CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

©***Cadernos de Dereito Actual*** Nº 22. Núm. Ordinario (2023), pp. 232-250
·ISSN 2340-860X - ·ISSNe 2386-5229

Delincuencia y seguridad de las *apps* afectivo-sexuales, con base en la etnografía realizada en el Proyecto Enrolla2

Crime and safety of sexual affective apps, based on the ethnography conducted in the Enrolla2 Project

R. Rebeca Cordero Verdugo[1]
Universidad Europea de Madrid
Jorge Ramiro Pérez Suárez[2]
Universidad Europea de Madrid
David Pavón Herradón[3]
Universidad Europea de Madrid
Antonio Silva Esquinas[4]
Universidad Europea de Madrid

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 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*,

[1] Profesora Titular en Sociología Aplicada de la Universidad Europea de Madrid. Investigadora Principal del Grupo de Conocimiento-Investigación en Problemáticas Sociales de la Universidad Europea de Madrid.
[2] Profesor Titular de Criminología Aplicada a Espacios Digitales de la Universidad Europea de Madrid. Investigador del Grupo de Conocimiento-Investigación en Problemáticas Sociales de la Universidad Europea de Madrid.
[3] Profesor de Derecho Penal y Procesal Penal de la Universidad Europea de Madrid. Investigador del Grupo de Conocimiento-Investigación en Problemáticas Sociales de la Universidad Europea de Madrid.
[4] Antonio Silva Esquinas, Profesor Adjunto en Criminología de la Universidad Europea de Madrid. Investigador del Grupo de Conocimiento-Investigación en Problemáticas Sociales de la Universidad Europea de Madrid.

Recibido: 27/03/2023
Aceptado: 13/10/2023
DOI: 10.5281/zenodo.10156520

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, especialmente llamativo en el caso de la revelación de la intimidad- y, asimismo, incentivar la cultura de la prevención o *compliance* con respecto a las entidades propietarias de dichas plataformas. Precisamente por ello, en esta ocasión[5] se hará especial hincapié en este último aspecto, la responsabilidad de la persona jurídica, la Ética Empresarial, los *Compliance Program* y la Inteligencia Artificial.

Palabras clave: Etnografía digital, aplicaciones afectivo-sexuales y revelación de la intimidad, responsabilidad de la persona jurídica, Ética Empresarial, *Compliance* e Inteligencia Artificial.

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, especially striking in the case of the revelation of intimacy- and, likewise, encourage the culture of prevention or compliance with respect to the companies that own said platforms. Precisely for this reason, on this occasion special emphasis will be placed on this last aspect, the responsibility of the legal entity, Business Ethics, the Compliance Program and Artificial Intelligence.

Keywords: Digital ethnography, affective-sexual apps and revelation of intimacy, responsibility of the legal entity, Business Ethics, Compliance and Artificial Intelligence.

1. Introducción

Son varios los estudios que de manera previa al presente se han llevado a cabo dando lugar a diferentes publicaciones[6], en torno a la circunstancia de la proliferación y expansión de las redes sociales que se ha producido en los últimos años y, en particular, de las denominadas *apps* informáticas afectivo-sexuales.

Estas aplicaciones son, sin duda, una nueva forma de comunicación e interacción de las personas, con todo lo positivo que ello conlleva, pero de igual manera, se han convertido en un nuevo ámbito o contexto de proliferación de posibles delitos, aspecto lógicamente negativo.

Acerca de esta problemática, como se ha indicado, se han realizado con carácter previo al presente, algunos análisis jurídicos de los riesgos que pueden tener lugar para los usuarios de estas plataformas de contacto y, de la misma forma,

[5] Algunas partes de este trabajo ya han sido previamente publicadas.

[6] 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. PAVÓN HERRADÓN, D., SILVA ESQUINAS, A., PÉREZ SUÁREZ, J.R., CORDERO VERDUGO, R.R., FONSECA DÍAZ, A.R., "Victimización de los usuarios de las aplicaciones afectivo-sexuales y cultura de compliance", en *Revista Vox Juris, vol. 41, núm. 2*, Universidad San Martín de Porres, Perú, 2023.

algunos análisis relacionados con las principales figuras delictivas que se producen en ciertas redes sociales, todo ello fruto de la observación y análisis llevados a cabo en los proyectos "*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 Madrid (con el código Enrolla2 2018/UEM34, financiado por la Universidad Europea)[7], estudio circunscrito hasta usuarios de edad no superior a los 35 años (desde los 18); y "*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)[8], referido en esta ocasión a usuarios con edades superiores a los 36 años y hasta los 50.

Este estudio se complementó con el denominado "*La gestión del deseo en tiempos del COVID* (CIPI/20/159)"[9], 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. Tanto este estudio como el que precede, el relativo a la *Generación X*, se retroalimentan metodológicamente, mediante 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, a través de estos proyectos pone también especial énfasis en el estudio de la seguridad de las *apps*, 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.

El punto de partida de este nuevo medio delictivo es asumir que en el entorno digital tienen lugar o se producen los mismos delitos que en el ámbito analógico. Aún más, ciertamente puede considerarse que en contexto digital tienen lugar con mayor facilidad los delitos que en medio analógico, si se tiene en cuenta el anonimato o falsa sensación de seguridad que la víctima percibe como consecuencia de los filtros que, en apariencia, tienen las aplicaciones[10].

De este modo, son muchas las figuras delictivas identificadas que se producen en el contexto de las aplicaciones informáticas afectivo-sexuales, esencialmente los que tienen que ver con la personalidad, la intimidad personal, la libertad en general y la libertad sexual en particular, lo cual se traduce en delitos tales como: la 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*, *amenazas de violencia (threats of violence)* o estafas.

Como ya se ha tenido ocasión de exponer en estudios previos al presente[11], algunos de estos comportamientos tienen un fácil encaje desde el prisma de la dogmática penal y el Derecho positivo, al identificarse el respectivo comportamiento

[7] En concreto, se analizaron seis *apps* afectivo-sexuales: *Tinder, Grindr, Badoo, Lovoo, Wapa y Wapa* (Silva *et al*, 2018).

[8] En concreto se analizaron cinco *apps* afectivo-sexuales: *Meetic, Pof, Lumen, Wapa y Wapo* (Silva "*et al"*, 2020).

[9] 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.

[10] SILVA ESQUINAS, A., FONSECA DÍAZ, A.R., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R.R. Y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia… cit., p. 6.

[11] PAVÓN HERRADÓN, D., SILVA ESQUINAS, A., PÉREZ SUÁREZ, J.R., CORDERO VERDUGO, R.R., FONSECA DÍAZ, A.R., "Victimización… cit.

con alguna de las figuras delictivas descritas en el Código Penal español. Sin embargo, muchos de esos delitos, entre los que se encuentra, por ejemplo, el de recepción no solicitada de materiales sexualmente explícitos y la pornografía de venganza (*revenge porn*), no tienen sencilla identificación en la norma penal sustantiva, por lo que debe acudirse a figuras clásicas 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[12].

Tal es el avance de estos fenómenos criminales que, incluso, se ha llegado a comprender a tenor de los anteriores comportamientos, la existencia de una nueva forma de violencia de género, llevada a cabo por medio del medio tecnológico en general[13] 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*"[14].

En atención a esta fenomenología, es esencial la labor que han de desempeñar las personas jurídicas propietarias de las aplicaciones. En este sentido, la actividad que gira en torno a las mismas debería reposar sobre los postulados de una correcta ética corporativa, pudiendo incurrir, en todo caso, en responsabilidad penal como consecuencia de los delitos que pudieran producirse en el seno de las mismas por razón de la interacción de los usuarios a través de las mismas.

Precisamente con relación a la posible responsabilidad de la persona jurídica, conviene recordar cómo la misma se introdujo en la norma penal sustantiva[15] introdujo en el año 2010, por medio de la reforma operada por la Ley Orgánica 5/2010[16], la responsabilidad penal de las personas jurídicas, la cual fue objeto de posterior modificación a través de la Ley Orgánica 1/2015[17]. La mencionada regulación tiene su *ratio legis*, en la evitación, en la medida de lo posible, de riesgos para los bienes jurídicos más importantes en el ámbito o contexto de la actividad empresarial, adoptándose este nuevo sistema de responsabilidad, a consecuencia del cual surge 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[18].

Con respecto a todo ello, a nivel internacional existen normas de estandarización y normativización en torno a la conformación de los llamados

---

[12] 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.

[13] 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.

[14] Así se denomina el estudio publicado por Van Der Wilk para el Parlamento Europeo en junio de 2018. Accesible en (último acceso 29-01-2023): https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

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

[16] 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.

[17] 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.

[18] En estos términos ya se expresó en PAVÓN HERRADÓN, D., SILVA ESQUINAS, A., PÉREZ SUÁREZ, J.R., CORDERO VERDUGO, R.R., FONSECA DÍAZ, A.R., "Victimización… cit.

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[19].

2. Aproximación a algunas de las tipologías delictivas observadas en la ciberesfera de las *apps* afectivo-sexuales

De los estudios etnográficos "*Enrolla2 Millenials"* y "*Enrolla2 Generación X"*, se han detectado la concurrencia de ciertos tipos delictivos en las aplicaciones afectivo-sexuales, en ocasiones sin clara respuesta legal por parte de la norma penal sustantiva[20]:

- La recepción no solicitada de materiales sexualmente explícitos y la pornografía de venganza (*revenge porn*):

La recepción no solicitada de materiales sexualmente explícitos es un fenómeno que no presentaría clara respuesta desde la norma penal española, pues no todos los supuestos encajan, entre otros, en el fenómeno del *sexting* no solicitado, cuyo tratamiento se produciría *ex* art. 197.7 CP, protector de la intimidad, ni en el delito de provocación sexual del art. 186[21], este último sistematizado en el Capítulo IV ("De los delitos de exhibicionismo y provocación sexual"), Título VIII ("Delitos contra la libertad sexual").

En todo caso, la ausencia de una específica tipificación de este fenómeno en el caso de mayores de edad requeriría del correspondiente tratamiento jurídico-penal. Debe tenerse en cuenta que, pese a ser habitual la recepción de este tipo de imágenes por los usuarios de las apps afectivo-sexuales, ello no lo convierte en un comportamiento tolerable y, menos aún, tal normalización no lo convierte en una acción que deje de atentar contra concretos intereses dignos de tutela.

Por su parte, la pornografía de venganza consiste en el acceso, uso y difusión de material de naturaleza sexual (contenidos gráficos o videos privados) sin consentimiento o, incluso, sin conocimiento de quien aparece en el mismo.

Se trata de unos comportamientos que quedaría incluidos dentro del grupo de delitos que conciernen a la intimidad de la persona[22], concretamente, en el art. 197.7, dentro del 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") CP.

- *Creepshots, Upskirting, digital voyeurism:*

Se incluye en este fenómeno *Creepshots* la toma de fotografías o vídeos sexualizados o de las áreas privadas de la persona sin su consentimiento, compartiéndolo posteriormente en línea.

El denominado *upskirting* se refiere a la acción por la que una persona realiza una fotografía por debajo de la ropa de una persona (una falda) sin su permiso,

[19] 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.

[20] En lo sucesivo, SILVA ESQUINAS, A., FONSECA DÍAZ, A.R., PAVÓN HERRADÓN, D., CORDERO VERDUGO, R.R. Y PÉREZ SUÁREZ, J.R., "Ciberdelincuencia… cit., y PAVÓN HERRADÓN, D., SILVA ESQUINAS, A., PÉREZ SUÁREZ, J.R., CORDERO VERDUGO, R.R., FONSECA DÍAZ, A.R., "Victimización… cit.

[21] *Vid.* PAÍNO RODRÍGUEZ, F.J., "Delitos de exhibicionismo y provocación sexual, delitos relativos a la prostitución y explotación sexual, y corrupción de menores", 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, pp. 179 y ss.

[22] *Vid.* 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, pp. 211 y ss.

estando recogido específicamente como delito en Inglaterra y Gales, no tanto así en el modelo español, tal y como desarrollaremos a continuación.

El voyerismo digital consiste en la práctica de observar en el entorno virtual a otras personas involucradas en conductas íntimas u acciones que generalmente se consideran de naturaleza privada.

Conforme al Código Penal, se trataría de comportamientos que quedarían incluidos dentro del grupo de delitos que conciernen a la intimidad personal[23], en esta ocasión en los arts. 197.1, 3, 5 y 6 de la norma penal española. La falta de una regulación expresa o singularizada de los anteriores comportamientos, hace que los mismos encajen en la descripción típica general del delito de descubrimiento y revelación de secreto de persona física, contenido en el precitado art. 197.

- *Doxing o doxxing* y *cyber stalking*:

El comportamiento conocido como *doxin*g, se refiere a investigar, manipular y publicar información privada sobre un individuo sin su consentimiento, para exponerle públicamente, avergonzarle e incluso, acceder y atacar a la persona en la vida real, a fin de acosarle o ejercer otros tipos de abuso.

A diferencia del anterior, el *cyber stalking* (acecho u hostigamiento cibernético) es la acción de espiar o recopilar información online sobre una persona y comunicarse con ella en contra de su voluntad. Este tipo de comportamientos se observan fundamentalmente por quien ha sido una pareja íntima.

Todo lo anterior puede resumirse en llevar a cabo una forma de acoso u hostigamiento a través de Internet, que tendría cabida, ante la ausencia de un tipo más específico que regulase este fenómeno delictivo, dentro de delitos contra la libertad[24], como una forma de coacción del art. 172 CP español, o como una forma de coacción del art. 172.ter, ambos ubicados en el Capítulo III ("De las coacciones") del Título IV ("Delitos contra la libertad"), ante la ausencia de un tipo más específico que regulase este fenómeno delictivo[25].

- *Cyber bullying*:

El *cyber bullying* (acoso cibernético, también descrito como *harassment* o acoso), consiste en un comportamiento reiterado en virtud del cual se utiliza contenido textual/escrito o gráfico con el objetivo de asustar y socavar la autoestima o la reputación de una persona.

Estas formas de acoso cibernético no están particularmente protegidas en el CP español como tales, sino que la protección que puede dispensarse frente a dichos comportamientos reside en varios de sus preceptos, aplicables según los casos. A este respecto, debe señalarse cómo por *acoso (harassment)* pueden comprenderse los actos de acoso a través de la ciberesfera más aislados, que atentan no obstante contra la integridad moral de la víctima, mientras que por *cyber bullying*, nos hallamos ante situaciones de acoso continuado en el tiempo entre menores a través de la Red[26]. En todo caso, la integridad moral no es el único interés legal puesto en peligro o lesionado a través de estas formas de acoso, sino que el mismo puede convivir con otros bien diversos, en atención a los concretos comportamientos que hayan sido llevados a cabo por el sujeto activo.

Así, la respuesta punitiva en aras a la protección de los diferentes bienes jurídicos viene dada, según los casos, por las figuras delictivas contenidas en el art.

---

[23] *Ibídem*.

[24] *Vid.* PAVÓN HERRADÓN, D., "Amenazas… cit., pp. 97 y ss.

[25] No obstante, en el Anteproyecto de Ley Orgánica de Garantía Integral de la Libertad Sexual, en tramitación en las Cortes Españolas, está prevista la eliminación de la exigencia de la alteración grave de la vida cotidiana de la víctima como resultado típico. Accesible en: http://www.igualdad.gob.es/Documents/APLOGarantia%20de%20la%20Libertad%20Sexual.pdf

[26] Vid. MIRANDA GONCALVES, R. "La infancia y la adolescencia en la era digital: nuevos retos para la garantía de sus derechos", *Revista Relações Internacionais do Mundo Atual*, v. 4, n. 42, 2023, pp. 465-489.

173.1, párrafo primero, en referencia a la integridad moral como interés a proteger[27], el art. 172 ter, como respuesta a la limitación coactiva de la libertad de la víctima[28], los arts. 169 y 171, también como forma de proteger la libertad del individuo frente a comportamientos catalogables como de amenazas (*ibidem*), el art. 184, cuando se trate de proteger la libertad o indemnidad sexuales de la víctima ante episodios de acoso sexual[29], e incluso el art. 197, cuando pretenda darse cobertura a la intimidad de la víctima, ante una acción tendente al descubrimiento y revelación de secretos de la misma[30] .

- *Catfish o s*uplantación de identidad (*impersonation*):

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*.

En ocasiones, la suplantación de identidad se produce creando una cuenta falsa o perfiles falsos *(catfish)* en estas *apps* afectivo-sexuales, con una identidad de género diferente, para lo que se toman fotos encontradas en la aplicación.

Es el proceso de robar la identidad de una persona para amenazar o intimidar, así como para desacreditar o dañar la reputación de un usuario. Se trata de una figura delictiva contenida en el art. 401 CP español, dentro del Capítulo IV ("De la usurpación del estado civil"), del Título XVIII ("De las falsedades"); por tanto, de un delito de naturaleza falsaria.

- *Hacking* y *cracking*:

Ambos se refieren al acto de interceptar comunicaciones y datos privados, en forma de piratería a través de cámaras web *(hackear* o *crackear*). Teniendo ello presente, el hacking haría referencia a la técnica de acceder a un sistema informático sin la correspondiente autorización, mientras que el *cracking* a las formas de inutilizar sistemas de protección sobre una aplicación informática.

Comenzando por el *hacking*, el Código Penal español dispensaría cobertura protectora a través del art. 197 bis, esto es, se configura, dentro de los delitos de descubrimiento y revelación de secretos[31], como una forma de protección de la intimidad; y lo hace incluyendo dos posibles modalidades de comisión: como aquel llevado a cabo por quien, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo; y mediante la interceptación de transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado.

En cuanto al *craking*, la respuesta penal protectora viene dada por el art. 264, que contiene un tipo específico de daños (conocido como delito de *sabotaje informático*), referidos a los de origen o medio informático, siendo, pues, su naturaleza, en contraste con la del delito de *hacking*, netamente patrimonial y, por

[27] *Vid.* CARUSO FONTÁN, V., "Tortura y otros medios contra la integridad moral", 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, pp. 115 y ss.
[28] PAVÓN HERRADÓN, D., "Amenazas… cit., pp. 97 y ss.
[29] *Vid.* ARMENDÁRIZ LEÓN, C., "Agresión, abuso y acoso sexual", 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, pp. 161 y ss.
[30] GORJÓN BARRANCO, Mª.C., "Descubrimiento… cit., 211 y ss.
[31] *Ibídem.*

consiguiente, no atentatoria de la intimidad de forma directa[32]. Concretamente, la ubicación sistemática del precepto se encuentra dentro del Capítulo IX ("de los daños"), del Título XIII ("De los delitos contra el patrimonio y el orden socioeconómico") del Código Penal.

- *Amenazas de violencia (threats of violence)*:

Las amenazas de violencia (incluidas amenazas de violación, amenazas de muerte, etc.) consisten en el anuncio de un mal futuro ilícito que es posible, impuesto y determinado con la finalidad de causar inquietud o miedo sobre una persona o sus descendientes y familiares. También se incluye la incitación a la violencia física o avisos falsos a servicios de emergencia o policía (*swatting).*

El tratamiento protector que dispensa el Código Penal español en estos supuestos, en cuanto a las amenazas señaladas, es el previsto en los arts. 169 y 171, especialmente en el primero de ellos[33], abordados para el estudio del acoso (*harassment*) y del *cyber bullying*, por lo que habrá de remitirse a lo allí indicado.

- El discurso de odio sexista y el empleo de comentarios sexistas e insultantes:

El discurso de odio sexista se define como expresiones que propagan, incitan, promueven o justifican el odio por motivos de sexo. Este tipo de expresiones son tuteladas, fundamentalmente, en el art. 510.1 CP español[34], dentro de la Sección 1ª ("De los delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizados por la Constitución"), del Capítulo IV ("De los delitos relativos al ejercicio de los derechos fundamentales y libertades públicas"), del Título XXI ("Delitos contra la Constitución").

- Estafas:

En ocasiones se solicita a los usuarios de las *apps* 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 los mencionados estudios etnográficos, 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.

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*

---

[32] *Vid.* PEDREIRA GONZÁLEZ, F.Mª., V., "Daños", 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, pp. 303 y ss.

[33] PAVÓN HERRADÓN, D., "Amenazas… cit., pp. 97 y ss.

[34] RODRÍGUEZ FERRÁNDEZ, S., "El ámbito de aplicación del actual artículo 510 CP en retrospectiva y en prospectiva tras la reforma penal de 2015", en *Revista de Derecho penal y Criminología, 3ª época, núm. 12*, 2014, pp. 165 y ss.

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"[35]. 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.

3. En particular, la revelación de la intimidad o uso indebido de datos que conforman la intimidad del usuario

Como se desprende especialmente del estudio realizado de las *apps* afectivo-sexuales con respecto a la llamada *"Generación X"*, existe un exceso de información que es solicitada a los usuarios de las aplicaciones. Se trata uno de los puntos más controvertidos generador de situaciones de riesgo para importantes intereses y bienes jurídicos de los particulares.

Ello, que tiene lugar especialmente en algunas de estas aplicaciones, supone un traslado de información exagerado, que involucra a sus circunstancias personales y familiares, al igual que, incluso, a sus circunstancias económicas. Se trata de una información solicitada al objeto del establecimiento de afinidades entre usuarios, pero que, a la vista de la importancia cualitativa y cuantitativa de los datos, podría favorecer o incentivar comportamientos atentatorios contra la intimidad y la normativa general sobre protección de datos.

De este modo, podríamos hallarnos en presencia de riesgos para eventuales comportamientos vinculados a la utilización indebida de información en masa de los usuarios o *big data* y, cuando menos, ante el riesgo de una eventual comunicación indebida a terceros de los datos que forman parte de la intimidad de un usuario en particular.

Estos posibles comportamientos quedarían encuadrados esencialmente ante acciones consistentes en 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 en tanto que los mismos han sido voluntariamente entregados por sus titulares. Procede abordar sucintamente por ello el derecho a la intimidad.

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 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"*[36], en torno a la cual es más que evidente el riesgo de utilización indebida por

[35] 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.

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

parte del tenedor de los datos o por parte de terceros que puedan llegar a tener acceso legal o ilegal a los mismos.

Como se ha anticipado, especialmente del estudio etnográfico elaborado con respecto a usuarios de las *apps* afectivo-sexuales pertenecientes a la llamada "*Generación X*", se comprueba que algunas de estas *apps* solicitan a los interesados un importantísimo número de datos de carácter personal que alcanzan incluso datos de carácter económico, los cuales en ocasiones han sido obtenidos de forma directa, mediante la petición de información relacionada con los ingresos y emolumentos salariales del quien se registra o crea su perfil en la aplicación, y en otras ocasiones de manera 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 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[37].

[37] Así lo expone GORJÓN BARRANCO, Mª.C., "Descubrimiento… cit, 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.

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 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*"[38], 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[39], 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.

De este modo, puede comprobarse cómo acontece un cierto margen de inseguridad para los usuarios en las aplicaciones objeto de estudio, bien como consecuencia de la información facilitada, bien por otras circunstancias tales como, por ejemplo, las situaciones ya descritas de usurpación de la personalidad, de atentados contra la intimidad o referentes a posibles estafas. Inseguridades a las que se unen otros extremos, como puede ser los *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[40].

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

[39] De nuevo, el estudio publicado por Van Der Wilk para el Parlamento Europeo en junio de 2018. Accesible en (último acceso 29-01-2023): https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

[40] PAVÓN HERRADÓN, D., SILVA ESQUINAS, A., PÉREZ SUÁREZ, J.R., CORDERO VERDUGO, R.R., FONSECA DÍAZ, A.R., "Victimización… cit.

Existen, pues, razones de política criminal que obligan a detenerse en el estudio de fenómenos como el descrito en el presente apartado, cuyas medidas correctoras pasan por la prevención de estos comportamientos mediante una política y una cultura de *Compliance* en las empresas propietarias de las aplicaciones, como forma de prevenir el delito y eximir la eventual responsabilidad penal que las personas jurídicas deberían asumir como consecuencia de aquellas prácticas de riesgo. Debe tenerse en cuenta, además, que la falta de seguridad señalada en líneas anteriores, no sólo perjudica directamente a los usuarios de las aplicaciones, sino que también conlleva un importante daño reputacional a las propias entidades propietarias de las mismas, con las consiguientes pérdidas económicas, razón por la cual estas entidades están igualmente llamadas a implantar un sistema de prevención de los riesgos penales que pueden concurrir en sus aplicaciones.

4. La responsabilidad penal de las personas jurídicas propietarias de las *apps*. Ética empresarial, *compliance* e inteligencia artificial

De los estudios etnológicos realizados en la investigación de las *apps* afectivo-sexuales con respecto a la "*Generación Millenials"* y la "*Generación X*", especialmente de esta última, se alcanzan algunas conclusiones que tienden a señalar que las aplicaciones analizadas desde este prisma presentan, dicho con carácter general, una precaria seguridad en algunos aspectos.

Como consecuencia de esta ausencia de seguridad en las *apps*, resulta sencillo la generación de ciertos riesgos como los anticipados para los usuarios, muchos de los cuales se comprenden dignos de protección penal, en tanto que afectan a derechos colectivos o supraindividuales esenciales y a derechos individuales de naturaleza fundamental.

No obstante lo indicado, 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[41].

La ausencia de seguridad en estas aplicaciones hace preguntarse acerca de la posible responsabilidad de las entidades propietarias de las mismas. En este sentido, conviene recordar, al menos sucintamente, el régimen de responsabilidad de las personas jurídicas, conforme al Ordenamiento jurídico-penal español, así como los conceptos de Ética Empresarial y *Compliance*, los cuales deben estar presentes en toda actividad empresarial.

Por lo que se refiere a la responsabilidad penal de la persona jurídica[42], la misma se introdujo en el Código Penal español en el año 2010, siendo posteriormente objeto de modificación en el año 2015[43]. Con respecto de este nacimiento de la

[41] En estos términos, *Ibídem.*

[42] 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.

[43] Vid. notas núm. 12 y 13.

responsabilidad de la persona jurídica, el *compliance* penal[44] 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.

De este modo, 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[45].

En este contexto, introduciendo también los conceptos de Ética Empresarial y *Compliance*, en el ámbito de las personas jurídicas se identifican las llamadas "estructuras de gobernanza, gestión de riesgos y *compliance*" (*governance, risk management and compliance*), las cuales permiten el control de la entidad mediante la implantación de acciones que deben regirse, en todo caso, por la ética corporativa, confeccionando mapas de riegos que permiten conocer las actividades generadoras de posibles ilícitos penales y no penales, controlando la observancia en todo momento de la norma que resulte de aplicación, y comprobando el correcto seguimiento de los procedimientos internos igualmente implantados en el contexto de la actividad desarrollada.

De este modo, una gobernanza adecuada supone un traslado correcto y exacto de la información en el seno de la organización, debiendo llegar de este modo a quienes tienen capacidad en la toma de decisiones, lo que debería permitir una ética empresarial adecuada.

Sólo desde este prisma es posible el control de los riesgos que pueden acontecer en la organización y su actividad. Así, es exigible a las empresas una correcta identificación y análisis de los riesgos que pueden comprometer a la organización, para después, con ese conocimiento, tratar de hacer una gestión adecuada de tales riesgos de manera que los niveles de los mismos resulten "aceptables". En este sentido, deben adoptarse políticas internas orientadas, fundamentalmente, a mitigar los riesgos o a prevenirlos, por lo que se puede comprender que una adecuada política de *compliance* supone velar por la observancia de las normas, desde la perspectiva de la ética empresarial, esto es, desde la generación de una cultura de cumplimiento voluntario de las normas internas y externas aplicables a la organización.

---

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

[45] 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".

Los planes de cumplimiento son ideados, por tanto, desde el ética corporativa y con el objetivo de la evitación de ilícitos penales, logrando con ello reducir las posibilidades de sanciones penales, las cuales, como se dice, afectarían a la organización tanto desde el punto de vista reputacional como económico. Modelos de organización y gestión previstos en el antes mencionado artículo 31.bis.5 de la norma penal material.

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 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*.

En todo ello emerge en el momento más actual un factor añadido, cual es el uso de la Inteligencia Artificial, muy presente en las aplicaciones objeto de comentario, en tanto que precisamente son sus algoritmos[46] los responsables de

[46] Igualmente resulta de interés revisar el estudio llevado a cabo con relación a la investigación y los algoritmos, precisamente a propósito de las *apps* afectivo-sexuales y las redes sociales. *Vid*. en este sentido SILVA ESQUINAS, A., CORDEO VERDUGO, R.R., PÉREZ SUÁREZ, J.R. y PAVÓN HERRADÓN, D., "¿Sortear óbices en el campo o aprender de ellos? Una reflexión sobre el impacto de los algoritmos en la investigación criminológica de las *apps* afectivo-sexuales y

poner en contacto a usuarios con perfiles semejantes. Precisamente a propósito de la Inteligencia Artificial o, cuando menos, de los avances tecnológicos, por lo que se refiere al ámbito del Derecho Penal en sentido material, se han generado nuevos escenarios y nuevas formas de criminalidad, en las que respectivamente, se han relacionado y estudiado, de manera primordial, las que tienen que ver, de nuevo, con las redes sociales y las aplicaciones o *apps*, y centrado en figuras delictivas que afectan esencialmente a la intimidad, la libertad sexual, la violencia de género, los menores y el patrimonio.

Todos estos comportamientos son coincidentes con los ya vistos en líneas anteriores, siendo los más paradigmáticos, por ejemplo, a los vinculados a la mencionada violencia de género a través de formas telemáticas de comunicación e interactuación, con una gran amalgama de manifestaciones, como los son las amenazas y las coacciones, el acoso y el *stalking*, los delitos contra la integridad moral y el *cyberbulling*, el *grooming*, la suplantación de identidad, el espionaje y otros delitos contra el honor, *sexting*, las vejaciones e injurias leves e, incluso, los quebrantamientos de condena o medidas de seguridad[47]; o igualmente puede atenderse a los vinculados a la estafa informática, de afectación netamente patrimonial, que recientemente ha sido modificada precisamente al objeto de ampliar su marco regulatorio y adaptarlo a la nueva realidad y fenomenología, diferenciándolo con mayor nitidez si cabe de la llamada estafa clásica.

Pues bien, al igual que para el conjunto de los ciudadanos, el mundo de la economía, de los negocios y de las empresas no se ha visto ajeno a este fenómeno incipiente del uso de las tecnologías y la Inteligencia Artificial, todo ello fruto de lo que ha venido a denominarse la evolución y globalización digital, en las que debemos comprender, respectivamente, *"el desarrollo tecnológico de avanzada, caracterizado por un internet más robusto, móvil y sensores de alta tecnología, combinados con la inteligencia artificial"* y *"en el uso generalizado de la tecnología"*[48]. Se trata de una forma de beneficiarse de la Ciencia que ha sido incorporada al ámbito empresarial, tanto en los procedimientos y procesos productivos, como en productos finales, y tanto *ad intra* como *ad extra*, esto es, tanto en métodos internos de funcionamiento, organización y creación, como en las formas de llevarse a cabo los diferentes negocios jurídicos y relaciones comerciales con terceros; avances tecnológicos e Inteligencia Artificial que, como se dice, de la misma manera, quedan finalmente incorporados a los propios productos y servicios, como lo son las *apps*.

Precisamente, esta nueva realidad hace imprescindible que, al unísono los mentados avances, deban darse unas condiciones jurídicas precisas que permitan proteger los intereses jurídicos en juego, en este caso de los usuarios de las aplicaciones, y que el ámbito de protección de la norma penal alcance también a los comportamientos que pueden sucederse en el contexto empresarial, al igual que viene sucedido en orden con la protección de la persona y sus bienes, a través de los llamados ciberdelitos. Por todo ello, una adecuada política de cumplimiento corporativo por parte de las entidades propietarias de las aplicaciones afectivo-sexuales, al igual que los de otras aplicaciones de diversa naturaleza, debe incluir necesariamente formas de prevención y mitigación de los riesgos penales igualmente con respecto del uso de las distintas formas de Inteligencia Artificial y avances tecnológicos.

---

las redes sociales", en Florit Fernández, C., Del Barrio Fernández, N., Soto Pineda, J.A. (coords.) y VV.AA., *Estudio interdisciplinar de los desafíos planteados por la Agenda 2030*, Thomson Reuters Aranzadi, 1ª edición, Cizur Menor (Navarra), 2022, pp. 439 y ss.

[47] A toda esta fenomenología se ha referido, entre muchos otros, MÉNDEZ HERNÁNDEZ, M., "Los delitos… cit., pp. 471 y ss.

[48] MARTÍNEZ LUNA, W.F., "Tecnologías disruptivas y Derecho. El Smart contract y los retos para la teoría general de los contratos", en Florit Fernández, C., Del Barrio Fernández, N., Soto Pineda, J.A. (coords.) y VV.AA., *Estudio interdisciplinar de los desafíos planteados por la Agenda 2030*, Thomson Reuters Aranzadi, 1ª edición, Cizur Menor (Navarra), 2022, pp. 269 y 270.

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[49], 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.

5. Conclusiones

El presente trabajo, parcialmente publicado, como otros que le precedieron, tiene el punto de arranque, especialmente, aunque no de manera exclusiva, del estudio etnográfico realizado en el marco 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*", de donde se deducen ciertos riesgos para los usuarios de las mencionadas aplicaciones (por tanto, ausencia de concretos márgenes de seguridad), los cuales podrían calificarse de graves, lo que implica la necesidad de dotarles de las oportuna protección desde el prisma del Ordenamiento jurídico-penal.

Como se hiciera en estudios previos, se ha hecho repaso, esta vez sucinto, de la mayoría de las situaciones de riesgo localizadas, tratando de responder a la pregunta de si las mismas hallan acomodo en alguna parte de la norma penal sustantiva española o si, por el contrario, resulta precisa una mayor concreción de estas situaciones en la legislación. De este modo, han sido objeto de mención a la recepción no solicitada de materiales sexualmente explícitos y la pornografía de venganza (*revenge porn*), *creepshots, upskirting, digital voyeurism, doxing o*

[49] 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".

*doxxing, cyber stalking, cyber bullying, s*uplantación de identidad (*impersonation*), *hacking, cracking*, *amenazas de violencia (threats of violence)* o estafas. Finalmente, por su carácter paradigmático en cuento a los riesgos de los usuarios de las *apps*, se hecho especial y separada referencia a la revelación de la intimidad, haciendo acopio de las ideas de trabajos previos acerca de la misma.

Quedan fuera del presente documento otros riesgos detectados en los estudios etnográficos realizados, como lo son la corrupción de menores o el tráfico de drogas, los cuales merecen mayor detenimiento debido a su gran complejidad técnica y circunstancial.

Es lógico que las entidades propietarias de las aplicaciones afectivo-sexuales asuman la responsabilidad frete a los riesgos y, en su caso, ante los delitos que puedan producirse en el contexto de su producto. En este sentido, se hace imprescindible fomentar la cultura preventiva con respecto a los riesgos penales, en pro de la protección de los usuarios de sus aplicaciones. Cultura de la prevención, Ética Empresarial, políticas de *Complance*, imprescindibles tanto por razones de compromiso social, como única forma de evitar las consecuencias indeseables que pudieran derivarse de la apreciación de los ilícitos penales descritos.

De esta manera, el Código Penal español ha articulado formas de prevención del delito, mecanismos gracias a los cuales estas empresas podrían quedar exentas o, al menos, lograr atenuar su responsabilidad, cuando tratan de mitigar o reducir al máximo posible los riesgos que para los usuarios se producen al emplear las *apps*. De esta forma, y como ya se ha tenido oportunidad de concluir en anteriores ocasiones, 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, existen limitaciones claras a la hora de poder atribuir la responsabilidad penal a las entidades titulares de las *apps*; en este sentido, se hace preciso: primeramente, comprobar que haya identificado los riesgos obrantes en su aplicación; en segundo lugar, verificar que se haya dado una eficaz planificación de los riesgos detectados, en orden a su mitigación, eliminación y prevención; tercero, que la entidad haya llevado a efecto y al tiempo, una correcta confección de procesos o procedimientos encaminados a la evitación de que dichos riesgos subsistan o se tornen en daños a los usuarios.

El Código Penal prevé precisamente este mecanismo de exoneración o, cuando menos, de atenuación, en el apartado 5 del artículo 31.bis. De acuerdo con lo descrito en la norma, 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.

Precisamente por estas previsiones legales, no resulta obvia u automática la atribución de responsabilidad a la persona jurídica, de tal suerte que debería profundizarse en el conocimiento de cuándo puede ciertamente atribuirse a la misma tal responsabilidad, esencialmente por una mala política de *Compliance*, esto es, y como también se ha dicho en anteriores ocasiones, 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.

Dificultades mayores si se añade el uso de la Inteligencia Artificial, muy presente en las aplicaciones de contactos, en tanto que precisamente son sus algoritmos los responsables de poner en línea a usuarios con perfiles semejantes. Precisamente, como se ha indicado en el presente estudio, a propósito de la

Inteligencia Artificial o, cuando menos, de los avances tecnológicos, por lo que se refiere al ámbito del Derecho Penal en sentido material, se han generado también nuevos escenarios y nuevas formas de criminalidad, en las que respectivamente, se han relacionado y estudiado, de manera primordial, las que tienen que ver, de nuevo, con las redes sociales y las aplicaciones o *apps*, y centrado en figuras delictivas que afectan esencialmente a la intimidad, la libertad sexual, la violencia de género, los menores y el patrimonio. Nuevo contexto que hará preciso seguir profundizando en conocer la manera en la que la Inteligencia Artificial puede tener sus efectos en la responsabilidad penal de las personas jurídicas propietarias de las aplicaciones que invaden la Red.

6. 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.

ARMENDÁRIZ LEÓN, C., "Agresión, abuso y acoso sexual", 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.

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

CARUSO FONTÁN, V., "Tortura y otros medios contra la integridad moral", 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.

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.

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.

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.

MARTÍNEZ LUNA, W.F., "Tecnologías disruptivas y Derecho. El Smart contract y los retos para la teoría general de los contratos", en Florit Fernández, C., Del Barrio Fernández, N., Soto Pineda, J.A. (coords.) y VV.AA., Estudio interdisciplinar de los desafíos planteados por la Agenda 2030, Thomson Reuters Aranzadi, 1ª edición, Cizur Menor (Navarra), 2022.

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.

MIRANDA GONCALVES, R. "La infancia y la adolescencia en la era digital: nuevos retos para la garantía de sus derechos", *Revista Relações Internacionais do Mundo Atual*, v. 4, n. 42, 2023, pp. 465-489.

PAÍNO RODRÍGUEZ, F.J., "Delitos de exhibicionismo y provocación sexual, delitos relativos a la prostitución y explotación sexual, y corrupción de menores", 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., "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., SILVA ESQUINAS, A., PÉREZ SUÁREZ, J.R., CORDERO VERDUGO, R.R., FONSECA DÍAZ, A.R., "Victimización de los usuarios de las aplicaciones afectivo-sexuales y cultura de compliance", en Revista Vox Juris, vol. 41, núm. 2, Universidad San Martín de Porres, Perú, 2023.

PEDREIRA GONZÁLEZ, F.Mª., V., "Daños", 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.

RODRÍGUEZ FERRÁNDEZ, S., "El ámbito de aplicación del actual artículo 510 CP en retrospectiva y en prospectiva tras la reforma penal de 2015", en Revista de Derecho penal y Criminología, 3ª época, núm. 12, 2014.

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.

SILVA ESQUINAS, A., CORDEO VERDUGO, R.R., PÉREZ SUÁREZ, J.R. y PAVÓN HERRADÓN, D., "¿Sortear óbices en el campo o aprender de ellos? Una reflexión sobre el impacto de los algoritmos en la investigación criminológica de las *apps* afectivo-sexuales y las redes sociales", en Florit Fernández, C., Del Barrio Fernández, N., Soto Pineda, J.A. (coords.) y VV.AA., Estudio interdisciplinar de los desafíos planteados por la Agenda 2030, Thomson Reuters Aranzadi, 1ª edición, Cizur Menor (Navarra), 2022.

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.