

CIBERDATA

**CIBERCRIMEN, DERECHO Y
SOCIEDAD DIGITAL**

CIBERDATA. CIBERCRIMEN, DERECHO Y SOCIEDAD DIGITAL

Nº 1, DICIEMBRE 2025

Edita: Instituto Andaluz Interuniversitario de Criminología, Universidad de Cádiz

Dirección: Mariana N. Solari Merlo

Edición: Noelia Valenzuela García

ISSN-e:

CONTACTO:

seccion.cibercrimen.uca@gmail.com

ENVÍO DE COLABORACIONES:

Se aceptan mini-investigaciones, entrevistas, novedades académicas y noticias.
Normas editoriales y plazos en la web o por correo electrónico.

ÍNDICE

EDITORIAL	4
MINI INVESTIGACIONES	5
Política criminal y cohesión social. <i>Luis Ramón Ruiz Rodríguez</i>	6
Juego inseguro: comprendiendo la victimización sexual en las comunidades digitales relacionadas con videojuegos. <i>Esther Nanclares González, Pablo Romero Seseña y Noemí Pereda Beltrán</i>	10
Posibles modelos de regulación del hacktivismo ético en la legislación es- pañola. <i>María José Rodríguez Mesa</i>	15
Criptomonedas y fraude: estafas de inversión. <i>Patricia Saldaña Taboada</i>	19
Posibles comportamientos delictivos en el happy slapping: una modalidad de ciberbullying. <i>Luis Rodríguez Moro</i>	24
EN PRIMERA PERSONA CON BERNARDINO CORTIJO FERNÁNDEZ	29
JURISDICCIÓN CIBER. CRISTIAN SÁNCHEZ BENÍTEZ	34
ÓRBITA ACADÉMICA	39

Desde la redacción

DRA. MARIANA N. SOLARI MERLO

UNIVERSIDAD DE CÁDIZ - ESPAÑA

ORCID: 0000-0002-7908-722X



Nos es grato presentar Ciberdata, una revista nacida en el seno de la Sección de Cibercrimen y Delitos Tecnológicos del Instituto Andaluz Interuniversitario de Criminología (Sección de Cádiz), integrada a su vez en la Universidad de Cádiz. Su creación responde al deseo de dar visibilidad y continuidad a una línea de trabajo que crece cada día, impulsada por la necesidad de comprender los nuevos retos del mundo digital desde la Criminología y el Derecho penal.

La publicación tiene una vocación divulgativa, pero mantiene la seriedad y el rigor propios del ámbito académico. Pretende acercar el conocimiento especializado a un público amplio — profesionales, investigadores, estudiantes y ciudadanos interesados en la seguridad digital— y mostrar la diversidad de perspectivas que confluyen en el estudio del cibercrimen.

Cada número reunirá distintas secciones que reflejan las facetas complementarias de esta materia. “Mini investigaciones” ofrecerá contribuciones breves de proyectos en curso; “Órbita académica” recogerá noticias, tesis, publicaciones y actividades de interés; otras secciones se alternarán semestralmente. Así, el número de diciembre contará con una entrevista (“En primera persona”) y con el análisis de alguna sentencia de relevancia en este ámbito (“Jurisdicción Ciber”). En junio, estas dos secciones serán sustituidas por el balance del informe anual de cibercriminalidad de España y por el estudio de un caso de actualidad cibercriminal. Con esta estructura, la revista aspira a ser un espacio de encuentro y reflexión, donde se compartan ideas, experiencias y resultados que contribuyan a comprender mejor la realidad del ciberespacio y sus implicaciones sociales y jurídicas.

Más que una simple publicación, esta revista quiere ser una forma de seguir aprendiendo y de construir comunidad, acercando la investigación a la sociedad y dando voz a quienes trabajan cada día por entender y prevenir la criminalidad en los entornos digitales.

Las contribuciones y colaboraciones de investigadores y profesionales serán siempre bienvenidas, así como el envío de noticias, tesis defendidas, publicaciones, programas o actividades de interés que puedan reflejar la vitalidad del ámbito académico y profesional del cibercrimen y la tecnología.

The background of the entire page is a complex, abstract pattern. It features a light beige or cream color with intricate, faint circuit-like lines in a light blue or grey tone. Scattered throughout are various geometric shapes: hexagons of different sizes, some with internal patterns, and concentric circles resembling ripples or fingerprints. There are also small, glowing blue dots and larger, soft blue circular highlights that give the background a sense of depth and technological sophistication.

Mini Investigaciones

POLÍTICA CRIMINAL Y COHESIÓN SOCIAL

LA CIBERDELINCUENCIA COMO PATRÓN

DR. LUIS RAMÓN RUIZ RODRÍGUEZ

UNIVERSIDAD DE CÁDIZ - ESPAÑA

ORCID: 0000-0003-3379-5762



Resumen. El ascenso de la cibercriminalidad a la categoría de los grandes fenómenos de la delincuencia viene impulsada tanto por datos objetivos que verifican esta realidad, como por buenas dosis de sobreactuación que influyen, de manera relevante, sobre el qué, el cómo y el cuánto de la misma. Determinar hasta qué punto la política criminal sobre la delincuencia tecnológica está más relacionada con los fines de protección de bienes jurídicos de relevancia penal que con puros objetivos de cohesión social, constituye uno de los retos más destacados de las venideras transformaciones jurídico penales.

Palabras clave. Ciberdelincuencia, Cohesión social, Política criminal

Abstract. The rise of cybercrime to the category of major criminal phenomena is driven both by objective data that confirm this reality and by a good dose of overacting that significantly influences its nature, scope, and scale. Determining the extent to which criminal policy on technological crime is more closely related to the protection of legally protected interests than to purely social-cohesion objectives is one of the most significant challenges for upcoming criminal-law transformations.

Keywords. Cybercrime, Social cohesion, Criminal policy

Cómo citar: Ruiz Rodríguez, Luis Ramón (2025). "Política criminal y cohesión social". En CiberData, núm. 1, 2025, pp. 6-9. Disponible en:

A lo largo de la Historia, la demonización magnificada de determinados perfiles criminales como la representación del mal absoluto, ha tenido como objetivo, además de luchar contra quienes ponen en riesgo el modelo sociopolítico de cada época, y la protección de los intereses de quienes ostentan posiciones de poder en cada modelo, cohesionar a grupos sociales en torno a enemigos comunes, y, casi siempre, con trazos gruesos, trazos sencillos de confeccionar y divulgar para mantener al grupo unido contra el barbarus.

El crecimiento de las poblaciones humanas y la complejidad derivada del mismo, fue

[illegible]

los demás de manera inasible ha constituido una fantasía difícil de alcanzar para las mayorías sociales de las sociedades expandidas y complejas, quedando reservada durante siglos esa posibilidad a toda clase de detentadores de ese poder político y económico. Por lo tanto, el esfuerzo por imponer poder sobre los demás, extramuros de lo institucional, se ha reservado, casi siempre, a formas de comportamiento calificadas por el poder institucional como delitos o crímenes.

Uno de los condicionantes más relevantes de todos estos modelos ha sido la posibilidad siempre presente, al menos teórica, de ejercer controles preventivos y respuestas post criminales cuyas manifestaciones eran de carácter material sobre los sujetos y sus intereses materiales. El comportamiento con trascendencia en el mundo físico recibía una respuesta en el mismo plano, por sutil que fuese, porque el terreno supra material quedaba reservado al mundo de las creencias, donde las reglas no las escriben ni las imponen los humanos, y si estas tenían impacto en el plano de la realidad, normalmente eran ejecutadas por otros humanos asumiendo un papel de intermediarios para dar consistencia a ese mundo invisible.

Estos cambios representan una oportunidad también para colmar los deseos de tomar parte en el ejercicio del poder, del poder político, del económico y social, y del individual sobre otros a los que, de algún modo, someter a la voluntad personal de cada sujeto. De una u otra manera, se ha percibido con mucha rapidez que la capacidad para ejercer influencia se ha expandido muy por encima de los modelos físicos tradicionales y, lo que es más importante, sin depender necesariamente de seguir los cauces institucionales habilitados por las diferentes estructuras de poder. La capacidad para escapar con más o menos éxito a esos controles ha servido de catapulta para que se expandan y diversifiquen los riesgos de sufrir daño en intereses personales y patrimoniales de primer nivel, pero, también, para que se

Durante todos estos procesos históricos, ejercer poder de forma no infractora sobre

identifiquen otros daños colectivos relacionados con la convivencia y el ejercicio de los derechos fundamentales y las libertades públicas.

Esta dualidad, que, no es nueva, pero, sí se manifiesta de forma distinta, se encuentra en el fondo de los enfoques que, de forma ajustada o magnificada, informan las políticas públicas y las posiciones científicas, incluidas las jurídico científicas, que pretenden afrontar esta realidad cuando se manifiesta en forma de delitos.

Afirmar que los delitos en la red, los crímenes virtuales, la ciberdelincuencia, constituyen un peligro inédito para las sociedades humanas, conlleva parte de razón y bastante de sobreactuación. Lo inédito tiene que ver con el formato y con el volumen o alcance. La sobreactuación con los intereses en juego, la naturaleza de los agresores y la transformación de las reglas del juego en la generación y en la solución de los conflictos.

En efecto, el formato representa lo fundamental de la transformación, y afecta a toda clase de aspectos de lo criminal. No sólo a la cuestión ejecutiva de los hechos delictivos, sino a la interpretación jurídica de los elementos relativos a esa ejecución. La acción típica, el consentimiento, la auto puesta en peligro, el error relevante o la legítima defensa se tienen que ver con nuevas miradas, porque la interacción autor-víctima no sólo es distante, sino que está sometida a nuevos condicionantes relacionados con el desarrollo y práctica de la voluntad, y esto requiere una reformulación y una adaptación constante del proceso interpretativo de la ciencia y la práctica jurídico penal. También el alcance o el volumen son elementos destacables, aspectos que hablan de impacto, pero no de un impacto en la criminalidad, sino de un impacto en toda clase de relaciones e interacciones humanas, donde la criminalidad sólo representa una parte de

ellas. Evaluar el impacto de las tecnologías en la criminalidad no supone sólo comparar el alcance del delito antes y después de su irrupción global, sino medir qué dimensión presenta entre todos los demás ámbitos de las relaciones humanas, porque, de otro modo, el estudio aislado del fenómeno delictivo sólo puede dar espacio al sesgo como mecanismo de análisis de este fenómeno social. Por ello, medir la evolución de la criminalidad en las tres últimas décadas, señalando un incremento creciente imputable a la cibercriminalidad, y que esa realidad llegue a determinar las grandes líneas de la política criminal para el conjunto de la delincuencia, constituye uno de los grandes retos del discurso penal que debe ser objeto de control y crítica.

En el terreno de la sobreactuación, probablemente consecuencia de lo anterior, también se pueden realizar observaciones de cierto interés. Así, en el ámbito de los intereses en juego, de los bienes jurídicos protegidos, si se hace excepción de los propios elementos corpóreos e incorpóreos necesarios para la existencia de la realidad digital, lo cierto es que apenas se han producido novedades a la hora de identificar nuevos objetos necesitados de protección penal. Algo que, no por esperado desde una observación calmada, no deja de tener relevancia para una adecuada aproximación a la ciberdelincuencia. Lo cual implica dos posibles afirmaciones: que la tecnología y la informática aún no, quizá más adelante, han transformado el orden y selección de las necesidades humanas cuya satisfacción deben ser objeto de protección penal, por un lado; y, en segundo lugar, que, en cambio, si han tenido la capacidad de modificar la percepción del impacto y de la peligrosidad que las mismas ejercen en la vida de las personas. Que en el reciente apagón eléctrico general, la primera opción barajada a todos los niveles fuese el ataque cibernético, hasta que ha sido descartado oficialmente, ilustra perfectamente este cambio en la percepción.

Hace décadas, sólo la mala gestión o la calidad de las infraestructuras (o sea, la mala gestión), habría surgido como causa principal, y es más que probable que sea lo que haya pasado. Pero, la cibercriminalidad ya ha pasado al imaginario colectivo, con una fuerte dosis de inducción interesada, al terreno de lo catastrófico, identificándose caos y cibercrimen como un riesgo cierto e inminente, obviando que el caos pueda tener su origen en la propia cibernética. Es decir, se trata de sostener que, como en la delincuencia tradicional del mundo físico, las estructuras sociales, políticas y de poder no causan el delito, sino la voluntad errática de los sujetos que los cometen, al menos para el quehacer jurídico penal.

Estos cambios de percepción también alcanzan a los sujetos participantes en la criminalidad virtual. El ciberdelincuente es presentado como un sujeto capaz, con herramientas formativas y materiales suficientes como para alejarle por completo del perfil del delincuente impulsivo y violento con déficits de control o con carencias vitales y materiales que justificaban un modelo de justicia penal centrado en la prevención general-especial y en la resocialización o reeducación del sujeto. Basta con observar la simbología visual más extendida que se ha creado alrededor del infractor penal en la red para corroborarlo: sujeto varón, encapuchado, con máscara, en un espacio cerrado privado, a oscuras y con tecnología avanzada a su disposición. La representación medieval del mal con formas demoníacas tiene su forma propia en la sociedad del futuro, de modo que, a partir de ahí, acudir a un derecho penal de autor específico para el cibercriminal hay muy poca distancia.

Con todos estos mimbres parece obligado preguntarse si se puede avistar una transformación de las reglas del juego en la generación y en la solución de los conflictos penales, en general, o en los de naturaleza virtual, en particular. No sería ninguna

novedad. La criminalidad económica ya alumbró figuras discutibles como la responsabilidad penal de las personas jurídicas, y la sociedad del riesgo generalizó los delitos de peligro y la expansión de los bienes jurídicos colectivos. Cambios en la figura de la autoría, mediados por el concepto de identidad digital; en la distinción entre peligro y resultado cuando este sólo se produce en el espacio virtual; en la determinación de la voluntad del autor cuando una inteligencia artificial contribuye a la ejecución del delito con aportación propia; o en la necesidad de mantener la pena de prisión como respuesta prioritaria del sistema penal cuando la conexión digital se puede convertir en poco tiempo en el bien jurídico más relevante del que privar a un ser humano, excepción hecha de la propia vida, constituyen retos políticos y jurídicos de primer nivel a los que la ciencia debe anticiparse frente a la impulsividad propia de la respuesta político criminal del día a día.

Son numerosos los retos, y equiparables las posibilidades de extralimitarse por sobreactuación, por lo que resulta imprescindible desarrollar un modelo de respuesta global para la cibercriminalidad que se mantenga dentro del modelo general del sistema penal, porque el derecho penal excepcional ya ha sido objeto de ensayo y consolidación durante años en otros ámbitos, con resultados mayoritariamente negativos para los derechos fundamentales y las libertades pública. Nada permite asegurar, como en otras ocasiones, que no se vayan a cometer errores similares en la búsqueda de la ansiada cohesión social frente al enemigo, pero estar atentos deviene en obligación del especialista, al menos, para que la ingenuidad no sea la nueva excusa con la que enfrentar el desencanto.

JUEGO INSEGURO: COMPRENDIENDO LA VICTIMIZACIÓN SEXUAL EN LAS COMUNIDADES DIGITALES RELACIONADAS CON VIDEOJUEGOS

NANCLARES-GONZÁLEZ, E. ORCID: 0009-0002-5894-1447. UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

ROMERO-SESEÑA, P. ORCID: 0000-0002-2268-3063. UNIVERSIDAD DE BARCELONA

PEREDA-BELTRÁN, N. ORCID: 0000-0001-5329-9323. UNIVERSIDAD DE BARCELONA



Resumen. Esta investigación explora cómo las comunidades digitales relacionadas con videojuegos pueden contribuir a la victimización sexual en línea. Alrededor del 20% de una muestra de 1.812 jugadores adultos en España reportaron haber experimentado este tipo de violencia. Los resultados revelan una asociación entre la victimización sexual y factores sociodemográficos y se identifican patrones de uso y factores de riesgo que aumentan la probabilidad de sufrir estas experiencias. Al visibilizar la violencia digital, se contribuye al diseño de políticas de prevención más efectivas, orientadas a crear comunidades de juego más seguras, inclusivas y responsables.

Palabras clave. Victimización, Videojuegos, Comunidades digitales, Prevalencia, Comportamiento dañino

Abstract. This study explores how digital communities related to video games can contribute to online sexual victimization. Approximately 20% of a sample of 1,812 adult players in Spain reported having experienced this form of violence. The findings reveal an association between sexual victimization and various sociodemographic factors, and identify usage patterns and risk factors that increase the likelihood of encountering such experiences. By making digital violence visible, this research contributes to the design of more effective prevention policies aimed at fostering safer, more inclusive, and more responsible gaming communities.

Keywords. Online gaming, Communities, Prevalence, Harmful behavior

Cómo citar: Nanclares-González, Esther, Romero-Seseña, Pablo, y Pareda-Beltrán, Noemí (2025). "Juego inseguro: comprendiendo la victimización sexual en las comunidades digitales relacionadas con videojuegos". En CiberData, núm. 1, 2025, pp. 10-14. Disponible en:

1. Contexto

La participación en juegos multijugador en línea es una práctica extendida que reúne a múltiples personas en todo el mundo, alrededor de la cual se comparten experiencias y

establecen vínculos sociales. Estos lazos, lejos de ser superficiales, pueden verse afectados por dinámicas problemáticas, como insultos, amenazas, acoso o comportamientos de índole sexual.

Durante años, el foco de la investigación ha estado puesto en los beneficios que acarrea jugar a videojuegos o, por el contrario, en la idea de que consumir videojuegos violentos genera violencia. Sin embargo, otra corriente de investigaciones trata de dilucidar qué factores predisponen a las personas jugadoras a experimentar victimización en los entornos digitales relacionados con videojuegos. En este sentido, los episodios de violencia en línea sufridos por la población jugadora y generados a partir de oportunidades delictivas no son simples anécdotas ni casos aislados, ya que se tratan de dinámicas reales que se desarrollan en el espacio virtual de manera análoga a cómo lo harían en el espacio físico, siguiendo la propuesta de ciberlugar de Miró-Llinares y Johnson (2018). De hecho, como algunos autores establecen, los entornos digitales podrían incluso aumentar las oportunidades para algunos tipos de violencia, como la violencia sexual, a partir de la denominada *technology-facilitated sexual violence* (Henry y Powell, 2018).

Partiendo de este contexto, la presente investigación se centra en avanzar en la comprensión de la victimización sexual acaecida en comunidades digitales de videojuegos, con el fin de identificar los factores individuales, contextuales y conductuales que subyacen a estas interacciones dañinas.

2. El estudio

Para explorar este fenómeno, realizamos una encuesta a 1.812 personas adultas en España que habían jugado a videojuegos en los últimos 12 meses (48,1% varones, 51,2% mujeres; edad media = 38,51 años, desviación típica = 11,96). Esta encuesta, distribuida

entre los meses de julio y septiembre de 2024 mediante una empresa para tal fin, recopila información sobre datos sociodemográficos (6 ítems), hábitos de ocio digital (23 ítems) y experiencias de victimización en línea (6 ítems), con el objetivo de comprender cómo y por qué se producen estas situaciones dentro de las comunidades digitales de videojuegos.

Atendiendo a los datos recopilados, inicialmente describimos las características generales de la muestra con el fin de identificar patrones de prevalencia. Posteriormente, analizamos cómo se relacionaban entre sí las diferentes variables mediante un análisis bivariado y, finalmente, aplicamos un modelo estadístico (regresión logística binaria) para detectar las variables que se asocian con un mayor riesgo de sufrir victimización sexual en línea.

3. ¿Qué hallamos?

3.1. Prevalencias de ocio digital y victimización sexual en línea

Respecto al análisis descriptivo, las personas encuestadas informaron diferentes patrones de uso del ocio digital. Tanto en el ámbito de Internet en general como en las comunidades relacionadas con videojuegos en particular, el consumo de vídeo en diferido fue la categoría más destacada por parte de la muestra; seguida del consumo de vídeo en directo o streaming o jugar a videojuegos ya sea solo o en modo multijugador en línea. Otras actividades como participar en comunidades cerradas, consumir contenido de pago en distintas plataformas o invertir en videojuegos, participar en e-sports y crear contenido de videojuegos para redes sociales, fueron menos comunes, predominando tanto usos ocasionales como la no participación.

En relación con la victimización sexual en línea, encontramos que el 19,6% de la muestra informó haber experimentado al menos un tipo, es decir, una de cada cinco

personas. La forma más común fue la recepción de mensajes sexuales no deseados, siendo una situación que afecta al 16,4% de la muestra. Aunque en algunos contextos esta práctica puede ser normalizada, se trata de un tipo de violencia digital que no debe subestimarse. Lo mismo ocurre con el resto de manifestaciones identificadas, que si bien presentan una menor prevalencia (entre el 4,4% y el 6,5%), también resultan preocupantes: difusión no consentida de contenido sexual; coacción para participar en encuentros o relaciones sexuales no deseadas; amenaza de difundir imágenes íntimas; y presión para enviar contenido de esta índole.

Aunque estas cifras puedan parecer bajas en términos porcentuales, al traducirlas a números absolutos, representan a más de 100 víctimas por cada categoría, poniendo de relieve la diversidad de formas que adopta la violencia sexual en entornos digitales: desde lo más cotidiano y aparentemente inofensivo como un mensaje, hasta la amenaza directa o el chantaje. Y muchas veces, estas conductas están conectadas entre sí, escalando en gravedad.

3.2. Factores de riesgo de sufrir victimización sexual en línea en comunidades digitales relacionadas con videojuegos

Con el fin de conocer las variables que tienen aparejadas un mayor riesgo de ser víctima, los análisis fueron dirigidos a examinar asociaciones existentes. En este sentido, podemos destacar que:

- En relación a los factores sociodemográficos, destacan el género y la edad, pues las mujeres y los jóvenes entre 18 y 25 años reportaron mayor exposición a comportamientos de violencia sexual en línea. Además, destaca especialmente la pertenencia al colectivo LGTBIQ+ como una de las variables más asociadas con ser víctima.

- En relación al ocio digital, destacan la creación de contenido y la participación activa en foros. Además, el riesgo aumenta cuando se juega acompañado de amigos, en comparación a cuando se juega en solitario. Un patrón similar ocurre en el consumo audiovisual, donde visionar contenido sobre videojuegos en directo o diferido presenta un riesgo notablemente mayor que el consumo de contenido general.

- En relación a la exposición de datos personales, quienes comparten su género, orientación sexual, nacionalidad, imagen o voz presentan tasas significativamente mayores de victimización. En cambio, quienes cuidan su privacidad en Internet parecen estar mucho más protegidos frente a estos riesgos.

3.3. Predictores de la victimización sexual en línea en comunidades digitales relacionadas con videojuegos

Desarrollamos un modelo de regresión logística para estimar la probabilidad de ser víctima de violencia sexual en línea, utilizando las variables sociodemográficas y actividades cotidianas como base. El análisis explica el 17,4% de los casos de victimización sexual en línea, es decir, que ciertos comportamientos y características que hemos tenido en cuenta de las personas encuestadas pueden aumentar o disminuir la probabilidad de sufrir este tipo de violencia en entornos digitales. Algunos de los hallazgos más relevantes son:

- Los hombres tienen un 30% menos de probabilidad de ser víctimas que las mujeres.

- Los adultos jóvenes, de entre 18 y 25 años, son más propensos a sufrir este tipo de victimización.

- Las personas que se identifican como parte del colectivo LGTBIQ+ tienen más del doble de probabilidad de sufrir violencia sexual en línea.

- Cuantas más horas se dedican a jugar a videojuegos semanalmente, mayor es el riesgo de sufrir victimización sexual en línea.

- El consumo de contenido digital en diferido aumenta el riesgo de ser víctima en línea, con una probabilidad dos veces mayor.

- Mantener la privacidad o limitar la difusión de datos personales reduce en un 43% la probabilidad de sufrir este tipo de conductas.

4. Conclusiones principales

Los resultados de este estudio nos muestran que la victimización sexual en comunidades digitales relacionadas con videojuegos no es un fenómeno marginal. De hecho, el riesgo se encuentra relacionado principalmente con dos factores. Por un lado, la identidad, donde las mujeres y la comunidad LGTBIQ+ son desproporcionadamente más vulnerables. Esto se puede explicar a través del concepto de sexismo hostil (Glick & Fiske, 1996), que nos ayuda a comprender cómo los roles de género y las actitudes discriminatorias se reproducen en línea, manifestándose en comportamientos dañinos. De hecho, y aunque el presente estudio no aborda el cibersexismo en un sentido amplio, los hallazgos se pueden alinear con dinámicas encontradas en estudios anteriores centrados en explorar las amenazas de agresión sexual, violación o cosificación de las jugadoras (Fox & Potocki, 2015; Fox & Tang, 2017; Scidone et al., 2024).

Y, por otro lado, desde el punto de vista del comportamiento, donde, como hemos comentado, el riesgo de victimización sexual en línea aumenta con la exposición prolongada a estos entornos digitales, ya que este riesgo no depende únicamente de las características personales, sino también de cómo utilizamos estos espacios. Los hallazgos se pueden entender desde el concepto de ciberlugar. Por ejemplo, este explicaría por qué un mayor tiempo de juego o el hecho de

compartir información personal estarían fuertemente relacionados con un mayor riesgo de ser víctima. A su vez, proteger la privacidad se convierte en un factor protector, al reducir significativamente el riesgo de sufrir este tipo de violencia.

Por último, para crear entornos más seguros, es necesario fomentar la alfabetización digital y la sensibilización sobre sexualidad y privacidad en línea. Adicionalmente, implementar herramientas de moderación más robustas en las plataformas, como mecanismos de denuncia más accesibles y códigos de conducta claros, puede ayudar a proteger activamente a las víctimas y grupos vulnerables.

En conclusión, además de aportar información sobre la victimización sexual en línea, resaltamos la necesidad de seguir investigando cómo los entornos digitales afectan a la seguridad de quienes hacen uso de ellos. Adoptar un enfoque integral que incluya prevención, políticas adecuadas y empoderamiento del usuario, es fundamental para reducir los riesgos asociados en las comunidades digitales relacionadas con videojuegos.

Referencias

- Fox, J., & Potocki, B. (2015). Lifetime video game consumption, interpersonal aggression, hostile sexism, and rape myth acceptance: A cultivation perspective. *Journal of Interpersonal Violence*, 31(10), 1912-1931. <https://doi.org/10.1177/0886260515570747>
- Fox, J., & Tang, W. Y. (2017). Women's experiences with general and sexual harassment in online video games: Rumination, organizational responsiveness, withdrawal, and coping strategies. *New Media & Society*, 19(8), 1290-1307. <https://doi.org/10.1177/1461444816635778>
- Glick, P., & Fiske, S. T. (1996). The ambivalent sexism inventory: Differentiating hostile and benevolent sexism. *Journal of Personality and*

Social Psychology, 70(3), 491–512. <https://doi.org/10.1037/0022-3514.70.3.491>

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence & Abuse*, 19(2), 195–208. <https://doi.org/10.1177/1524838016650189>

Miró-Llinares, F., & Johnson, S. D. (2018). Cybercrime and place: Applying environmental criminology to crimes in cyberspace. In G. J. N. Bruinsma, & S. D. Johnson (Eds.), *The Oxford handbook of environmental criminology*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780190279707.013.39>

Scidone, E., Phillips, M. J., & Pantaleo, A. M. (2024). Hiding in the shadows: A qualitative exploration of women gamers identities and perceptions of the video gaming context. *SN Social Sciences*, 4, 181. <https://doi.org/10.1007/s43545-024-00980-z>

Para más información:

Nanclares, E., Romero-Seseña, P. & Pereda, N. (2025). Unsafe Play: Understanding Sexual Victimization in Digital Gaming Communities. *European Journal on Criminal Policy and Research* <https://doi.org/10.1007/s10610-025-09642-z>

Financiación:

La publicación de este trabajo es parte del proyecto GamerVictim, sobre el análisis fenomenológico y victimológico, y respuesta jurídica a las conductas problemáticas en torno a comunidades digitales asociadas a videojuegos, financiado por el PROGRAMA PROMETEO 2023 - CIPROM/2022/332.

POSIBLES MODELOS DE REGULACIÓN DEL HACKTIVISMO ÉTICO EN LA LEGISLACIÓN ESPAÑOLA

DRA. MARÍA JOSÉ RODRÍGUEZ MESA

UNIVERSIDAD DE CÁDIZ - ESPAÑA

ORCID: 0000-0003-4977-9978



Resumen. El hacking ético implica acceder sin autorización a sistemas informáticos con finalidad preventiva, lo que plantea dudas sobre su encaje penal cuando falta consentimiento. Si el bien jurídico protegido es la intimidad, el hacktivismo ético quedaría excluido; si lo es la seguridad de los sistemas, podría exceptuarse. El trabajo analiza la compatibilidad de los modelos bug bounty y CVD con el art. 197 bis CP y propone dos vías regulatorias: exigir dolo específico o introducir una exención penal ligada a protocolos CVD.

Palabras clave. Hacktivismo ético, Intrusismo informático, Seguridad de los sistemas, Bug bounty

Abstract. Ethical hacking involves unauthorized system access for preventive purposes, raising questions about criminal liability when consent is absent. If the protected legal interest is privacy, ethical hacktivism would be excluded; if it is system security, exceptions may be justified. This paper examines the compatibility of bug bounty and CVD models with Article 197 bis of the Spanish Criminal Code and proposes two regulatory approaches: requiring specific criminal intent or introducing an exemption linked to CVD protocols.

Keywords. Ethical hacktivism, Unauthorized computer access, System security, Bug bounty

Cómo citar: Rodríguez Mesa, María José (2025). "Posibles modelos de regulación del hacktivism ético en la legislación española". En CiberData, núm. 1, 2025, pp. 15-18. Disponible en:

El calificativo de ético no neutraliza el hecho de que la conducta nuclear del hacking consista en acceder a un sistema informático vulnerando las medidas de seguridad establecidas originariamente. Esto es, acceder a una red en la que se almacenan y/o circulan datos de naturaleza heterogénea. Dichos datos pueden ser propios de una empresa, como por ejemplo patentes o cartera de clientes, o de un particular; públicos o privados; personales o no personales; etc.

El hacking ético solo se diferencia del hacking “negro” en su finalidad: en el primer caso para alertar sobre posibles fallos o brechas de seguridad; y en el segundo para cualquier otra finalidad que no sea la mencionada, incluida la consistente en el “mero fisgoneo”.

La cuestión que plantea, por tanto, la decisión de legalizar o no el hacking ético es si es suficiente con que se pruebe el elemento subjetivo que lo define, o, en el caso de que la intromisión en el sistema no esté debidamente autorizada por el titular del mismo, el hackeo ha de estar jurídico-penalmente prohibido.

Si se considera que el bien jurídico protegido en el delito de intrusismo informático es la intimidad personal, el hacktivismo ético quedaría excluido del ordenamiento jurídico español, pues en aquellos casos en los que el sistema de información contenga base de datos de terceros, sería precisa la autorización de cada uno de éstos para el acceso al sistema informático. Si es la intimidad personal el bien jurídico vulnerado, tendrán que ser los titulares de los datos, y no el titular del sistema, el que preste la debida autorización.

Es cierto que en la actualidad este problema queda diluido en gran medida debido a las cláusulas genéricas sobre protección de datos en los que de forma previa se autoriza a la compañía al acceso de los datos, y en consecuencia a su autorización para el acceso por parte de un tercero. En estos casos no habría problemas en aquellos casos en los que el acceso se lleva a cabo por parte del personal contratado autorizado para detectar vulnerabilidades o fallas en el sistema. Mayores problemas pueden plantear los modelos de bug bounty o recompensas, y sobre todo el modelo de CVD.

Con respecto al bug bounty, son varias las empresas que ofertan sus servicios en

España. Así, por ejemplo, la plataforma de bug bounty en español DragonJar es un servicio que se encarga de hacer la mediación entre los investigadores de seguridad y las empresas que deciden sacar su programa de recompensas. La plataforma cumple exclusivamente un servicio de mediación, pues el contrato se firma entre la empresa u organización y una comunidad de hackers éticos a fin de que éstos detecten las posibles vulnerabilidades en los sistemas y redes de la empresa. Una vez detectadas las vulnerabilidades se comunican a las empresas para que tomen las medidas necesarias y eviten ataques en el futuro. El valor de la recompensa va a depender de la gravedad de la vulnerabilidad que se haya encontrado.

Si se admite que el acceso debe ser autorizado por la empresa u organismo titular del sistema de información y no por los terceros titulares de los datos, el contrato de la empresa con la comunidad de hackers es ya autorización suficiente para que la conducta no sea típica, por lo que se trata de un modelo compatible con la actual regulación.

A diferencia de lo que ocurre en otros países, en España la Administración Pública no recurre a este tipo de programas, lo que implica que las vulnerabilidades solo puedan ser descubiertas por parte de los empleados o funcionarios encargados de la seguridad de los sistemas. Es de destacar, en este ámbito la experiencia piloto llevada a cabo por la Generalitat de Catalunya que invitó a 15 hackers para llevar a cabo el primer bug bounty de una Administración pública en España. La finalidad, además de la identificar vulnerabilidades en los sistemas de información y prevención de futuros ataques, era la de valorar las posibilidades y riesgos de este tipo programas en el ámbito de la Administración. A pesar del éxito del programa, en el que los hackers colaboraron desinteresadamente, son muchos los

aspectos, principalmente administrativos, que habría que regular para que los programas de bug bounty mediante recompensa pudieran convertirse en una alternativa viable en la Administración Pública.

La rigidez de la normativa sobre contratación de la Administración Pública (oferta pública, delimitación de tareas, precio, determinación de la parte contratista, etc.) es incompatible con la indeterminación de un modelo de bug bounty basado en una recompensa al hacker que detecte la vulnerabilidad cuya cuantía no viene establecida previamente, sino que depende de la gravedad de la vulnerabilidad detectada. Sería preciso, por una parte, crear un tipo de contrato administrativo adecuado a las particularidades del bug bounty; y, por otra, establecer una serie límites, compromisos y prohibiciones a los hackers que participen en el programa, pues no hay que olvidar que se les está dando acceso a sistemas informáticos públicos con datos sensibles y confidenciales, e incluso puede tratarse de sistemas informáticos pertenecientes a infraestructuras críticas.

Por último, y en cuanto a los programas CVD, España es uno de los países que ni siquiera se ha planteado su aplicación. Es más, con la actual redacción del art. 197 bis CP en la que el mero acceso no autorizado es delito, la comunicación de una vulnerabilidad grave por parte de un hacker ético a una empresa u organismo público sería la prueba del acceso ilícito, y por tanto de la comisión del delito. Ello implica que las vulnerabilidades detectadas por los hackers éticos no sean comunicadas o lo sean de forma anónima.

La implantación de un modelo de CVD en España como ocurre en países bajos, EEUU o Japón, exigiría en primer lugar una modificación de la tipificación vigente que, conforme a la posibilidad que deja abierta

tanto el Convenio de Budapest como la Directiva 2014/40/UE, eximiera de responsabilidad penal a los hackers éticos que comuniquen la vulnerabilidad detectada.

No obstante, y antes de analizar los posibles modelos de exención penal, es preciso destacar que ello solo es posible si se admite que el bien jurídico protegido en este delito es la seguridad de los sistemas informáticos y no la intimidad personal ni la privacy. Y ello, porque tanto la intimidad personal como la privacy serían objeto de lesión con el mero acceso no autorizado, y ello con independencia de cuál sea la intención del sujeto activo. Ahora bien, si se entiende que el bien jurídico protegido es la seguridad de los sistemas informáticos, concretado en el caso del art. 197 bis CP en la confidencialidad de los sistemas, aquellas conductas dirigidas a potenciar la seguridad del sistema o de parte del mismo detectando y comunicando posibles vulnerabilidades, no lesionan, sino que contribuyen a la protección del bien jurídico seguridad de los sistemas informáticos, al proteger la confidencialidad de los mismos frente a posibles intromisiones ilícitas.

De considerarse éste el bien jurídico protegido, las alternativas para eximir de responsabilidad penal al hacker ético que actúe amparado por un modelo de CVD son principalmente dos: exigir como elemento subjetivo distinto del dolo la intención de obtener datos u otra intención delictiva; o incluir una cláusula de exención de la responsabilidad penal en aquellos casos en los que se comunique la vulnerabilidad conforme a los protocolos establecidos.

De ambas alternativas, la primera no exige una regulación previa del modelo de CVD, pues la simple ausencia del elemento subjetivo impide que la conducta sea típica. No obstante, y a pesar de ser una solución más simple y que no contradice al Convenio ni a la Directiva, se estaría destipificando el

■ “snooping” o fisgoneo no autorizado de los sistemas.



La segunda alternativa, exige tener previamente un protocolo de CVD, y solo eximiría de responsabilidad penal a quienes detecten y comuniquen la vulnerabilidad conforme al protocolo establecido. La exención, que habría de configurarse como una norma penal en blanco respecto al protocolo CVD, encontraría su fundamento en la ausencia de lesión o puesta en peligro del bien jurídico protegido: la seguridad de los sistemas informáticos.

La adopción de una política CVD incrementa la seguridad de las organizaciones, aunque ello también significa que la organización debe ser capaz de responder a la vulnerabilidad detectada. Una vez implantado en un Estado la política CVD, cualquier organización puede recibir un informe de vulnerabilidad. Sin embargo, cuando no existe una política CVD los reportadores de vulnerabilidades no tienen claro cómo responderá la organización, e incluso si su conducta pudiera ser perseguida como delito, por lo que la reacción esperada de la organización puede influir en el comportamiento de un posible divulgador. Una organización que no está respaldada por una política de CVD puede, por ejemplo, no saber cómo responder o no entender la vulnerabilidad y, por lo tanto, podría decidir ignorarla o negar la existencia de la vulnerabilidad. Incluso pueden malinterpretar las intenciones del divulgador y denunciarlo a la policía.

CRIPTOMONEDAS Y FRAUDE: ESTAFAS DE INVERSIÓN

DRA. PATRICIA SALDAÑA-TABOADA

UNIVERSIDAD DE MÁLAGA - ESPAÑA

ORCID: 0000-0002-9989-7457



Resumen. Las criptomonedas han pasado de ser una innovación en el comercio electrónico a una herramienta para la comisión de delitos. En los últimos años han atraído a criminales que las utilizan para favorecer el desarrollo de estafas de inversión. Estas estafas no dependen solo de la tecnología, sino de estrategias de captación altamente persuasivas, ingeniería social y, más recientemente, el uso de Inteligencia Artificial para crear contenido falso. La prevención debe centrarse en disuadir estos mecanismos de manipulación más que en la prohibición del uso de los cryptoactivos.

Palabras clave. Estafas de inversión, Criptomonedas, Ingeniería social, Esquema piramidal

Abstract. Cryptocurrencies have evolved from being an innovation in e-commerce to a tool for committing crimes. In recent years, they have attracted criminals who use them to facilitate investment scams. These scams rely not only on technology, but also on highly persuasive recruitment strategies, social engineering and, more recently, the use of artificial intelligence to create fake content. Prevention efforts should focus on deterring these manipulation mechanisms rather than prohibiting the use of crypto assets.

Keywords. Investment scams, Cryptocurrencies, Social engineering, Pyramid schemes

Cómo citar: Saldaña-Taboada, Patricia (2025). "Criptomonedas y fraude: estafas de inversión". En CiberData, núm. 1, 2025, pp. 19-23. Disponible en:

1. Las criptomonedas como herramienta para la comisión de ciberdelitos

Las criptomonedas, creadas en 2008 a partir del Bitcoin fueron concebidas como una alternativa descentralizada al sistema bancario tradicional (Nakamoto, 2008). Son monedas virtuales protegidas mediante criptografía, que permiten realizar transacciones entre pares (peer-to-peer) sin intermediarios financieros. Sin embargo, esta descentralización y su anonimato relativo atrajeron la atención de aquellos con motivaciones delictivas.

El punto de inflexión en la vinculación entre criptomonedas y delitos lo marcó la introducción del Bitcoin como forma de pago en el mercado clandestino "Silk Road" (Christin,

2013). Desde entonces, su uso se ha expandido a todo tipo de actividades delictivas: crimen organizado, financiación del terrorismo, y por supuesto, cibercrimen.

2. Estafas cometidas con criptomonedas

En España, preocupa especialmente el uso de criptomonedas en delitos contra el patrimonio como el blanqueo de capitales y, con especial intensidad, las estafas.

Como ocurre en cualquier estafa tipificada en el Código Penal (art.248CP), el núcleo del delito sigue siendo el mismo: engaño con ánimo de lucro para inducir a error a la víctima, que realiza un acto de disposición patrimonial en perjuicio propio o ajeno. Lo que cambia en este caso es el medio: las criptomonedas se convierten en el vehículo idóneo para dar verosimilitud al engaño y dificultar el rastreo posterior de los fondos.

Las tipologías de estafas vinculadas al uso de criptomonedas son variadas y en constante evolución. Uno de los ejemplos son las Rug pull (tirón de alfombra), para la que los estafadores crean tokens, NFT o supuestos proyectos de criptomonedas que prometen elevadas rentabilidades. Atraen capital mediante campañas agresivas, y una vez tienen suficientes fondos, desaparecen sin dejar rastro. Un ejemplo reciente es el caso de la criptomoneda “\$Libra”, promocionada por el presidente argentino Javier Milei (Salvador, 2025). Relacionado con esto se encuentran también los Exit scams o “estafas de salida” en los que el fraude se produce cuando plataformas aparentemente legítimas de compraventa de criptomonedas cesan sus operaciones de forma repentina y desaparecen con los fondos de los usuarios. El caso más paradigmático ha sido el de “Mt.Gox 2” (Ibarra, 2021).

No obstante, las estafas menos sofisticadas y más comunes son las de phishing y suplantación de plataformas legítimas, en las que los atacantes crean páginas web que

imitan servicios reales -billeteras digitales, exchanges o incluso bancos- y atraen a las víctimas con pretextos como premios, alertas de seguridad o supuestas actualizaciones (Ministerio Público Fiscal, 2024). Una vez el usuario introduce sus credenciales, los estafadores acceden a sus fondos y los transfieren a monederos imposibles de rastrear.

3. Estafas de inversión con criptomonedas

Las estafas de inversión merecen una atención especial por su impacto económico y social. El desconocimiento generalizado sobre el funcionamiento de las criptomonedas, sumado a las promesas irreales de rentabilidad, han permitido a los delincuentes construir entramados sofisticados para atraer y engañar a sus víctimas.

De forma general, las estafas de inversión con criptomonedas comienzan con el estafador diseñando una estructura de captación que le permite aproximarse a potenciales víctimas. Una vez establecida la conexión frecuentemente a través de redes sociales, correos electrónicos o incluso conocidos, utiliza un discurso persuasivo sobre las supuestas ventajas de invertir en criptomonedas, atrayendo a la víctima con la promesa de altos rendimientos a medio o largo plazo. Una vez la víctima accede, el delincuente facilita los mecanismos de inversión, bien mediante transferencia de dinero fiduciario, bien directamente en criptomonedas. En muchos casos, se simulan rendimientos falsos a través de plataformas diseñadas para mostrar beneficios inexistentes, lo que incentiva nuevas aportaciones económicas. Cuando la víctima solicita retirar sus fondos o los beneficios prometidos, se le imponen condiciones adicionales (pagos, comisiones, contratación de servicios), o directamente se bloquea el acceso. Finalmente, cuando el estafador percibe que no obtendrá más dinero,

desaparece con el capital recaudado.

En ciertas ocasiones, el fraude evoluciona hacia un esquema piramidal: la víctima, para recuperar su inversión o acceder a beneficios, debe captar a nuevos participantes. Las ganancias aparentes de los primeros miembros se nutren de los fondos de los últimos, en un ciclo que se sostiene hasta el colapso del sistema. Aunque se trata de una metodología clásica, la irrupción de las criptomonedas ha facilitado su expansión global. Un ejemplo paradigmático de este delito en España es el de la macroestafa “Arbistar” investigada por la Fiscalía de la Audiencia Nacional, que habría recaudado para los estafadores más de 6000 bitcoins (valorados en cerca de 600 millones de euros), afectando a miles de víctimas (Agencia EFE, 2025).

3.1. Mecanismos de captación: del falso bróker al romance virtual

El éxito de este tipo de fraude depende, en gran medida, de los métodos empleados para atraer y convencer a la víctima. La fase de captación es esencial, ya que si no se establece el vínculo de confianza la inversión no llegaría a producirse.

Los delincuentes suelen adoptar roles persuasivos como brókeres expertos, asesores financieros o incluso se valen de conocidos de su entorno. Es común el uso de redes sociales, aplicaciones de mensajería o plataformas de citas para iniciar el contacto. En este sentido, ha aparecido el término Pig butchering (“engorde del cerdo”), que consiste en que, tras una fase de contacto prolongado y aparentemente desinteresado, el estafador establece una relación de confianza con la víctima y una vez se ha generado ese vínculo, se introduce la propuesta de inversión (Acharya & Holz, 2024). Esta modalidad se vincula con las llamadas estafas románticas, que a través de una supuesta relación romántica, aprovechan la intimidad emocional para manipular la

voluntad de la víctima (Cross, 2023).

Especialmente frecuente es la figura del falso bróker, que asegura una alta cualificación técnica y experiencia en inversiones con criptomonedas. A través de este perfil profesional, persuade a la víctima para invertir bajo su intermediación (Agencia EFE, 2023).

3.2. Uso de tecnologías emergentes y manipulación digital

El avance tecnológico ha elevado el nivel de sofisticación de estas estafas. Los delincuentes emplean técnicas de marketing digital para construir una narrativa de éxito e inducir a la inversión. Para ello, crean perfiles falsos en redes sociales, páginas web clonadas y generan material gráfico, desde capturas de pantallas manipuladas hasta vídeos y anuncios falsos. Todo ello para mostrar a las potenciales víctimas los beneficios esperados de una inversión con criptoactivos.

En muchos casos se está observando, fruto de la sofisticación y adaptación de los criminales a las nuevas tecnologías, que se utilizan sistemas de Inteligencia Artificial (IA) para crear contenido falso protagonizado por celebridades nacionales que supuestamente avalan la inversión (Ministerio del Interior, 2025). Se reproducen imágenes, voces y testimonios digitales que inducen a error. Las víctimas, al ver rostros conocidos “recomendando” los criptoactivos, creen estar ante una oportunidad legítima y segura (Ministerio del Interior, 2025).

A través de enlaces disponibles en estos contenidos, se redirige al usuario a páginas web falsas, diseñadas para simular medios de comunicación o casas de cambio reales. En estas páginas se ofrece un vídeo explicativo y se proporcionan contactos para iniciar la inversión (Europa Press, 2024). Además, algunos grupos delictivos llegan a instalar software de control remoto en los dispositivos

de las víctimas, con el que acceden directamente a sus cuentas bancarias o wallets, ampliando el alcance y el daño de la estafa (20minutos, 2023).

4. Conclusiones y recomendaciones

Las estafas de inversión con criptomonedas han crecido de forma significativa, generando pérdidas millonarias y afectando a miles de víctimas, que, en muchos casos, no encuentran mecanismos efectivos de restitución. Las características propias de los cryptoactivos dificultan la recuperación de los fondos y la persecución de los responsables, planteando desafíos para los sistemas de justicia penal y los legisladores.

Más allá del componente tecnológico, el éxito de estas estafas se basa en: estrategias de captación altamente persuasivas, utilización de identidades falsas o manipuladas, explotación emocional de las víctimas y sobre todo, el desconocimiento de los riesgos reales asociados a las inversiones con cryptoactivos. A menudo las criptomonedas no son el medio real de inversión, sino un simple gancho para atraer a la víctima. Por tanto, el foco de la prevención no debe estar únicamente en la regulación de las criptomonedas, sino en disuadir el éxito de los mecanismos de ingeniería social que permiten el fraude, especialmente en aquellos casos sofisticados que utilizan sistemas de Inteligencia Artificial.

5. Referencias

- 20minutos. (2023, noviembre 14). Recuperan más de 10.000 euros estafados con inversiones en criptomonedas. 20 minutos. <https://www.20minutos.es/noticia/5190092/0/recuperan-mas-10000-euros-estafados-con-inversiones-criptomonedas/>
- Acharya, B., & Holz, T. (2024). An Explorative Study of Pig Butchering Scams (Versión 1). arXiv. <https://doi.org/10.48550/ARXIV.2412.15423>
- Agencia EFE. (2023, julio 6). Detenido por estafar 2,5 millones simulando ser bróker de inversión en criptomonedas. 20minutos. <https://www.20minutos.es/noticia/5145017/0/detenido-por-estafar-2-5-millones-simulando-ser-broker-inversion-criptomonedas/>
- Agencia EFE. (2025, mayo 28). La Fiscalía asegura que la estafa con criptomonedas de Arbistar ganó cerca de 600 millones de euros en bitcoins desaparecidos. 20minutos. <https://www.20minutos.es/noticia/5716602/0/criptomonedas-estafa-fiscalia-asegura-arbistar-gano-600-millones-bitcoins-desaparecidos/>
- Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. Proceedings of the 22nd International Conference on World Wide Web, 213-224. <https://doi.org/10.1145/2488388.2488408>
- Cross, C. (2023). Romance baiting, cryptorom and 'pig butchering': An evolutionary step in romance fraud. Current Issues in Criminal Justice, 0(0), 1-13. <https://doi.org/10.1080/10345329.2023.2248670>
- Europa Press. (2024, marzo 18). Aumentan las estafas de criptomonedas con imágenes de famosos españoles como Broncano y Pedroche para robar dinero. Europa Press PortalTIC. <https://www.europapress.es/portaltic/ciberseguridad/noticia-aumentan-estafas-criptomonedas-imagenes-famosos-espanoles-broncano-pedroche-robar-dinero-20240318153142.html>
- Ibarra, J. (2021, julio 3). 7 mayores robos de bitcoin de la historia. CriptoNoticias. <https://www.criptonoticias.com/seguridad-bitcoin/7-mayores-robos-bitcoin-historia/>
- Ministerio del Interior. (2025, abril 7).

■ Detenidas seis personas por estafar más de 19 millones de euros usando inteligencia artificial. <http://platon:10100/opencms/es/detalle/articulo/Detenidas-seis-personas-por-estafar-mas-de-19-millones-de-euros-usando-inteligencia-artificial/>

Ministerio Público Fiscal. (2024, septiembre 25). Dieron de baja y alertan sobre un sitio falso sospechado de captar credenciales de cuentas de la plataforma Binance. <https://www.fiscales.gob.ar/ciberdelincuencia/dieron-de-baja-y-alertan-sobre-un-sitio-falso-sospechado-de-captar-credenciales-de-cuentas-de-la-plataforma-binance/>

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

Salvador, R. (2025, febrero 22). Qué es el «rug pull», y cómo arruinó en 6 horas a 40.000 inversores en la criptomoneda de Milei. La Vanguardia. <https://www.lavanguardia.com/internacional/20250222/10411634/que-es-rug-pull-arruino-inversores-libra-criptomoneda-milei.html>

POSIBLES COMPORTAMIENTOS DELICTIVOS EN EL HAPPY SLAPPING: UNA MODALIDAD DE CIBERBULLYING

DR. LUIS RODRÍGUEZ MORO

UNIVERSIDAD DE CÁDIZ - ESPAÑA

ORCID: 0000-0003-3814-2170



Resumen. Este trabajo analiza las posibles responsabilidades penales de los sujetos que, del modo que sea, participan en la conducta de Ciberbullyng conocida como Happy Slapping, en la que unos sujetos agreden a otro u otros con el objeto de que ello sea grabado con un teléfono móvil y difundido a través de las TICs.

Palabras clave. Happy Slapping, Ciberbullying, ciberacoso escolar, Bullying, Derecho penal

Abstract. This work analyzes the possible criminal responsibilities of subjects who participate in the Cyberbullying conduct known as Happy Slapping, in which some subjects assault another or others with the aim of having it recorded with a mobile phone and disseminated through ICT.

Keywords. Happy Slapping, Ciberbullying, Bullying, Criminal Law

Cómo citar: Rodríguez Moro, Luis (2025). "Posibles comportamientos delictivos en el happy slapping: una modalidad de ciberbullying". En CiberData, núm. 1, 2025, pp. 24-27. Disponible en:

1. Definición de Happy Slapping

La expresión anglosajona Happy Slapping, que podría traducirse “bofetada feliz”, se ha extendido en nuestras fronteras para referirse al comportamiento violento que consiste en la grabación en vídeo (con un teléfono móvil) de todo tipo de agresiones (empujones, golpes, peleas) que, acompañadas de intimidaciones y/o menosprecios, cometen de forma colectiva unos sujetos sobre otros, con la finalidad de compartirlas en redes sociales o en aplicaciones de mensajería instantánea. Al acontecer con más asiduidad en colegios y ambientes estudiantiles, resulta habitual que los sujetos implicados sean menores de edad, tanto los que forman parte de su perpetración como los que la sufren. Constituye una modalidad de acoso que, en su versión más grave, consiste en la filmación, en espacios urbanos alejados del público (patios,

vestuarios, explanadas), de importantes palizas con consecuencias corporales, pero que se efectúan para ser filmadas y difundidas en la red, con el objeto de ganar popularidad y/o ridiculizar más aún a las víctimas, lo que se traduce en consecuencias dañinas añadidas de naturaleza psicológica para estas. Suelen representar el colofón, o algún momento álgido, de un comportamiento generalizado de Bullying que, al ser difundido por las TICs, lo es también de Ciberbullying; dos realidades (en lo físico y en lo digital) que cohabitan en este tipo de comportamientos violentos.

Cierto es que esta realidad también puede acontecer fuera del contexto escolar y de un proceso de Bullying entre menores, eligiendo víctimas desconocidas al azar por pertenecer a algún colectivo concreto, vulnerable o no (mendigos, discapacitados, anarquistas, pijos, homosexuales, trans), aunque con el mismo objetivo de alcanzar reconocimiento con su difusión y, en su caso, generar rechazo hacia ese colectivo de pertenencia.

2. Comportamientos delictivos en el Happy Slapping

Ni el Happy Slapping ni el Bullying ni el Ciberbullying están castigados como realidades delictivas autónomas en el Código Penal, pero algunas de las variadas conductas en las que toman forma serán susceptibles de abarcar algunos tipos penales tradicionales, lo que dependerá del rol y comportamiento desprendido por cada individuo del colectivo acosador. Se pueden diferenciar los delitos cometidos por quienes efectúan la agresión, por quienes la presencian, provocan o jalean, por quienes la graban con sus teléfonos y por quienes la difunden a través de las TICs.

Cuando los autores sean menores de edad, la responsabilidad penal de los que tengan entre 14 y 17 años se dirimirá por la LO 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. Los que no alcancen los 14 años no serán

responsables penales, y solo se les aplicará lo previsto en las normas sobre protección de menores del Código Civil y otras disposiciones vigentes, siendo los padres -de todos ellos- los que asuman la responsabilidad civil derivada de los delitos cometidos.

2.1. Respuesta penal para quien agrede

En los casos más graves en los que se producen “agresiones” se cometerá un delito de lesiones del art. 147.1 o 2 CP, estimando una modalidad u otra en función de si el menoscabo a la integridad corporal o psíquica de la víctima requiera o no objetivamente para su sanidad, además de una primera asistencia facultativa, tratamiento médico y quirúrgico. Se aplicará el tipo agravado del art. 148 si se emplea algún arma u objeto peligroso, se efectúa con ensañamiento, o la víctima es menor de 14 años. Y será otra modalidad de lesiones, la del art. 147.3 CP, si la agresión consiste en golpes o maltratos que no han generado ninguna de las lesiones descritas.

Muy habitual será la comisión de un delito contra la integridad moral del art. 173 CP, si lo que hace el agresor es infligir un “trato degradante” sobre la concreta víctima que sea grave e inequívocamente humillante y vejatorio: como obligarle a soportar que otros le escupan u orinen, a lamer urinarios, a mojarse bajo una ducha o a quedarse desnudo en la calle. Algunas sentencias requieren que el ataque sea insistente y reiterado, pues la sistematización suele ser la que genera ese menoscabo a la integridad moral, aunque cabrían hechos aislados si son especialmente graves y relevantes (SAP Castellón 355/2010, de 21 de octubre). Sin ser un ataque físico contra la persona, podría apreciarse un delito de injurias del art. 208 CP cuando el autor realice acciones o emita expresiones que lesionen la dignidad de la víctima, perjudicando gravemente su reputación o su autoestima: como llamarla bollera o misógino.

Otro delito que podría aplicarse es el de amenazas, de los art. 169 y ss. CP, si lo realizado es amenazar con la causación de un mal a alguno de los bienes y/o derechos de la víctima, debiendo aplicarse una modalidad u otra en función de si son condicionales o no o de si se amenaza con un mal constitutivo de delito o no.

Y podría apreciarse un delito de coacciones del art. 172 CP si, con violencia, se obliga a la víctima a hacer cosas que no quiere o a no hacer las que quiere, si estas no son constitutivas de un trato de degradante.

2.2. Respuesta penal para quien participa en la agresión, pero sin agredir

Se trata de los sujetos que, no efectuando ninguna de las conductas del epígrafe anterior, participan de ese colectivo, de mucha o poca gente, que presencian la agresión, provocan o jalean ataques, se mofan o se ríen de la víctima o simplemente presencian el espectáculo desde la distancia que sea.

Resultará difícil apreciar formas de coautoría en los delitos cometidos por los agresores, pues estos sujetos normalmente no son partícipes de un plan común con el que se agrede, amenaza o inflige un trato degradante, salvo, claro está, se pueda probar que dicho plan existe, esto es, que hay un acuerdo común de realizar esa conducta conjuntamente, repartiéndose actividades: mientras unos empujan o impiden la huida otros agreden. Pero sin ese acuerdo, los que rodean a la víctima no la “agreden”.

Sí es cierto que, según el caso, formando ese corro, apretujándose o empujando, pueden impedir que la víctima huya, obligándole a aguantar algo que no desea. En este sentido, y a título de autoría, a lo sumo, podría apreciarse un delito de coacciones. Aunque se podría argumentar, también según la participación de cada uno, una responsabilidad a título de “cooperador

necesario” o “cómplice” de los delitos que cometen quienes agreden -con las mismas penas o las inferiores en grado que las de los autores, respectivamente-. La “inducción” -con la misma pena que el autor- resultará más complicada de acreditar ya que esta forma de participación requiere que se induzca “de forma directa” a cometer un delito “concreto”, lo que difícilmente se consigue solo presenciando el suceso, gritando o riendo, aun impidiendo la huida de la víctima. Pero no sería descartable si la grabación muestra cómo alguien del colectivo hace surgir una concreta idea en el autor de agredir o degradar de un modo específico que finalmente este último efectúa.

No serán responsables penales los sujetos que, desde la distancia que sea, miran, gritan o ríen.

2.3. Respuesta penal para quien graba

El que solo graba no interviene activamente en la “coejecución” de los delitos que constituyen la agresión a título de coautor. Podría ser, a lo sumo, partícipe (inductor o cooperador, necesario o no) si efectúa alguna de las conductas descritas en el epígrafe anterior: si forma parte de la masa que rodea a la víctima sin dejarle escapatoria o si indica a los agresores qué es lo que concretamente tienen que hacer a la víctima.

Como delito propio, podría considerársele autor de un descubrimiento de secretos del art. 197.1 CP si se dan sus elementos típicos: utilizando artificios de grabación se descubre un secreto de la víctima y se actúa con esa intención.

2.4. Respuesta penal para quien difunde

Normalmente, el sujeto que graba la agresión es el que la difunde a través de las TICs. Sea o no el caso, el que realice esta última acción, podría cometer Doxing (difundir públicamente datos privados del menor con el propósito de intimidar, humillar o amenazar) u Outing (hacer pública

■ su orientación sexual, identidad de género, religión u otra información sensible, sin su consentimiento). Si con la grabación se han obtenido esa clase de secretos, la difusión podría constituir, pues, un delito de revelación de secretos del art. 197.3 CP (SAP Málaga 452/2009, de 16 de septiembre), que lleva una pena más grave que la prevista en el delito de descubrimiento.

También se podría cometer un delito contra la integridad moral si con la difusión se abochorna y ridiculiza a la víctima, lo que se podría conseguir con la simple divulgación del vídeo tal cuál o, más aún, si a este se le añaden referencias o comentarios que resulten más despectivos y ridiculizantes.

Por último, si la víctima ha sido elegida por su adscripción a un grupo determinado (ser mujer, homosexual, extranjero), y si con la difusión de lo grabado a través de las TICs se fomenta o incita al odio, la hostilidad, la discriminación o la violencia contra ese grupo que representa, o contra personas determinadas por su pertenencia a él, se podría aplicar a este difusor de contenidos un delito de odio del art. 510 CP.



En Primera Persona

ENTREVISTA CON BERNARDINO CORTIJO FERNÁNDEZ

POR NOELIA VALENZUELA GARCÍA

UNIVERSIDAD DE CÁDIZ - ESPAÑA

ORCID: 0000-0003-0851-9168



D. Bernardino Cortijo, Doctor en Derecho y Ciberingeniería, matemático e ingeniero civil. Fue Comisario de Policía Nacional y fundador de las Unidades de Ciberdelincuencia, además de representante de España en el Consejo de Europa. Actualmente es Director de Seguridad y Fraude de Telefónica y socio fundador de DACOR Intelligence. Profesor universitario, conferenciante y autor de diversas obras, es una de las figuras más reconocidas en el ámbito de la ciberseguridad y la investigación tecnológica.

P. Durante tu trayectoria en Telefónica, ¿qué tipo de incidentes o brechas de seguridad fueron más difíciles de contener o gestionar? ¿Qué aprendizaje crees que sigue siendo vigente hoy?

R. Lo más importante es tener una visión de riesgos en cada momento para poder priorizar por criticidad. Los intentos de ataque, el robo de datos y el ciberfraude son constantes a diario. No basta con herramientas tecnológicas: los procesos de prevención y control son tan importantes como las herramientas, y también la experiencia del personal experto en cada puesto.

Dado que muchos incidentes implican engaño al usuario, al empleado o al cliente, los casos más complejos son los que facilita el propio usuario sin saberlo. Por ejemplo: si con un simple toque se puede provocar el borrado de un disco, la decisión —inducida por engaño— nos deja poco margen salvo actuar preventivamente con formación y alerta.

También son muy complejos los ataques por persistencia. Sea cual sea la modalidad, cuando los intentos son repetitivos acaban causando brecha. Aquí, las acciones de defensa basadas en ciberinteligencia resultan muy eficaces.

Cada día veo distintos ciberriesgos y ataques, y me sorprende que la mayoría son los mismos de hace una década, aunque ahora cuentan con herramientas más accesibles, facilidad para programar malware e incluso uso de IA que los mejora o agiliza.

P. ¿Cuál dirías que es el mayor punto ciego actual en la seguridad digital de grandes infraestructuras o servicios críticos? ¿Qué está más expuesto de lo que la mayoría imagina?

R. Lo primero es diferenciar el área de la empresa crítica de la que hablamos, porque en todas hay cuestiones de seguridad digital. La más olvidada es la organizativa —gobernanza—. Dependemos de terceras partes (proveedores o incluso administraciones), el famoso “supply chain”, que puede arruinarnos por el mal hacer de un proveedor: es el efecto mariposa.

Luego está la gestión del riesgo y, sobre todo, el apetito de riesgo: el umbral que fijan los responsables para mejorar resultados o cumplir mandatos. Por eso, siempre hay que hacer un mapa de riesgos específico para esa organización y ese momento, y contemplar la gestión de crisis dentro de la gobernanza.

En el plano tecnológico, en grandes empresas industriales con zonas robotizadas o automatizadas, todas las redes de datos deben separarse de las redes informáticas y auditarse por separado, sin parar producción y considerando que es una empresa no crítica. Aquí hay muchos puntos ciegos: segmentaciones IP mal diseñadas, crecimientos sin planificación, híbridos cloud/SOC compartidos, y ofimática/aplicaciones internas basadas en servicios de terceros sin garantías de recuperación (hay que leer los contratos).

También fallan los sistemas internos de operaciones: aplicaciones desarrolladas deprisa que funcionan, pero con errores o puertas falsas y sin desarrollo seguro, pese a que la normativa europea lo exige. Añade la mala gestión de la información sensible: consejos de administración no protegidos, documentos que se pierden o roban, planes comerciales que acaban en la competencia. La solución pasa por un plan de control de la información, formación interna y uso adecuado de la tecnología. Además, NIS2 sanciona conductas irresponsables y DORA regula el sector bancario. Y la IA y los modelos generativos que se están incorporando sin conocimiento ni verificación generarán nuevos puntos ciegos.

Para un atacante, una infraestructura crítica es un laberinto con varias entradas: servicios multimedia, domótica, robótica, accesos de personal, móviles en la red, VPN remotas desde casas u hoteles, conexiones interno-externas.... Los detalles importan: la arquitectura de red debe diseñarse y respetarse, pero donde más vulnerabilidades hay es en los procedimientos. En servicios críticos, las rotaciones de personal, el diseño seguro y el manejo de datos son vitales. Y no pueden faltar revisiones constantes con red teams controlados.

P. La IA ha irrumpido en todos los sectores, también en el delictivo. ¿Qué uso de la IA por parte de atacantes te preocupa especialmente? ¿Y cómo puede aprovecharse desde la defensa?

R. La inmersión en IA por parte de organizaciones y personas sin entender qué implica será un problema inmediato. Se han puesto en manos de todos herramientas espectaculares, pero no se enseña a usarlas ni a comprender sus implicaciones.

Te cuento algo: he hablado con asociaciones que representan a cientos de empresas y miles de ciudadanos. Muchas usan ChatGPT, Perplexity, Arc, Copilot, etc., y les proporcionan datos personales, financieros o de expedientes —a menudo en servicios gratuitos— para que les ayuden en sus trabajos. Eso habla por sí solo.

Además, hoy es fácil programar sin saber programar, así que es sencillo crear rutinas de troyanos o malware que confundan a usuarios e incluso a programas de seguridad, cambiando

código para hacerse invisibles y ampliar alcance. Algunos estarán protegidos, pero muchos no.

En defensa, estamos preparando modelos de IAG y monitorizaciones activas con lenguajes naturales y multimodales (tipo GPT o Gemini) para automatizar decisiones con grandes volúmenes de datos, reglas e instrucciones. Lo clave hoy no es solo detectar, sino automatizar respuestas: cambiar parámetros, limitar IP, restringir conexiones salientes, balancear accesos ante DoS, etc. Un sistema de contramedidas autónomo (o asistido) con todo preconfigurado es posible, parecido a los sistemas expertos clásicos (en un portaviones, por ejemplo, ante un incendio, un humano no procesa todo en segundos; un sistema experto sí).

Esto exige una capa de toma de datos con acceso a todos los sistemas, filtrado y preparación, un modelo IAG/LLM (p. ej., GPT-5, Falcon, Llama), código de eventos de seguridad y una capa operativa (SOAR) integrada con SIEM, IDS, firewalls, GRC, para playbooks y control de incidentes, todo ello auditado (evidencias). Hay plataformas comerciales que lo orquestan, pero hay que adaptarlo a cada caso.

P. ¿Estamos preparados para ataques combinados, como ciberataques coordinados con desinformación o suplantación de identidad mediante deepfakes? ¿Qué brechas ves en la respuesta institucional o empresarial?

R. No creo que estemos preparados; casi siempre los ataques son combinados. En los masivos o indiscriminados, una buena configuración hecha por profesionales y formación reducen más del 75 % de los riesgos.

Pero los casos graves que sufren los ciudadanos —derivados de ataques a empresas que custodian sus datos— sí suelen ser mixtos. El ser humano es el eslabón más débil (y también el más fuerte): puede ser engañado con facilidad, y entonces el sistema queda expuesto.

Por eso, prefiero procedimentar, documentar, formar al personal y a los usuarios, y después monitorizar e implantar modelos sencillos. Las herramientas funcionan y son importantes, pero hay que crear procesos auditables y comprensibles.

P. ¿Qué tipo de perfil profesional falta hoy en los equipos de ciberseguridad? ¿Formamos bien en la dimensión humana, estratégica y ética de la seguridad?

R. Hay técnicos estupendos, con una capacidad bestial, pero son pocos. Es difícil encontrar expertos verdaderos en modelos de seguridad. Dirijo un máster en Ciberdelincuencia centrado en lo investigativo y forense, e incidimos en lo jurídico: 50 % de los contenidos son jurídico-procesales. No solo por su uso en procedimientos, sino para comprender la actividad del ciberdelincuente y cómo operan las organizaciones criminales. No todo vale para todo: como en medicina, un cardiólogo no tiene que saber de psiquiatría.

Otra carencia es la visión global y estratégica. Muchos empresarios contratan a “informática” para diseñar la seguridad, cuando debe hacerlo un experto en ciberseguridad (o seguridad global) y luego tecnología implanta. Ejemplo: hay que saber si un empleado hace entradas remotas un fin de semana sin justificación o descargas masivas: eso debe vigilarlo un experto en seguridad; el responsable de informática facilita la información o automatiza reglas.

La ética es clave: no es postureo. También afecta al empresario o político que usa datos pero no pone medios para protegerlos: eso también es ética.

P. ¿Detectas una desconexión entre el avance técnico y la cultura digital de la población? ¿Qué errores repetimos por falta de alfabetización en seguridad?

R. No lo veo como desconexión, sino como exceso de innovación para todos —dispositivos, comunicaciones rápidas, programas intrusivos, necesidad de usarlos a diario— con muchos riesgos y pocos avances legislativos y operativos: desprotección de la ley en datos (a pesar del GDPR), exceso de necesidad de uso (recordemos el apagón global), administraciones no preparadas, delincuentes muy activos, globalización de comunicaciones y datos.

Hay desconocimiento, sí, pero también exceso de digitalización. Muchas veces obligan a usar sistemas incomprensibles (impuestos por Internet, certificados o firmas electrónicas poco amigables), cuando técnica y organizativamente sería posible hacerlo sencillo. En cambio, impiden ir físicamente o hablar por teléfono con una persona. No estoy en contra de la digitalización —me dedico a ello—, pero no vale todo. La alfabetización no es solo del usuario: también del que pone los sistemas y de la administración. Y esto es global.

P. En términos de coordinación entre entidades privadas, administraciones públicas y cuerpos policiales, ¿dónde ves más debilidades? ¿Qué tipo de cooperación real es posible?

R. Sin trabajo conjunto entre administración y empresas, mal asunto. Y la Policía ya no puede ser independiente: debe trabajar con el ciudadano, la empresa y los técnicos, y estos deben ayudar. También al revés. Hay medidas que pueden tomarse antes de la judicialización para evitar males mayores.

El problema es que muchas veces depende de personas, no de la institución. Existe coordinación entre policías. En su momento fui representante en el Convenio de Ciberdelitos (Consejo de Europa). Hoy casi todos los países lo han incorporado y se ha avanzado más. Europol funciona bien en coordinación operativa. Ahora toca coordinar con la sociedad civil. Hay avances, pero insuficientes. También los órganos judiciales deben mejorar: el ciberespacio va muy rápido y no podemos seguir los plazos de la sociedad del “derecho romano”.

Seamos positivos: todo ha mejorado mucho en esta década. La coordinación y los medios policiales son mejores. Algunas compañías colaboran bien, pero carecen de defensa jurídica a veces; por eso hace falta legislación y aplicación judicial que sostenga esa colaboración.

P. Si mañana tuvieras que diseñar una estrategia nacional urgente contra los riesgos digitales, ¿qué tres prioridades marcarías sin dudar?

R. Sería pretencioso hacerlo solo: hay muchas áreas y se hace con equipo. Pero me mojo.

Debe alinearse con la UE (legislaciones y estándares). Alcance temporal: 5 años, con dos premisas: prevención proactiva (ciberinteligencia y medidas prospectivas) y ciberresiliencia (capacidad de recuperación automática al estado inicial). Ámbito: administración, servicios críticos y regulados, y pymes —algunas críticas—.

Modelo basado en zero trust (“nunca confíes, verifica siempre”) y análisis de riesgos, guardando evidencias y corporación.

Áreas: gobernanza, regulación, sistemas de alta protección (críticos), detección-respuesta, ciberinteligencia y ciberdelito, capacitación y formación, IAG, cooperación nacional e

internacional (empresa-administración), plan de ciudadanía, indicadores y un observatorio de la realidad digital. Priorizaría:

1. Gobernanza digital operativa: CERT nacional; equipos responsables de NIS2, DORA, IA, GDPR, cibercrimen y judicial; procedimientos de desescalado y ejecución; autoridad de ciberresiliencia; estrategia y planes sectoriales de detección-respuesta; gabinete de crisis.
2. Protección de servicios e infraestructuras críticas y suministros.
3. Cibercrimen y seguridad: prospectiva (ciberinteligencia), mecanismos de coordinación y control, seguimiento horizontal y empresas; unidad de IA/IAG.

Y medición, auditorías y ciudadanía (planes de formación).

En mi experiencia, he pasado por Administración, Policía, cibercrimen, gran empresa, ingeniería, consejos y pyme especializada: todas son importantes en la seguridad de un país. Hay que proteger al Estado y a las infraestructuras, pero también a las pymes y al ciudadano, que es el principal afectado.



Jurisdicción Ciber

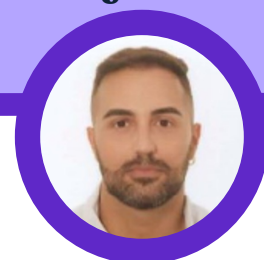
¿Es posible sancionar penalmente en España la difusión de las deepfakes pornográficas?

A propósito de la Sentencia del Juzgado de Menores de Badajoz 86/2024, de 20 de junio

DR. CRISTIAN SÁNCHEZ BENÍTEZ

UNIVERSIDAD DE JAÉN - ESPAÑA

ORCID: 0000-0001-6725-1320



Resumen. En jurisdicción ciber, se analiza cuáles son las posibilidades reales del castigo del Deepfake en España en la actualidad.

Palabras clave. Deepfake, Condena menores, LO protección integral de los menores

Abstract. In cyber jurisdiction, this paper examines the real possibilities for punishing deepfakes in Spain today.

Keywords. Deepfake, Juvenile Sentencing, Comprehensive Protection of Minors Act.

Cómo citar: Sánchez Benítez, Cristian (2025). "¿Es posible sancionar penalmente en España la difusión de las deepfakes pornográficas? A propósito de la Sentencia del Juzgado de Menores de Badajoz 86/2024, de 20 de junio". En CiberData, núm. 1, 2025, pp. 35-38.

En una fecha indeterminada entre los meses de agosto y septiembre de 2023, varios adolescentes –todos menores de edad– de la localidad de Almendralejo (Extremadura) generaron mediante aplicaciones de inteligencia artificial imágenes manipuladas de veinte vecinas de la localidad, también menores de edad, en concreto, de edades comprendidas entre los once y quince años. Para ello, los menores emplearon al menos dos aplicaciones que habían obtenido desde enlaces subidos a la aplicación de mensajería Telegram: clothoff.io y CLF 2 bot. Con estas herramientas, y a partir de fotografías reales de las menores obtenidas en sus perfiles en redes sociales, crearon nuevas imágenes de sus rostros a las que se les superponían imágenes de otros cuerpos femeninos desnudos, “en poses que enfatizaban los órganos sexuales, aparentando de modo realista corresponder a las propias menores” (según se indica en el apartado de Hechos Probados de la resolución objeto de análisis, la cual me facilitó Omar Abdedaim-Herrera). De hecho, según informaciones aparecidas en prensa, cuando las imágenes se difundieron tras compartirlas los menores en dos grupos de WhatsApp, una de las afectadas llegó a jurar a sus padres que no había hecho nada.

A este tipo de imágenes –y vídeos e incluso textos y audios de voz– generadas con herramientas de inteligencia artificial y que aparentan representar a personas, objetos, lugares o sucesos reales, se las conoce como deepfakes. Se trata de un término creado a partir de la unión de los vocablos deep (profundo) y fake (falsificación), y que en castellano puede traducirse como ultrafalsificaciones o ultrasuplantaciones. El prelegislador español de 2025, en la Exposición de Motivos del Proyecto de Ley Orgánica de protección integral de los menores de edad en los entornos digitales, define las ultrafalsificaciones como “imágenes o voces manipuladas tecnológicamente y extremadamente realistas”. La Unión Europea por su parte define el término ultrasuplantación como “un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos” (artículo 3 del Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024).

No ha de pasarse por alto que la totalidad de los autores de las ultrafalsificaciones de Almendralejo eran varones, que todas las víctimas eran mujeres y que las imágenes generadas eran de naturaleza sexual. Ello concuerda con lo revelado por diversos estudios sobre la temática, por cuanto encuentran que la inmensa mayoría de los autores de estos contenidos, casi siempre de naturaleza sexual (asociando cuerpos ficticios, desnudos y/o en poses o contextos de naturaleza sexual a rostros reales), así como de su posterior difusión, son hombres; mientras que más del 90% de las víctimas son mujeres. Estos datos evidencian que este fenómeno es una manifestación clara de violencia digital y sexual de género, sin que ello suponga negar la posibilidad de que entre los autores de estos comportamientos en

algunos casos pueda haber mujeres, de que entre las víctimas pueda haber a veces hombres y de que la naturaleza de los deepfakes no siempre sea sexual (en ocasiones se generan y difunden contenidos de carácter vejatorio); ni se niega la necesidad político-criminal de sancionar estas conductas con independencia del sexo de víctimas y victimarios y del carácter sexual o no de los contenidos.

Retomando el caso, el 20 de junio de 2024, en la Sentencia –de conformidad– 86/2024, el Juzgado de Menores de Badajoz declaró a los menores de Almendralejo (quince) responsables de veinte delitos de trato degradante del artículo 173.1 del Código penal, pues la difusión ocasionó “humillación y desasosiego en las afectadas”; y de veinte delitos de difusión de pornografía infantil del artículo 189 del mismo texto, ya que la totalidad de las víctimas, como se indicó, eran menores de edad. Recuérdese que este último precepto incluye en el concepto de pornografía infantil la conocida entre los especialistas como la pornografía infantil virtual: “imágenes realistas [falsas, en tanto que creadas artificialmente, pero que aparentan ser reales] de un menor participando en una conducta sexualmente explícita o imágenes realistas [ídem] de los órganos sexuales de un menor, con fines principalmente sexuales”.

La magistrada impuso a los menores la medida de libertad vigilada durante un año, “con contenido especialmente orientado a recibir formación afectivo sexual, sobre uso responsable de las tecnologías de la información y la comunicación, sensibilización en materia de igualdad y género, así como intervención en los aspectos deficitarios que presenten los menores, de acuerdo con los respectivos informes del Equipo Técnico”. Asimismo, se decretó en el fallo “la devolución, a cada uno de los menores, de sus terminales móviles previamente formateados o restaurados a

valores de fábrica, quedando así eliminados cualesquiera contenidos o imágenes relativas a las menores perjudicadas, que obtuvieron accediendo de manera irregular, a las aplicaciones referidas en los hechos probados”. También fueron condenados al pago de las costas, pero sorprende sin embargo que no se contenga en la resolución referencia alguna al pago de eventuales responsabilidades civiles derivadas del delito. Desconozco si es que los representantes legales de las perjudicadas declinaron la vía penal para solicitar la reparación civil o si es que directamente renunciaron a dicha reparación.

Por otra parte, en septiembre de 2025 se conoció que la Agencia Española de Protección de Datos había sancionado administrativamente (EXP202503445) a uno de esos menores con una multa de 2.000 euros (que se redujo a 1.200 euros por reconocimiento de responsabilidad y pago voluntario). Y ello porque la difusión por su parte de las imágenes manipuladas con inteligencia artificial, asociando “rostros reales a cuerpos desnudos que no se corresponden”, supuso un tratamiento ilícito de datos personales, “por cuanto la imagen es un dato personal” y porque dicho tratamiento “se efectuó sin que concurriera ninguna de las causas de legitimación enumeradas en el artículo 6.1 del Reglamento General de Protección de Datos”. Quizá con esta segunda sanción a este menor ya condenado con anterioridad por los mismos hechos se infringe el principio non bis in ídem, que prohíbe la doble sanción (incluso cuando una sea de naturaleza penal y otra administrativa) si existe identidad de sujetos, hechos y fundamento sancionador. Un mes después, la Agencia apercibió (EXP202506010) a un niño de trece años que había difundido una deepfake sexual de una menor (aparecía su rostro real asociado a un cuerpo desnudo ajeno), generada a partir de una fotografía real que aquella había publicado en su perfil de Instagram.

De este modo, a día de hoy es posible sancionar penal y administrativamente en España la difusión de deepfakes pornográficas o de contenido vejatorio sin necesidad de emprender modificaciones normativas. Además de las mencionadas sanciones administrativas impuestas por la Agencia Española de Protección de Datos y de los precitados delitos de trato degradante y de pornografía infantil (para cuando las imágenes generadas con inteligencia artificial representen a menores de edad) aplicados por el Juzgado de Menores extremeño, existen otros tipos penales que la doctrina ha llegado a proponer para el castigo de estos comportamientos. Así, se ha planteado la posibilidad de emplear los delitos contra el honor (injurias) y contra la intimidad. Respecto de estos últimos, no resulta adecuada su invocación por la sencilla razón de que no hay imágenes ni intimidad real que proteger en los casos de deepfakes. No hay atentado a la intimidad en la difusión de una ultrafalsificación porque los contenidos difundidos son falsos. En mi opinión, en la medida en que la difusión de deepfakes, por su naturaleza cosificadora, atenta principalmente contra la integridad moral, bien jurídico más amplio y que podría integrar también los ataques contra el honor, es el delito de trato degradante el tipo penal más idóneo para reprimir tales conductas.

Sin embargo, desde marzo de 2025 se tramita en el Congreso de los Diputados el precitado Proyecto de Ley Orgánica para la protección integral de los menores de edad en los entornos digitales, que incluye entre sus novedades la incriminación expresa de la difusión, exhibición o cesión de la imagen corporal o la voz de una persona generados con inteligencia artificial u otras tecnologías, “de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorios”. La creación o la mera posesión de estos contenidos serían penalmente atípicas, salvo que pudieran encuadrarse en el amplísimo delito de pornografía infantil,

siempre y cuando las víctimas de estas ultrafalsificaciones generadas pero no compartidas fuesen menores de edad.

Para tal fin se pretende introducir un nuevo artículo (173 bis), ubicado entre los delitos contra la integridad moral –de hecho, se exige en el delito proyectado que concurra en el autor el ánimo de menoscabar la integridad moral de la víctima–, y que castigaría con la pena de prisión de entre uno y dos años la difusión de estas deepfakes sexuales o gravemente vejatorias; y con la pena en su mitad superior –de un año y medio a dos años– si se hiciera a través de “un medio de comunicación social, por medio de internet o mediante el uso de tecnologías” –lo que suele ocurrir en la mayor parte de los casos–, “de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual”.

Como se ha podido ver en los párrafos anteriores, el ordenamiento jurídico español ya cuenta con varios instrumentos sancionadores (penales y administrativos) perfectamente aplicables a este tipo de supuestos. Así, la concreta tipificación penal de la difusión de las ultrasuplantaciones sexuales o gravemente vejatorias no resultaría necesaria, en la medida en que se cuenta ya con varios tipos penales que pueden utilizarse y que de hecho se han utilizado para su represión. No es que piense que no deban castigarse penalmente comportamientos como los acaecidos en Almendralejo. Son lo suficientemente graves como para invocar al Derecho penal, cuya intervención en tales casos resultará indispensable tanto para prevenir la comisión de hechos análogos como para sancionar contundentemente los ya perpetrados. De lo que se duda aquí es de la conveniencia de crear un nuevo delito expreso de difusión de deepfakes, por resultar innecesario, puesto que puede aplicarse, entre otros, el delito de trato degradante. Un nuevo delito que, adviértase,

se situaría, como aquel, entre los delitos contra la integridad moral y que tendría idéntico límite superior de la pena (dos años). En cualquier caso, habrá que esperar un tiempo –quizá años– para poder constatar si la reforma proyectada, de aprobarse, aunque prescindible por los motivos expuestos, resulta positiva al menos en un sentido preventivo general: en términos de reforzamiento simbólico de un mensaje de intolerancia social-penal frente a hechos como el comentado en la presente contribución.

Créditos:

Este trabajo se ha desarrollado en el marco del Proyecto PROPIMAGENXXI “Protección penal de la imagen frente al chantaje de los nuevos desafíos del siglo XXI: venganzas sexuales, fake news, trampantojos y otros enredos”, financiado por la Agencia Estatal de la Investigación del Ministerio de Ciencia e Innovación del Gobierno de España dentro del Programa de Generación de Conocimiento 2024 (Ref.: PID2024-15934OGB-IOO).

The background is a complex, abstract composition. It features a light beige base with a network of thin, grey circuit-like lines. Overlaid on this are several geometric shapes: a large, central hexagon with a glowing blue and white border, and a cluster of smaller hexagons to its right. Scattered throughout are numerous concentric circles and smaller, solid-colored circles in shades of grey and blue. The overall effect is one of digital connectivity and scientific precision.

Órbita Académica

Noticias del Instituto

Participación en la Noche Europea de los Investigadores 2025

El pasado 26 de septiembre de 2025, las investigadoras Gloria González y Noelia Valenzuela, junto con el investigador Manuel Luis Ruiz, representaron al Instituto Andaluz Interuniversitario de Criminología (IAIC) en la Noche Europea de los Investigadores, celebrada en la Plaza del Rey de San Fernando (Cádiz).

El equipo presentó dos actividades centradas en la prevención de la ciberdelincuencia y la educación digital. La primera, titulada “TriviCrimen de Derecho Penal y Criminología”, invitaba al público infantil a participar en un juego de preguntas sobre seguridad digital y riesgos online. El segundo taller, “Ciberdetectives en acción”, tenía como objetivo enseñar a los más jóvenes a identificar perfiles de riesgo en redes sociales y chats de videojuegos.

Los participantes recibieron un carné de ciberdetective y, los más pequeños, una lupa simbólica como obsequio. Ambas actividades fueron un éxito de participación, contribuyendo a fomentar un uso responsable y seguro de Internet entre niños y niñas.

Proyectos de investigación

Dos investigadoras del Instituto han obtenido financiación en las últimas convocatorias de proyectos competitivos:

En el proyecto del Ministerio de Ciencia, Innovación y Universidades, “Protección penal de la imagen frente al chantaje en los nuevos desafíos del siglo XXI”, a cargo de la profesora María Acale, se abordarán los retos jurídicos que plantea la manipulación y difusión no consentida de imágenes, analizando las respuestas legales y las nuevas formas de vulneración de la intimidad.

En el proyecto de la Junta de Andalucía, “VICIA: Programa criminológico de mejora en la información, prevención y acompañamiento de las víctimas de violencia interpersonal contra la infancia y la adolescencia”, a cargo de la profesora Gloria González, se trabajará en la creación de materiales educativos y herramientas de análisis que contribuyan a mejorar la prevención y la atención a las víctimas.

Programa CIBERIS-UCA

La Sección de Cibercrimen del IAIC (Universidad de Cádiz) ha lanzado la primera edición del Programa CIBERIS-UCA: Cibercrimen, Investigación y Sociedad Digital.

Se trata de una iniciativa dirigida a estudiantes de los grados en Derecho y Criminología interesados en participar en proyectos de prevención y divulgación sobre cibercrimen y sociedad digital.

El programa combina formación universitaria con aprendizaje aplicado, permitiendo al alumnado implicarse en acciones reales de investigación y sensibilización social.

Próximos eventos

Marzo 2026 · Albacete

V Encuentro de la REJIC (Red de Jóvenes Investigadores en Criminología)

Los días 5 y 6 de marzo de 2026 se celebrará en la Facultad de Derecho de la Universidad de Castilla-La Mancha (Albacete) el V Encuentro de la REJIC, un foro de intercambio entre jóvenes investigadores e investigadoras que contribuyen al avance de la Criminología en España.

Entre las líneas de trabajo propuestas destacan los estudios sobre ciberdelincuencia y su impacto en la investigación criminológica, así como la innovación en métodos de análisis, la prevención del delito y la aplicación de nuevas tecnologías al estudio del comportamiento criminal.

Junio 2026 · Cádiz

Congreso Anual de la Asociación de Profesorado de Derecho Penal

Los días 10, 11 y 12 de junio de 2026 se celebrará en la Universidad de Cádiz el Congreso Anual de la Asociación de Profesorado de Derecho Penal, uno de los encuentros más relevantes del ámbito jurídico español.

El congreso abordará los nuevos desafíos del Derecho penal en la sociedad tecnológica, incluyendo temas como la inteligencia artificial, la ciberdelincuencia y la protección de datos personales.

El evento situará a Cádiz como referente académico y científico en el debate sobre el futuro del Derecho penal y su adaptación a los cambios del entorno digital.

Junio 2026 · Coruña

XV Congreso español de Criminología de la SEIC

Los días 10, 11 y 12 de junio de 2026 se celebrará en la Universidad da Coruña el I Congreso Ibérico y XV Congreso Español de Criminología, un encuentro científico que busca reforzar la cooperación internacional en esta disciplina.

Bajo el lema “Horizontes compartidos en Criminología”, el congreso promoverá el diálogo entre investigadores de España y Portugal y la ampliación de redes académicas con países latinoamericanos de habla española y portuguesa.

El evento situará a La Coruña como punto estratégico para el desarrollo de proyectos conjuntos en criminología, destacando la necesidad de colaboración transnacional para afrontar los retos actuales en la investigación criminológica.



CIBERCRIMEN

Y DELITOS TECNOLÓGICOS
IAIC - UCA