madrid, núm. 6*, Madrid, 2002, pp. 99-131; SIERRA LOPEZ, M.V., "Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 198", en Del Carpio Delgado, J. (coord.) y AA.VV., *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, Tirant lo Blanch, Valencia, 2018, pp. 133-186.

mayor respuesta punitiva, cuando los datos comprometidos en el comportamiento descrito afectan a la *"ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere menor de edad o una persona discapacitada necesitada de especial protección"* (art. 197.5 CP) y, asimismo, cuando *"los hechos se realizan con fines lucrativos"* o, aún más, si afectan a los datos acabados de señalar y median tales fines lucrativos (art. 197.6 CP).

Efectivamente, como ya se expresara en el análisis jurídico de los principales riesgos que existen para usuarios de las *apps* afectivo-sexuales de la "*Generación Millenials*"[26], los datos que facilitan los consumidores de estas aplicaciones pueden afectar, entre otros aspectos, a su salud, ideologías y vida personal y familiar, sin que, por el contrario, en muchas ocasiones los usuarios puedan limitar a quiénes y con qué finalidad van dirigidos esos datos. Riesgo constatado en el estudio publicado por el Parlamento Europeo en 2018[27], el que se advierten los riesgos de privacidad en las plataformas de citas en línea, incluyendo eventuales comportamientos indebidos en materia de *big data* o utilización masiva de datos.

3. LAS APSS Y LA CULTURA DE *COMPLIANCE*.

3.1. La seguridad de las Apps. Escenario para la reflexión y el debate.

Del estudio etnológico realizado en la investigación de las *apps* afectivo-sexuales con respecto a la "*Generación X*", se obtienen algunas conclusiones que apuntan a que las aplicaciones analizadas desde este prisma presentan, expresado con carácter general, una precaria seguridad en algunos aspectos. Como se ha anticipado en líneas anteriores, precisamente la falta de seguridad en las aplicaciones es uno de los principales agentes generadores de la puesta en riesgo o lesión de bienes jurídicos titularidad de los usuarios de las *apps* e, incluso, de titularidad o interés general o carácter supraindividual.

No obstante esta idea, lo cierto es que existen diferencias entre unas y otras aplicaciones, lo que permite también y, en consecuencia, apuntar a que algunas de ellas serían bastantes más seguras que otras. A este respecto, mientras que las debilidades en materia de seguridad en las aplicaciones se comprueban bastante comunes, existen sin embargo diferencias importantes entre unas *apps* y otras en los puntos fuertes de seguridad, lo que genera una opinión positiva de unas sobre otras.

Hecha la anterior precisión, se erigen como ejemplos paradigmáticos de la escasa seguridad que presentan algunas de las aplicaciones estudiadas, desde la absoluta ausencia, en algunos casos, de mecanismos preventivos que habilitan condiciones para que se produzcan situaciones como las descritas en el apartado 2 que precede, como

[26] SILVA ESQUINAS, A., FONSECA DÍAZ, A., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R. y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia… p. 31.

[27] De nuevo, el estudio publicado por Van Der Wilk para el Parlamento Europeo en junio de 2018. Accesible en (último acceso 29-11-2021):
https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

pudiera ser en el caso de comportamientos consistentes en la usurpación de la personalidad, hasta características que hacen que nos hallemos ante espacios en sí mismo inseguros desde el prisma del usuario, como podría ser, entre otros, por lo que se refiere en particular a los delitos patrimoniales y a los delitos contra la intimidad, por la demanda de un amplísimo elenco de datos personales para causar alta y definir el perfil del usuario o establecer su grado de compatibilidad o afinidad con terceros (llegando incluso en algunos casos a preguntarse, se insiste, por datos tales como los ingresos económicos mensuales, las propiedades o vehículos de los que se es titular, o circunstancias relativas al estado civil de familiares).

A los anteriores nichos de inseguridad se unen, de nuevo entre otros, extremos tales como *links* sobre consejos en materia de seguridad obrantes en idiomas distintos al materno del usuario, o un *staff* de seguridad prácticamente inapreciable por los consumidores de las *apps*, llegando a advertirse incluso una forma grave de desviación en el caso de alguna aplicación, en la que pueden interpretarse desde los perfiles de los usuarios y los contenidos que manejan, formas de trabajo sexual, presencia indebida e inapropiada de menores e, incluso, venta de sustancias tóxicas, supuestos en los que la inseguridad puede interpretarse o derivarse de la normalización misma de estas situaciones.

Finalmente, también resulta muy llamativo cómo no se produce un tratamiento igual por sexos o por razón de las ocasiones en las que hombres y mujeres se presentan como víctimas de comportamientos reprochables, en materia de medios para denunciar comportamientos que pueden comprenderse desviados por los usuarios. De este modo, se aprecia en algunos casos la mayor inseguridad para las mujeres sobre los hombres, al preverse que estos tienen más medios de denuncia que aquéllas, dado que, en ocasiones, su capacidad de protección se limita a la mera acción de "bloqueo de la persona", a pesar de ser las que de manera sistemática sufren un mayor número de episodios de acoso o actos de violencia física, verbal o sexual.

Esta falta de seguridad, además de perjudicar directamente a los usuarios de las aplicaciones, también genera perjuicios a las propias entidades propietarias de las mismas. De este modo, a título ilustrativo, podría señalarse cómo la circunstancia de que existan perfiles falsos, redunda negativamente en la reputación de la *app*, causa un daño reputacional, en tanto que los usuarios pasarán a considerarla insegura y de baja calidad, lo que podrá producir un menor número de usuarios. Es por ello que las empresas, tanto por la pérdida económica como por la reputacional, deberían ser las primeras interesadas en mejorar sus niveles de calidad y seguridad.

En todo caso, teniendo en cuenta las conclusiones del estudio etnográfico llevado a cabo en el ámbito del Proyecto "*Enrolla2. Percepciones de seguridad y actitudes de riesgo en individuos pertenecientes a la Generación X vinculadas al uso de aplicaciones informáticas afectivo-sexuales*", parece plausible la existencia de riesgos graves para los usuarios de las mismas y, por consiguiente, imprescindible dotarles de la necesaria seguridad, lo que debe tener lugar empleando como herramienta específica a tal efecto, la cultura preventiva y la ética corporativa por parte de las entidades titulares de las mentadas aplicaciones.

3.2. Acerca de la prevención de los riesgos penales y las *apps*.

Sin ánimo de profundizar en ello en este momento, sí resulta obligado recordar sucintamente, llegado a este punto y en atención a lo expuesto en el anterior subapartado, cómo una de las más importantes novedades del Derecho Penal contemporáneo ha sido la incorporación de la responsabilidad penal de la persona jurídica[28], la cual tiene su reflejo en la norma penal sustantiva española con la reforma del Código Penal de 2010 y la posterior de 2015[29].

Con respecto de este nacimiento de la responsabilidad de la persona jurídica, el *compliance* penal[30] emergió precisamente como respuesta a este nuevo escenario y como forma de reducción de los riesgos y de prevención de la comisión de comportamientos jurídico-penalmente reprochables en el seno de las empresas, todo ello mediante la promoción de la llamada cultura preventiva, esto es, por medio de una cultura ética y de cumplimiento.

Efectivamente, la norma penal sustantiva establece en su artículo 31.bis, apartado 1, el régimen de responsabilidad de la persona jurídica; en su apartado 2, la exoneración o, al menos, atenuación, de dicha responsabilidad, cuando la entidad haya adoptado, antes de la comisión del hecho delictivo *"modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión"*; y, en su apartado 5, cómo deben ser dichos modelos de organización y gestión[31].

En este contexto, todo estudio del alcance del *compliance* penal aplicable a una entidad, como lo son las titulares de las *apps* afectivo-sexuales estudiadas, debe llevarse a cabo desde la óptica de permitir que, *ad intra*, obtengan una mayor visibilidad de su manera de hacer, de la forma de ejercer un control efectivo sobre sus actividades, y de

[28] Sobre la responsabilidad penal de la persona jurídica, Vid., ALMODÓVAR PUIG, B., "La responsabilidad penal de las personas jurídicas", en Liñán Lafuente, A. (coord.) y VV.AA., *Delitos económicos y empresariales*, Dykinson, Madrid, 2020, pp. 83-106; DOPICO GÓMEZ-ALLER, J., "La responsabilidad penal de las personas jurídicas", en De la Mata Barranco, N., Dopico Gómez-Aller, J., Lascuraín Sánchez, J.A. y Nieto Martín, A., *Derecho Penal Económico y de la Empresa*, Dykinson, Madrid, 2018, pp. 129-168; SIMÓN CASTELLANO, P., "Responsabilidad penal de las personas jurídicas, mapa de riesgos y cumplimiento en la empresa", en Simón Castellano, P., Abadías Selma, A. (coords.) y AA.VV, Mapa de Riesgos penales y prevención del delito en la empresa, Bosch-Wolters Kluwer, Madrid, 2020, pp. 31-76.

[29] Vid. notas al pie núm. 13 y 14.

[30] BACIGALUPO ZAPATER, E., *Compliance y Derecho Penal*, Aranzadi, Cizur Menor (Navarra), 2011.

[31] Artículo 31.bis.5 Código Penal español:

"Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:

1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios".

la manera de adoptar soluciones correctas sopesando riesgos legales que pueden producirse a consecuencia de las mismas, logrando, en definitiva, detectar fraudes e incidencias en sus procesos o formas de gestión así como los riesgos de ilícitos penales que pueden producirse en torno a su actividad, tanto en el seno de la entidad, como por terceras personas que se relacionen con la misma; y, por otra parte, que, *ad extra*, el *compliance* penal les sirva de aval ante las Administraciones, autoridades y clientes o usuarios, como sinónimo de compromiso con la legalidad y con las buenas prácticas empresariales.

En todo caso, debe partirse de la idea de que, a falta de una correcta identificación, análisis y estudio de los principales riesgos de *compliance*, no sólo penales sino también extrapenales, no será posible identificar las obligaciones que en materia de prevención de ilícitos deban adoptarse por la empresa. Es por ello que la organización de la misma debería poder determinar con precisión tanto la normativa aplicable a su actividad, como las obligaciones que afectan a cada una de sus áreas u organización, para a continuación poder adoptar las oportunas medidas de control, en orden a mitigar o minorar sus posibilidades de comisión.

Además de lo anterior, la entidad debería realizar una evaluación de riesgos, tanto penales como extrapenales, teniendo en cuenta sus características y circunstancias internas y externas, al objeto de localizar las situaciones de riesgo de *compliance* y las personas que pueden encontrarse expuestas a las mismas.

La eficacia del correspondiente *Plan de Prevención de Riesgos Penales* se hace depender, en todo caso, de la correcta detección y localización de los riegos que se derivan de la actividad de la entidad, del correcto diseño y constante mejora y adaptación a la legalidad de los procesos y los procedimientos reguladores de la actividad de la empresa, así como del funcionamiento a nivel interno de la misma y de sus relaciones con terceros.

En consecuencia, las entidades titulares de las *apps* afectivo-sexuales objeto de estudio, deberían llevar a cabo una correcta medición de los riesgos derivados de su actividad para los usuarios de las mismas, algunos de los cuales se han detallado, y que se producen en el momento actual, según la concreta entidad de que se trate. Tras ese análisis o mapa de riesgos, estas entidades deberían diseñar procedimientos que eliminaran o redujeran al máximo los riesgos presentes, así como establecer formas de control constante de dichos procedimientos, procediendo a su constante adaptación y mejora. Sólo cuando el *compliance program*, esto es, cuando el modelo de organización y de gestión adoptados por las entidades alcanzaran los parámetros definidos en el artículo 31.bis.5 de la norma penal sustantiva, podrían optar a exonerar o, al menos, atenuar, su responsabilidad como persona jurídica, por los ilícitos que pudieran tener lugar en el entorno de su respectiva *app*.

No obstante todo lo indicado, no puede obviarse, de una parte, la limitación que el propio Código Penal establece con respecto de la responsabilidad penal de las personas jurídicas, que no es otro que limitar los delitos por los cuales podría responder directamente la entidad, a título de autor, lo que lleva a excluir, por ejemplo, de entre los delitos abordados en el presente estudio, el de usurpación de estado civil, no atribuible en ningún caso a las entidades titulares de las aplicaciones por no haberse previsto legalmente, a pesar de que dicho delito tenga lugar en su propia aplicación, si

bien por parte de alguno de sus usuarios; imposibilidad de responder penalmente incluso aunque la producción del ilícito acontecido fuera achacable a la entidad por una ineficiencia o insuficiencia de los medios de seguridad implementados y que debieran estar orientados a la eliminación, en este caso, de los riesgos de suplantación de identidad en el entorno de la *app*.

Y, asimismo, de otra parte, tampoco puede obviarse que, para atribuir responsabilidad penal a la persona jurídica, en aquellos casos en los que en atención al delito en particular resultaría posible, sin embargo para ello deberán concurrir los requerimientos del artículo 31.bis.1, esto es, fundamentalmente, que la persona física actuante esté vinculada a la entidad y lo haga en nombre o por cuenta de la empresa, y en beneficio de la misma[32], lo que sin embargo, no suele darse en la casuística analizada en el estudio etnográfico que sirve de base al presente estudio, debiendo concluirse al menos provisionalmente en este momento, al fin, las serias dificultades existentes para achacar responsabilidad penal directa a las empresas titulares de las aplicaciones en caso de no acreditarse debidamente los márgenes legales que le incumben como persona jurídica, en perjuicio de la seguridad de los usuarios de las mismas.

4. CONCLUSIONES.

La inicial conclusión presente trabajo resulta esencialmente del estudio etnográfico realizado en el ámbito del proyecto "*Enrolla2. Percepciones de seguridad y actitudes de riesgo en individuos pertenecientes a la Generación X vinculadas al uso de aplicaciones informáticas afectivo-sexuales*", en virtud del cual parece plausible la existencia de riesgos graves para los usuarios de las mismas y, por consiguiente, imprescindible dotarles de la necesaria seguridad.

De entre estas situaciones de riesgo detectadas, en el presente trabajo se ha procedido a conocer, con respecto a algunas de ellas (el resto quedarán para un posterior estudio), cuál sería su identificación conforme a las previsiones del Código Penal español, para a continuación hacer un breve análisis jurídico-penal de las mismas. En concreto, se ha centrado esta verificación en los comportamientos consistentes en el *Catfish* o la usurpación de identidad, los timos y las acciones de revelación de la intimidad, los cuales, respectivamente, tendrían encaje en las figuras delictivas de usurpación de estado civil (art. 401 CP), estafa (arts. 248 y ss. CP) y descubrimiento y revelación de secreto (arts. 197 y ss. CP), llegándose a la conclusión de que, mientras las estafas y los atentados contra la intimidad son plenamente posibles, identificables con

[32] Artículo 31.bis.1 Código Penal español:
"En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:
a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.
b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso".

el tipo penal, sin embargo no ocurre así plenamente en el caso del delito de creación de una identidad irreal, pues dicho comportamiento sólo sería relevante como delito de usurpación cuando se llevara a cabo por parte de un usuario una suplantación de la identidad de otra persona, con la que cree estar interactuando otro usuario, pero no cuando tiene lugar la creación de una personalidad irreal, figurada, de cara a entablar relación con otros usuarios.

Parece razonable atribuir a las entidades titulares de las aplicaciones una responsabilidad penal por los riesgos que los usuarios de las mismas tienen. Y, de la misma forma, entender que estas empresas podrían quedar exentas o, al menos, atenuar su responsabilidad, cuando tratan de mitigar o reducir al máximo los riesgos que para los usuarios se producen al emplear las *apps*. Con respecto a este último aspecto, parece, en consecuencia, que el fomento de la cultura de la prevención y la ética empresarial se presenta como una de las mejores herramientas al servicio de los intereses tanto de los usuarios como de las propias entidades.

Si embargo, para poder atribuir responsabilidad penal a una persona jurídica titular de una *app*, no basta con verificar que no haya llevado a cabo una eficaz planificación de los riesgos obrantes en su aplicación, al tiempo que una correcta confección de procesos o procedimientos encaminados a la evitación de que dichos riesgos subsistan o se tornen en daños a los usuarios, todo ello de acuerdo con lo previsto en el apartado 5 del artículo 31.bis de la norma penal sustantiva; para que dicha responsabilidad sea achacable a la entidad de que se trate, se hace preciso, por una parte, que el comportamiento indebido observado en la *app* sea identificable con alguna de las figuras delictivas con respecto a las cuales la persona jurídica puede ser responsable y, de otra parte, que una vez lo anterior, concurran los requisitos y circunstancias que se hallan descritas en el apartado 1 del anteriormente citado artículo 31.bis del Código Penal, esto es, esencialmente, que la persona física actuante esté vinculada a la entidad y lo haga en nombre o por cuenta de la empresa, y en beneficio de la misma.

En consecuencia, no resulta claro y por eso cabe preguntarse en qué casos sería posible la responsabilidad penal de las entidades propietarias de las apps afectivo-sexuales, como consecuencia de la omisión de medidas de seguridad para sus usuarios, por las acciones contrarias a la norma jurídico-penal que pudieran llevar a cabo otros usuarios, más allá de ser el contexto en el que se produce el comportamiento de estos sobre aquellos y, tal vez por ello, más allá de un responsable exclusivamente de corte civil frente a las víctimas de estos delitos.

5. BIBLIOGRAFÍA.

- ALMODÓVAR PUIG, B., “La responsabilidad penal de las personas jurídicas”, en Liñán Lafuente, A. (coord.) y VV.AA., *Delitos económicos y empresariales*, Dykinson, Madrid, 2020.
- BACIGALUPO ZAPATER, E., *Compliance y Derecho Penal*, Aranzadi, Cizur Menor (Navarra), 2011.
- CORDERO VERDUGO, R.R., PÉREZ SUÁREZ, J.R. Y SILVA ESQUINAS, A., “La gestión del deseo afectivo-sexual en la crisis de la Covid-19”, en *La vida cotidiana en*

tiempos de la COVID. Una antropología de la pandemia, Del Campo Tejedor, A., (coord.) y AA.VV., Los Libros de la Catarata, Madrid, 2021.

- DÍAZ LÓPEZ, J.A., *El delito de usurpación del estado civil*, Dykinson, Madrid, 2010.
- DOPICO GÓMEZ-ALLER, J., "La responsabilidad penal de las personas jurídicas", en De la Mata Barranco, N., Dopico Gómez-Aller, J., Lascuraín Sánchez, J.A. y Nieto Martín, A., *Derecho Penal Económico y de la Empresa*, Dykinson, Madrid, 2018.
- DOPICO GÓMEZ-ALLER, J., "Estafa y otros fraudes en el ámbito empresarial", en De la Mata Barranco, N., Dopico Gómez-Aller, J., Lascuraín Sánchez, J.A. y Nieto Martín, A., *Derecho Penal Económico y de la Empresa*, Dykinson, Madrid, 2018.
- FERNÁNDEZ SALINERO SAN MARTÍN, M.A., "Tema práctico I: Estafa (arts. 248-251 bis CP)", en Abadías Selma, A., Bustos Rubio, M. (dirs.) y AA.VV., *Temas prácticos para el estudio del Derecho Penal Económico*, Colex, A Coruña, 2020.
- GÓMEZ-JARA DÍEZ, C., *Compliance penal y responsabilidad penal de las personas jurídicas. A propósito de la UNE 19601. Sistemas de Gestión de Compliance Penal*, Aranzadi, Cizur Menor (Navarra), 2020.
- GORJÓN BARRANCO, Mª.C., "Descubrimiento y revelación de secretos", en Armendáriz León, C. (dir.), Bustos Rubio, M. (coord.) y VV.AA., *Parte Especial del Derecho Penal a través del sistema de casos*, Tirant lo Blanch, Valencia, 2020.
- JORGE BARREIRO, A., "El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP", en *Revista Jurídica Universidad Autónoma de Madrid, núm. 6*, Madrid, 2002.
- LIÑÁN LAFUENTE, A., "Capítulo III. Estafas y otras defraudaciones", en Liñán Lafuente, A. (coord.) y VV.AA., *Delitos económicos y empresariales*, Dykinson, Madrid, 2020.
- MÉNDEZ HERNÁNDEZ, M., "Los delitos de violencia de género a través de medios telemáticos", en Ortega Burgos, E., (dir.), Andújar, J., Imbroda B.J., Tuero, J.A., Frago Amada, J.A. (coords.) y AA.VV., Actualidad Penal 2019, Tirant lo Blanch, Valencia, 2019.
- NIETO MARTÍN, A., "Falsedades en la empresa", en De la Mata Barranco, N., Dopico Gómez-Aller, J., Lascuraín Sánchez, J.A. y Nieto Martín, A., *Derecho Penal Económico y de la Empresa*, Dykinson, Madrid, 2018.
- NÚÑEZ CASTAÑO, E., "Los delitos patrimoniales de defraudación (I): estafa, apropiación indebida y administración desleal", en Galán Muñoz, A. y Núñez Castaño, E., Manual de Derecho penal Económico y de la Empresa, 2ª edición, Tirant lo Blanch, Valencia, 2018.
- PAVÓN HERRADÓN, D., "Amenazas y coacciones", en Armendáriz León, C. (dir.), Bustos Rubio, M. (coord.) y AA.VV., *Parte Especial del Derecho Penal a través del sistema de casos*, Tirant lo Blanch, Valencia, 2020.
- PAVÓN HERRADÓN, D., *El delito de falsedad documental societaria*, Bosch-Wolters Kluwer, Madrid, 2016.

- SIERRA LOPEZ, M.V., "Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 198", en Del Carpio Delgado, J. (coord.) y AA.VV., *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, Tirant lo Blanch, Valencia, 2018.
- SILVA ESQUINAS, A., FONSECA DÍAZ, A.R., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R.R. Y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia violeta. Análisis jurídico con perspectiva de género en base a la etnografía del Proyecto Enrolla2", en *Revista Internacional de Derecho Contemporáneo, vol. 74*, Legis Editores, Colombia, 2021.
- SIMÓN CASTELLANO, P., "Responsabilidad penal de las personas jurídicas, mapa de riesgos y cumplimiento en la empresa", en Simón Castellano, P., Abadías Selma, A. (coords.) y AA.VV, Mapa de Riesgos penales y prevención del delito en la empresa, Bosch-Wolters Kluwer, Madrid, 2020.