

Grado en Derecho

Trabajo de final de Grado (21067/22747)

Curso académico 2021-2022

LA VIOLENCIA DE CONTROL SOBRE LAS MUJERES EN REDES SOCIALES

UN ANÁLISIS DEL ORDENAMIENTO JURÍDICO ESPAÑOL

María del Rocío Pallicer García

216939

Tutora del trabajo:

Migle Laukyte



**Universitat
Pompeu Fabra**
Barcelona

Declaración de autoría y originalidad:

Yo, MARÍA DEL ROCÍO PALLICER GARCÍA, certifico que el presente trabajo no ha sido presentado para la evaluación de ninguna otra asignatura, ya sea en parte o en su totalidad. Certifico también que su contenido es original y que soy la única autora, no incluyendo ningún material anteriormente publicado o escrito por otras personas excepto de aquellos casos indicados a lo largo del texto.

Como autora de la memoria original de este Trabajo de Fin de Grado autorizo a la UPF a depositarla y publicarla en el e-Repository: Repositorio Digital de la UPF, <http://repositori.upf.edu>, o en cualquier otra plataforma digital creada por la Universidad, de acceso abierto a Internet.

Esta autorización tiene carácter indefinido, gratuito y no exclusivo, es decir, soy libre de publicarla en cualquier otro lado.

Firmado

MARÍA DEL ROCÍO PALLICER GARCÍA

Barcelona, 15 de mayo de 2022

RESUMEN

El objetivo de este trabajo consiste en dejar constancia de la importancia que tiene actualmente la violencia de control en el canal de comunicación que se han convertido las redes sociales, así como expresar los peligros que conllevan si no se tratan jurídicamente con cautela.

Se pretende analizar cuál es la normativa existente en el ámbito de la violencia de control *online*. De esta forma se examina el ordenamiento jurídico europeo y español, juntamente con las actuaciones que llevan a cabo cada red social y las posibilidades de protección que poseen las mujeres ante tales actuaciones abusivas.

Dicho análisis vendrá acompañado de una crítica sobre el régimen jurídico existente, así como también una propuesta de soluciones ante la falta de mecanismos de protección que sufren las usuarias *online*.

ÍNDICE:

| | |
|--|-----------|
| INTRODUCCIÓN: LOS MEDIOS TECNOLÓGICOS COMO INSTRUMENTO DE CONTROL. LA VIOLENCIA DE CONTROL EN LAS REDES SOCIALES | 1 |
| 1. LA VIOLENCIA DE CONTROL | 2 |
| 1.1 Definición y concepto..... | 3 |
| 1.2 Conductas que surgen alrededor de este fenómeno: Impersonation, Doxing, Video and image based-abuse, Astroturfing, Zoombombing | 4 |
| 1.3 La subsunción y la creación de nuevos delitos en el Código Penal: acoso, difusión de imágenes y usurpación e implantación de identidad | 6 |
| 1.4 La afectación en los datos personales de las víctimas: El impacto en las mujeres y acciones que pueden llevar a cabo en España | 7 |
| 2. LA ACTUACIÓN DEL ESTADO:..... | 9 |
| 2.1. La normativa europea:..... | 9 |
| 2.2 La violencia de control penalmente relevante en las relaciones de pareja | 11 |
| 2.3 Protección a las víctimas: legislación vigente: | 12 |
| 2.3.1 Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género | 12 |
| 2.3.2: Ley de Enjuiciamiento Criminal: Artículo 544 ter: | 13 |
| 3. LA ACTUACIÓN DE LAS EMPRESAS: | 14 |
| 3.1 Análisis de las redes sociales más influyentes y su actuación ante el abuso online: 15 | |
| 3.2 El conflicto entre el derecho fundamental de la víctima sobre la intimidad y propia imagen, contra el derecho de la libertad de expresión del agresor | 18 |
| 3.3 Posibilidades que tienen las mujeres de prevención y protección ante el abuso online | 21 |
| 4. CRÍTICA ANTE LA SITUACIÓN ACTUAL Y POSIBLES SOLUCIONES | 23 |
| CONCLUSIONES:..... | 29 |

INTRODUCCIÓN: LOS MEDIOS TECNOLÓGICOS COMO INSTRUMENTO DE CONTROL. LA VIOLENCIA DE CONTROL EN LAS REDES SOCIALES

Se estima que aproximadamente el 27% de las mujeres residentes en España de 16 o más años han sufrido a lo largo de su vida violencia de control por alguna de sus parejas¹. Este tipo de violencia se puede incardinar como un subgénero de la llamada violencia de género la cual constituye un problema primordial que afecta a una gran parte de la sociedad y que cada día al encender la televisión nos encontramos ante noticias relacionadas con estos casos que tristemente tienen un final fatídico. Este final suele ser la punta del “iceberg” de numerosos actos que realiza la pareja sobre la víctima, tales como la humillación en el ámbito domiciliario, amenazas; o el acto del que se centrará este trabajo, el control que realiza la pareja sobre la mujer a través del canal de comunicación que se han convertido las redes sociales.

Aunque la violencia de género es un tema de gran actualidad, la violencia de control es igual de perjudicial pero pasa más desapercibida y se desplaza muy sigilosamente mediante amenazas o coacciones², por ello considero que es digno de investigación y análisis. En la base de este hipotético “iceberg” nos encontramos con el control constante que realiza la pareja a la mujer mediante la tecnología, ya sea en un caso de violencia de género que ya ha sido denunciado (y habiendo aplicado las respectivas medidas cautelares y/o de protección), o cuando aún no ha sido así.

El objetivo de este trabajo es dar visibilidad a la violencia de control de la pareja sobre la mujer que se realiza en el ámbito de las redes sociales, así como también intentar dar una posible solución jurídica ante esta problemática que cada vez más a menudo se está dando y que aumenta a pasos agigantados (sobre todo en parejas de menores o adolescentes³), lo cual preocupa de forma mayor.

¹ Datos extraídos de la Macroencuesta de Violencia contra la mujer realizada el 2019 por la Delegación del Gobierno contra la Violencia de Género, concretamente, la página 46.

MACROENCUESTA DE VIOLENCIA CONTRA LA MUJER 2019 Delegación del Gobierno contra la Violencia de Género. (n.d.). Delegación del Gobierno contra la Violencia de Género. https://violenciagenero.igualdad.gob.es/violenciaEnCifras/macroencuesta2015/pdf/Macroencuesta_2019_estudio_investigacion.pdf

² European Parliament, Directorate-General for Internal Policies of the Union, Dizdarevic, I., Cucu, V., Ribeiro Oertel, R. (2020). *Violencia contra las mujeres : violencia psicológica y control coercitivo : sintesis*, European Parliament. <https://data.europa.eu/doi/10.2861/86732>

³ Ariadna Martín Montilla, María Pazos Gómez, María del Valle Cecilia Montilla Coronado, & Cristina Romero Oliva. (2016). UNA MODALIDAD ACTUAL DE VIOLENCIA DE GÉNERO EN PAREJAS DE JÓVENES: LAS REDES SOCIALES. *Educación XXI*, 19(2), 405–429.

Se divide el trabajo en tres secciones. En primer lugar, se intenta investigar qué es la violencia de control y sus implicaciones, donde se ha tratado ampliamente en el ámbito psicológico, pero no en el jurídico.

En segundo lugar, se expone cuál es el papel que adopta el Estado acerca de la violencia de control con la *Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género*, así como con el artículo 544 ter de la Ley de Enjuiciamiento Criminal. También se tratan las posibles actuaciones que pueden realizar las empresas creadoras de estas redes sociales cuando el derecho fundamental a la libertad de expresión del agresor y el derecho a la intimidad de la víctima entran en conflicto.

En tercer lugar, se realiza una crítica constructiva sobre este fenómeno dentro del ordenamiento jurídico español, así como las posibles soluciones que se podrían adoptar realizando un análisis del campo jurídico existente y teniendo en cuenta las necesidades reales de las víctimas.

1. LA VIOLENCIA DE CONTROL

Hemos de tomar consciencia de los tiempos en los que vivimos. Un mundo globalizado e interconectado donde estamos constantemente en contacto con una gran diversidad de personas en todo momento. Así, nuestro principal canal de comunicación es a través de los medios tecnológicos, ya sea a través de teléfono móvil, correo electrónico, o el que se centra este trabajo, las redes sociales. Estas se han convertido en un pilar fundamental en el mantenimiento, el desarrollo o la ruptura de relaciones de pareja⁴.

Las redes sociales se pueden definir como una vía virtual de interacción que permite la relación y comunicación entre personas. Las redes sociales se caracterizan por el hecho de que permiten crear un perfil público e intercambiar mensajes con otras personas o grupos⁵. Todas las redes sociales tienen diferentes finalidades: unas están destinadas al intercambio de imágenes y/o vídeos, otras al intercambio de información política, otras están dedicadas al ámbito laboral, al ocio, etc. Algunos ejemplos de las redes sociales son: Twitter, Instagram, Facebook, Tik Tok, etc.

⁴ Fox, C.L. y Warber, K. (2014). Social networking sites in romantic relationships: Attachment, uncertainty, and partner surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 7(1), 3-7.

⁵ Lloria García, P. (2020). *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*. Iustel

En paralelo a las redes sociales, nos encontramos con las Aplicaciones (o *Apps*), las cuales se dedican únicamente al intercambio de mensajes de manera instantánea y operan de una forma más privada que las redes sociales. Un ejemplo de *Apps* serían WhatsApp o Telegram.

Pero no todo el mundo utiliza este medio con la única finalidad de comunicarse, sino también para realizar comportamientos dañinos. En este campo nos centramos en la pareja, las cuales son controladas mediante agresiones verbales y psicológicas⁶. Por lo tanto, hablamos también de un control físico y psicológico.

1.1 Definición y concepto

La violencia de control, como se ha mencionado anteriormente, constituye un subgénero de la ya conocida violencia de género. En este trabajo se quiere dar un paso más allá y cuestionar qué significa la violencia de control y qué comportamientos incluye dentro del ámbito tecnológico.

En este aspecto, la Ley Orgánica 1/2004⁷ define la violencia de género como *la violencia que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia.*

Por lo tanto, se incluyen la violencia psicológica, física, económica y/o sexual; además, implica relaciones coercitivas y abusivas. Así, la violencia de género incluye el control coercitivo.

Dentro de este control se circunscriben una serie de pautas relativas a la manipulación emocional y psicológica: amenazas y agresiones o cualquier otro tipo de abuso para causar daño emocional o físico a otra persona.

Esta violencia de control se caracteriza por el hecho de ser repetitivo, es decir, no se limita a un solo acto aislado, sino que son una serie de comportamientos de control continuos y deliberados donde la persona abusadora tiene el objetivo de poseer poder y control sobre su pareja⁸.

⁶ Borrajo, E., Gámez-Guadix, M., Pereda, N. y Calvete, E. (2015c). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior*, 48, 358-365.

⁷ Así como esta LO regula y define lo que es la Violencia de género, también lo expresa la Llei 5/2008, sobre el dret de les dones a erradicar la violencia masculista.

⁸ *Violencia de género, violencia machista y control coercitivo.* (n.d.). FutureLearn <https://www.futurelearn.com/info/courses/salud-de-la-mujer-en-el-postparto/0/steps/68332>

Una vez delimitado el ámbito de aplicación de la violencia de control, cabe incluir estos comportamientos en el ámbito tecnológico. Así, encontramos el *online abuse*, el cual se ha definido como un *conjunto de comportamientos repetidos que tienen como objetivo controlar, menoscabar o causar un daño al otro miembro de la pareja*⁹.

Sobre la conducta controladora en relación al abuso *online* encontramos que se incluyen ciertos actos, como pueden ser: los insultos públicos o privados en las redes sociales, el control de las mismas, la difusión de informaciones comprometidas o secretos, las amenazas o el uso indebido o robo de contraseñas. Asimismo, se ha constatado que el hecho de que se realicen estas actuaciones en redes sociales¹⁰ constituye un precedente de un comportamiento agresivo en el mundo analógico.

1.2 Conductas que surgen alrededor de este fenómeno: Impersonation, Doxing, Video and image based-abuse, Astroturfing, Zoombombing

Como se ha mencionado anteriormente, las redes sociales forman parte de nuestro día a día al convertirse en un canal de comunicación, y con ello, se han creado nuevas actuaciones delictivas en la red (como por ejemplo el abuso *online* anteriormente mencionado). De esta forma, el ordenamiento jurídico se ha encontrado ante el reto de tener que adaptarse rápidamente a estos nuevos comportamientos delictivos.

El abuso *online* incluye una diversidad de tácticas y comportamientos maliciosos que van desde compartir contenido vergonzoso o cruel sobre una persona, la suplantación de identidad, el *Doxing*, el acecho y la vigilancia electrónica; hasta el uso no consentido de fotografías y amenazas violentas.

Asimismo, es interesante definir algunas de estas nuevas figuras jurídicas a efectos de entender con más profundidad cuáles son algunas conductas que se están introduciendo como delito en nuestro ordenamiento jurídico.

En primer lugar, nos encontramos con el *Impersonation* que trata de crear una cuenta/perfil falso en una red social para luego hacerse pasar por esa persona¹¹.

⁹ Reed, L. A., Tolman, R. M. y Ward, L. M. (2017). Gender matters: Experiences and consequences of digital dating abuse victimization in adolescent dating relationships. *Journal of Adolescence*, 59, 79-89.

¹⁰ Borrajo, E., Gámez-Guadix, M., Pereda, N. y Calvete, E. (2015c). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior*, 48, 358-365.

¹¹ Reznik M. Identity theft on social networking sites: developing issues of Internet impersonation. *Touro law review*. 2013; 29 (2):455-.

En segundo lugar, tenemos el *Doxing*, el cual consiste en recopilar información sobre la identificación personal (como la dirección del domicilio o el correo electrónico) para posteriormente publicarla sin permiso¹².

Además, nos encontramos ante la figura del *Video and image based-abuse*¹³ el cual trata de la creación y distribución no consensuada de imágenes privadas sexuales¹⁴.

Seguidamente, es remarcable definir dos conceptos que han surgido muy recientemente; el *Astroturfing* (muy relacionado con las *fake news* y la *misinformation*) y el *Zoombombing*. El primero hace referencia al movimiento social que se desarrolla en el escenario de las redes sociales con la finalidad de que las personas se reúnan, acuerden una agenda común y se organicen para motivar una queja o emitir informaciones falsas (ya sea de contenido político, comercial o periodístico)¹⁵. En cambio, el segundo hace referencia a la intromisión (normalmente *trolls*) en llamadas de Zoom, Reddit, Discord, etc de usuarios donde se comparte contenido inadecuado que produce la finalización de la llamada¹⁶.

No obstante la definición de estos fenómenos, cabe esclarecer que todas estas acciones se engloban en el llamado “*online harassment*”¹⁷.

Aun así, es importante remarcar que a lo que realmente se atañe este trabajo es a la violencia de control, es decir, al acoso en línea de las mujeres, a veces llamado cibersexismo o cibermisoginia, que es específicamente un abuso de género dirigido a mujeres y adolescentes en línea. Y, dentro de este cibersexismo o cibermisoginia, encontramos las posibles actuaciones (anteriormente mencionadas) que puede realizar el agresor contra la víctima.

¹² Mery, H. C. (2021). The dangers of doxing and swatting: why texas should criminalize these malicious forms of cyberharassment. *St. Mary's Law Journal*, 52(3), 905-944

¹³ Image-based Abuse: Debate and Reflections on the “Iveco Case” in Spain on Twitter. (2020). *Journal of Interpersonal Violence*, 886260520967143–886260520967143. <https://doi.org/10.1177/0886260520967143>

¹⁴ McGlynn, C., & Rackley, E. (2016). Not “revenge porn,” but abuse: Let’s call it image-based sexual abuse. <https://inherentlyhuman.wordpress.com/2016/02/15/>

¹⁵ Keller, Schoch, D., Stier, S., & Yang, J. (2020). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication*, 37(2), 256–280. <https://doi.org/10.1080/10584609.2019.1661888>

¹⁶ Elmer, Neville, S. J., Burton, A., & Ward-Kimola, S. (2021). Zoom Bombing During a Global Pandemic. *Social Media + Society*, 7(3), 205630512110353–. <https://doi.org/10.1177/2056305121103536>

¹⁷ Chadha, Steiner, L., Vitak, J., & Ashktorab, Z. (2020). Women’s Responses to Online Harassment. *International Journal of Communication (Online)*, 239–.

1.3 La subsunción y la creación de nuevos delitos en el Código Penal: acoso, difusión de imágenes y usurpación e implantación de identidad

Las nuevas conductas explicadas anteriormente también han causado interés y preocupación en la sociedad española, por lo que el ordenamiento jurídico español ha actuado para castigar penalmente estas actuaciones. Estas figuras a medida que van apareciendo se van incardinando analógicamente en el tipo delictivo adecuado del Código Penal (en adelante CP).

De esta manera, encontramos que el *Doxing* es penado en España realizando una subsunción analógica del artículo 172.2 del CP, sobre coacciones¹⁸. El *Astroturfing* es penado aplicando el artículo 284.2 del CP, sobre divulgación de noticias falsas¹⁹.

En referencia al *Zoombombing*, no se ha encontrado ningún tipo penal en el que pueda incardinarse esta conducta, ni tampoco jurisprudencia donde se aplique algún artículo del CP referido a esa acción, ya que el “castigo” de esta conducta se ha dejado en manos de la empresa de la plataforma en cuestión, de las cuales todas recurren a la finalización de la llamada, sin una ulterior sanción.

Asimismo, en el mismo CP español se han creado y añadido nuevos delitos relacionados con algunas de estas actuaciones dentro de Internet, como pueden ser el delito de acoso predatorio o *stalking* del artículo 172 ter del CP, la difusión in consentida de imágenes íntimas (a lo que anteriormente hemos mencionado como *Video and image based-abuse*) del artículo 197.7 del CP o la usurpación e implantación de identidad (en referencia a lo definido anteriormente como *Impersonation*) del artículo 401 del CP.

Se puede apreciar cómo estos nuevos delitos sí han tenido una aplicación práctica en la jurisprudencia, así se ve, por ejemplo, en la sentencia del 26 de enero de 2022 de la Sala de lo Penal del Tribunal Supremo²⁰ que aplica el artículo 172 ter del CP sobre el *Stalking*. En relación al delito de difusión in consentida de imágenes íntimas encontramos la sentencia de 17 de marzo de 2022 de la Sala de lo Penal del Tribunal Supremo²¹. Y, en referencia al delito de usurpación e implantación de identidad, encontramos la sentencia de 28 de noviembre de 2017 de la Audiencia Provincial de Jaén²².

¹⁸ Encontramos numerosa jurisprudencia al respecto, por ejemplo, la reciente sentencia de 18 de febrero de 2022 de la Audiencia Provincial de Pontevedra (Roj: SAP PO 552/2022 - ECLI:ES: APPO:2022:552).

¹⁹ No obstante, se extrae de la jurisprudencia que no se suele aplicar este tipo delictivo para castigar el *Astroturfing*.

²⁰ Roj: SAP PO 552/2022 - ECLI:ES: APPO: 2022:552

²¹ Roj: STS 974/2022 - ECLI:ES:TS: 2022:974

²² Roj: SAP J 1203/2017 - ECLI:ES:APJ:2017:1203

1.4 La afectación en los datos personales de las víctimas: El impacto en las mujeres y acciones que pueden llevar a cabo en España

No podemos negar que la mayoría de los actos que se incardinan dentro de la violencia de control se basan en vulneraciones y emisión de datos personales de las víctimas. Normalmente estos actos de control suelen ser amenazas o coacciones que realizan los abusadores basándose en la amenaza de compartir datos o imágenes/vídeos íntimos. Todo ello son datos personales de las víctimas. Ante esta problemática, ¿qué puede hacer la víctima para protegerse?

En algunos países, como Canadá, apreciamos cómo la víctima ha de recurrir a la vía de su propia protección ante la violencia de control y el peligro de poder haberse emitido datos personales sin su consentimiento²³. Ello es debido a la falta de regulación y protección estatal de los datos personales de usuarios de diferentes países.

Es sabido que es necesaria una protección legislativa, judicial y constitucional del tratamiento de los datos personales, porque, de tratarse ilegalmente dichos datos, nos encontraríamos con una vulneración de la vida privada.

En el campo virtual de las redes sociales²⁴, la situación es más compleja a causa de la dificultad de determinar la ley aplicable debido a la globalidad que presentan las redes sociales (porque se extralimitan a la soberanía de cada país). Esto puede conducirnos a la “red oscura” donde no es aplicable ninguna ley.

La cuestión fue abordada por parte de la Unión Europea con la regulación de 2018, exactamente, el Reglamento 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos. Además, es recomendable la aplicación de *soft law*, para un efecto preventivo, porque ya es sabido que en el mundo tecnológico no puede regirse todo por una ley con aspectos clásicos.

En España, con la transposición de esta Directiva, se creó la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*²⁵.

²³ Veletsianos, G., Houlden, S., Hodson, J., & Gosse, C. (n.d.). Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame. *SAGE*, 20(12), 4689–4708.

²⁴ Mansouri, O. (2021). Protection of Personal Data in Social Media (Comparative Analysis). *International Review of Law*, 9(3). <https://doi.org/10.29117/irl.2020.0124>

²⁵ *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. (2021, December 5). BOE.es <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

Anteriormente a la adopción de esta Ley ya se creó un Organismo para velar por la protección de los Datos personales, y, con la adopción de esta Ley Orgánica, su función primordial es velar por su cumplimiento. Este Organismo es la Agencia Española de Protección de Datos²⁶ (AEPD), cuyo ámbito de actuación se extiende a toda España.

Con esta problemática en el ámbito de violencia de control, se emitió una guía²⁷ cuya finalidad fue proporcionar información sobre las consecuencias de ciertas conductas abusivas en Internet, así como facilitar unas pautas para evitar ser víctimas de ello (o incluso por cometer estos actos sin ser conscientes de su gravedad).

Además, desde el Gobierno y la AEPD se ha creado el *Convenio entre el Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad y la Agencia Española de Protección de Datos*²⁸ debido a que se ha visto que en relación a la violencia de control, la protección de datos es muy importante. Con este Convenio se pretende que los dos Organismos colaboren entre ellos en materia de violencia de género, donde la violencia de control extiende su ámbito de actuación cuando se tratan de redes sociales o cualquier ámbito del mundo virtual.

No obstante, ni con la *Ley Orgánica 3/2018 ni el Convenio de colaboración entre Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad y la Agencia Española de Protección de Datos* se produce una protección integral de la víctima. Puede ser que estos instrumentos sean efectivos en base a la protección de los datos personales tanto para la prevención de robo y compartición, como para el control del transcurso de estos datos y la denuncia en caso de uso indebido de estos²⁹. Pero a la hora del castigo de los actos que se incardinan dentro de la violencia de control, nos encontramos con la misma incógnita inicial: no se proporciona un mecanismo integral y eficiente de protección a la víctima de violencia de control.

Por tanto, la propia víctima al no tener mecanismos de protección integrales, recurren al bloqueo de contactos, la creación de un perfil privado, cambiar su número de teléfono, reportar el comportamiento del agresor a la plataforma *online*, reducir la presencia en línea o incluso dejar

²⁶ (n.d.). Agencia Española de Protección de Datos | AEPD. <https://www.aepd.es/es>

²⁷ Agencia Española de Protección de Datos. (n.d.). Protección de datos y prevención de delitos. <https://www.aepd.es/sites/default/files/2019-11/guia-proteccion-datos-y-prevencion-de-delitos.pdf#%5B%7B%22num%22%3A96%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22FitH%22%7D%2C846%5D>

²⁸ *Disposición 14983 del BOE núm. 251 de 2019.* (2019, October 18). BOE.es. <https://www.boe.es/boe/dias/2019/10/18/pdfs/BOE-A-2019-14983.pdf>

²⁹ Rosa María García Sanz. (2011). REDES SOCIALES ONLINE: FUENTES DE ACCESO PÚBLICO O FICHEROS DE DATOS PERSONALES PRIVADOS (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas). *Revista de Derecho Político*, 81, 102–.

de utilizar la red social, o reportar el comportamiento a una agencia protectora *offline* (*offline protective agency*)³⁰.

2. LA ACTUACIÓN DEL ESTADO:

2.1. La normativa europea:

Antes de desarrollar la normativa estatal, es cuestión central aclarar que el ordenamiento jurídico español está muy influido por la normativa europea. Esta normativa ha empujado que el Estado español legisle sobre estas materias de nuevas tecnologías y nuevos medios de comunicación.

A nivel europeo nos encontramos con que no existe normativa específica relativa al abuso *online* contra las mujeres, únicamente existe normativa contra el abuso sexual a menores *online*³¹.

Desde un primer momento ante esta materia sobre abuso, por un lado, y redes sociales por otro, la Unión Europea no se ha quedado atrás y ya en 2001 legisló sobre las nuevas tecnologías y sus implicaciones con el *Convenio sobre la Ciberdelincuencia, en Budapest el 23 de noviembre de 2001*. Con ello, España introdujo las respectivas modificaciones en su ordenamiento ratificando el presente Convenio e introduciendo la *Ley Orgánica 5/2010* que modificaba el Código Penal e introducía algunos actos tecnológicos como penalmente relevantes. Pero la reforma más relevante del Código Penal fue aquella que se realizó en 2015 e introdujo disposiciones relevantes donde se tipifican los diferentes tipos de cibercrimen, como el artículo 197 bis que penaliza el acceso no autorizado a sistemas informáticos, o el 197 ter que castiga la producción, adquisición, importación o entrega a terceros de datos de acceso o software desarrollado o adaptado con el fin de cometer delitos. Además, en 2019 se creó la Estrategia

³⁰ De acuerdo a la estadística realizada por: (2021, March 1). Measuring the prevalence of online violence against women. <https://onlineviolencewomen.eiu.com/>. De entre las mujeres encuestadas que sufrieron online abuse, el 55% se decantaron por bloquear a sus contactos, entre un 30% decidieron limitar o dejar de tener presencia online, y solo un 14% decidieron reportarlo a agencias protectoras offline.

³¹ *Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.* (n.d.). EUR-Lex. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32011L0093>

Nacional de Ciberseguridad³², cuyo principal objetivo es “*garantizar el uso fiable y seguro del ciberespacio, protegiendo los derechos y libertades de los ciudadanos, y promoviendo el progreso económico*”.

Asimismo, España con el Convenio de Budapest proporcionó un amplio abanico de medios para la investigación y la obtención de pruebas electrónicas relativas a los delitos cometidos en línea a través de las nuevas tecnologías, así como para cualquier otro delito que implique pruebas electrónicas. Algunos de estos medios son³³: el análisis del *big data*, el desarrollo de sistemas integrados de información, de sistemas de información geográfica, centros de mando integrado, uso de drones, la utilización de cámaras con reconocimiento facial o el registro de los dispositivos de almacenamiento masivo de información, entre otros.

En relación a la persecución de delitos incardinados en la violencia de control, no encontramos novedades a parte de los mecanismos tecnológicos típicos que conocemos, que son: el transmisor de radiofrecuencia y la unidad *2 track* para el agresor y la unidad *2 track*³⁴ para la víctima; con esto se consigue que el agresor mantenga la orden de alejamiento (física) impuesta por el juez.

No obstante, no introducen ningún mecanismo relacionado con redes sociales que eviten el contacto con la víctima de violencia de control.

En consonancia con ello y limitándonos a nuestro ámbito de actuación sobre la Violencia de Género y de control, con el *Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica de 11 de mayo de 2011*, se clarificó que la violencia sobre la mujer es perseguible contra todas las formas de violencia (ya sea física, psicológica, de control, etc.) y se ha de intentar proteger, prevenir, perseguir y eliminar esta violencia.

³² *Estrategia Nacional de Ciberseguridad 2019*. (n.d.). DSN. <https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019>

³³ López-Barajas Perea, I. (2017, Febrero). Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos. *Revista de Internet, Derecho y Política*.

³⁴ *Dispositivos de control telemático de medidas y penas de alejamiento - Delegación del Gobierno contra la Violencia de Género*. (n.d.). Delegación del Gobierno contra la Violencia de Género. <https://violenciagenero.igualdad.gob.es/informacionUtil/recursos/dispositivosControlTelematico/home.htm>

A nivel europeo no encontramos normativa sobre la violencia *online* contra las mujeres, lo que provoca que estas actuaciones no sean perseguibles, lo cual quedan impunes. Existen estudios³⁵ que argumentan que estas dos normativas marco mencionadas anteriormente podrían ser complementadas para así conseguir que los delitos contra mujeres online se conceptualicen en los marcos del delito cibernético y queden amparados sobre el Convenio de Budapest.

2.2 La violencia de control penalmente relevante en las relaciones de pareja

En España se interpreta que el control no es una clase de violencia física o psíquica, sino que es una situación que proviene de ambas, tanto si los actos se producen en el mundo analógico como en el virtual³⁶. Los actos de control mediante violencia física o psíquica generalmente adquieren relevancia penal cuando se producen de manera habitual y continuada. Sin embargo, los hechos de control que se pueden producir de manera alternativa con uno o más actos y que se ejecutan fundamentalmente en el mundo virtual, tienen que ver normalmente con delitos de coacciones o amenazas.

Por lo tanto, para los delitos de amenazas o coacciones (o el de habitualidad), para completar el injusto y que superen la “barrera” del principio de la insignificancia, y se pueda así subsumir la violencia de control en su respectivo tipo penal, se han de dar los requisitos adecuados para que la afectación al bien jurídico sea suficiente, y la habitualidad y la permanencia son válidas para completar el injusto que se requiere para subsumirlo a un tipo penal³⁷.

Entonces, ¿qué pasa cuando no se supera la “barrera” del principio de insignificancia, o no se prueba esta violencia? No se podrá subsumir al tipo penal y no será perseguible penalmente. De esta forma, para una protección a las víctimas de violencia de control, desde una perspectiva diferente al campo penal, tenemos la vía que nos proporciona la *Ley Orgánica 1/2004 de 28 de diciembre, de medidas de protección integral contra la violencia de género*.

³⁵ PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE. (n.d.). Coe. <https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44>

³⁶ Lloria García, P. (2020). *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*. Iustel.

³⁷ Lloria García, P. (2006). *Aproximación al estudio del delito permanente*. Comares. Pp. 124-126

2.3 Protección a las víctimas: legislación vigente:

2.3.1 Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género

Esta ley es la base para la protección de las víctimas de la violencia de género y de control. En su artículo 1 se delimita su ámbito de aplicación y se aprecia que la violencia de control se incardina dentro del ámbito de aplicación de esta ley ya que se incluyen todas las actuaciones que hagan referencia tanto a la violencia física como a la psicológica (las coacciones, amenazas, la privación de libertad o la agresión sexual).

Asimismo, la finalidad de esta ley es establecer mecanismos de protección integral para las mujeres víctimas de violencia de género (como ya se ha dicho física o psicológica) y prestarles la asistencia necesaria, así como también erradicar esta violencia, sancionarla y prevenirla.

A efectos de este trabajo, no se ha encontrado ninguna disposición que se especifiquen medidas de protección en redes sociales ni en ningún campo virtual. Solamente se menciona en el artículo 64 que, en relación a las medidas de salida del domicilio, alejamiento o suspensión de las comunicaciones, se podrá utilizar la tecnología adecuada para verificar de inmediato su incumplimiento. Se habla de incumplimiento una vez la víctima ha informado de este abuso y se han decretado las medidas cautelares pertinentes del artículo 544 de la Ley de Enjuiciamiento Criminal, pero no se habla en ningún momento de una protección efectiva en el ámbito tecnológico porque el mecanismo de protección activo entra en juego una vez el abusador ya ha quebrantado estas medidas cautelares y/o de protección, esto deja a la víctima una sensación de desprotección que puede comportar secuelas psicológicas a la misma.

No obstante, en 2016 el Consejo General del Poder Judicial emitió una guía práctica³⁸ en relación a la LO 1/2004, con un enfoque más tecnológico y donde se especifican expresamente los derechos de las víctimas.

³⁸CGPJ - Guías prácticas. (2016, November 3). Poder Judicial. <https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Actividad-del-Observatorio/Guias-practicas/Guia-practica-de-la-Ley-Organica-1-2004--de-28-de-diciembre--de-Medidas-de-Proteccion-Integral-contr-la-Violencia-de-Genero--2016->

Aun teniendo este enfoque más actual y tecnológico, esta guía está más dirigida a enunciar la coordinación con otras instituciones y a la actividad jurisdiccional en general, pero sobre todo a la actuación procesal donde se incorporan las nuevas tecnologías en todos los momentos del proceso para agilizarlo y garantizar en todo momento los derechos de las partes. Pero no se incluye así la protección de las víctimas, ni la prevención de la violencia de género y de control en las nuevas tecnologías.

2.3.2: Ley de Enjuiciamiento Criminal: Artículo 544 ter:

Habiendo analizado y constatado que la LO 1/2004 no confiere un tipo de protección diferente a las medidas de protección habituales que se establecen en el mundo analógico, nos encontramos con el artículo 544 ter de la Ley de Enjuiciamiento Criminal.

Esta disposición otorga a la víctima de violencia de género (así como también a la de violencia doméstica) un estatuto integral de protección donde se incluyen las medidas cautelares de carácter civil³⁹ y penal⁴⁰, así como aquellas medidas de protección social y asistencia necesaria. No se especifican medidas cautelares de protección para el ámbito tecnológico, únicamente se nombran las nuevas tecnologías para facilitar el proceso judicial tanto a la víctima como al agresor y así garantizar los derechos de las dos partes.

No obstante, con la guía práctica del Consejo General del Poder Judicial de 2016, se ha hecho un acercamiento a proteger al menos un aspecto del abanico de derechos de la víctima, como es el derecho al olvido que abre un mecanismo paralelo a la aplicación de las medidas del artículo 544 ter de la Ley de Enjuiciamiento Criminal.

³⁹Algunas de las medidas civiles son:

- La atribución del uso y disfrute de la vivienda familiar.
- La determinación del régimen de la prestación alimenticia, custodia, visitas, comunicación y estancia con los hijos, quedando incluida aquí la posibilidad de suspensión de la patria potestad o custodia de menores y del régimen de visitas.
- Las estipuladas en el art. 158 del Código Civil y, entre ellas, cualesquiera disposición que el Juez considere oportuna a fin de apartar al menor de un peligro o de evitarle perjuicios.

⁴⁰ Algunas de las medidas penales son:

- La prohibición de aproximarse o comunicarse con determinadas personas (arts. 544 bis Ley de Enjuiciamiento Criminal y 64 Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género), siendo necesario fijar una distancia mínima entre el inculpaado y la persona protegida (art. 64.3 LOMPIVG) y la duración de la prohibición.
- La prisión provisional (con los requisitos y presupuestos del art. 505 y concordantes de la LECrim).
- La prohibición de acudir a un determinado lugar (art. 544 bis LECrim).
- La expulsión del domicilio familiar y la prohibición de volver al mismo (art. 64 LOMPIVG).

En virtud de la sentencia del Tribunal de Justicia de la Unión Europea del 13 de mayo de 2014 sobre el derecho al olvido⁴¹, cuando se haya cometido un delito, la víctima podrá solicitar al juez de violencia sobre la mujer que se adopte la medida cautelar de la retirada de las imágenes de la red social. Para retirar ese contenido es necesario solicitar a los servidores de la red social la anulación de la difusión. No obstante, si no lo hace el propio servidor lo deberá hacer el órgano judicial ordenando la retirada de los contenidos.

Aun así, igualmente se podrán solicitar las medidas de prohibición de acercamiento, pero sobre todo las de prohibición de comunicación con la víctima como medida cautelar, porque en estos casos, aunque es obvio que a las víctimas les aterra el acercamiento, lo que más les atemoriza es la comunicación⁴². Y precisamente en ello se han de enfocar las medidas cautelares. No obstante, como se ha analizado, aunque actualmente el canal de comunicación principal son las *Apps* y redes sociales, el Estado no ha regulado exactamente sobre ello, dejando la mayoría de las decisiones sobre las medidas de protección en manos de las empresas propietarias del servidor de las redes sociales.

3. LA ACTUACIÓN DE LAS EMPRESAS:

De acuerdo con el Estudio Anual de Redes Sociales de 2021 realizado por IAB Spain⁴³, el 92% de los jóvenes de entre 16 y 25 años utilizan las redes sociales. El uso principal de las redes sociales continúa siendo fundamentalmente social.

Destacan las actividades relacionadas con el chateo y envío de mensajes a contactos (con un 65%). Ver vídeos y música (con un 57%) se mantiene en segunda posición y en tercer lugar 'ver qué hacen mis contactos' con un 45%.

En relación a las diferentes redes sociales que existen, podemos destacar que la pandemia ha afectado a cómo las usamos: aumenta el uso de Instagram con un 83%, Tik Tok con un 63% y Twitter con otro 63%, en contraposición tenemos a Facebook y YouTube que disminuyen su uso en un 70%. Aun así, la aplicación que más se ha utilizado ha sido WhatsApp con aproximadamente un 90%.

⁴¹Documents. (2014, May 13). CURIA - Documents. <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES>

⁴² Lloria García, P. (2020). *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*. Iustel.

⁴³AB Spain presenta el 'Estudio de RRSS 2021'. (2021, May 5). IAB Spain. <https://iabspain.es/iab-spain-presenta-el-estudio-de-rrss-2021/>

Con esto, podemos ver que no es necesario volver a incidir que la base de nuestras relaciones y la forma en cómo nos comunicamos es principalmente a través de las aplicaciones de mensajería y las redes sociales. Con ello, pretendemos realizar un análisis de cómo las redes sociales más utilizadas hacen frente a la problemática de la violencia de control (abuso *online*).

3.1 Análisis de las redes sociales más influyentes y su actuación ante el abuso online:

De acuerdo a la anterior estadística, se han elegido las 4 redes sociales (y la aplicación) más influyentes y utilizadas para analizar su actuación ante el abuso *online*. Estas son: WhatsApp, Facebook, Instagram y Twitter.

En primer lugar, la aplicación WhatsApp en su Centro de ayuda⁴⁴ facilita todo tipo de información ante cualquier tipo de abuso. Ante ello, la *App* proporciona un mecanismo de Bloqueo de contactos para evitar que la persona en cuestión pueda seguir comunicándose con la víctima. Sin embargo, aunque se facilita este bloqueo, la *App* no proporciona una ulterior protección: no se comunica con las autoridades para informar sobre la situación de abuso, no eleva las pertinentes acciones legales que tienen a su disposición, etc. Únicamente proporciona esta vía de bloqueo, lo que supone que el agresor pueda seguir comunicándose con la víctima a través de otro número de teléfono, o en el mismo número, a través de grupos que tengan en común las partes.

Es sorprendente cómo WhatsApp informa a sus usuarios sobre la importancia y rechazo que dan al uso no autorizado de mensajería automática o masiva en WhatsApp⁴⁵, alertando que ante cualquier mensaje que reciban sobre este uso, automáticamente suspenderán la cuenta en cuestión y emprenderán las acciones legales pertinentes si se infringen las condiciones de Servicio de la Aplicación. En contraposición, encontramos la posición que emprenden ante el abuso hacia las personas, las cuales como se ha mencionado, sólo tienen la opción de bloquear al contacto. Y si es el caso que la persona denunciase y si las autoridades pertinentes lo requieran y necesiten información adicional, WhatsApp entraría en juego proporcionando ulterior información.

⁴⁴ Política de privacidad - EEA. (2022, March 10). WhatsApp. <https://www.whatsapp.com/legal/privacy-policy-eea#privacy-policy-working-with-authorities>

⁴⁵ Centro de ayuda de WhatsApp - Uso no autorizado de mensajes automáticos o mensajes masivos en WhatsApp. (n.d.). WhatsApp FAQ. <https://faq.whatsapp.com/general/security-and-privacy/unauthorized-use-of-automated-or-bulk-messaging-on-whatsapp>

También es entendible esta tenue actuación de la *App* ante víctimas de abuso ya que estas son particulares/ciudadanos civiles. Por ello, se han de garantizar los derechos de estos, sobre todo el derecho a la libertad de expresión y a la intimidad (por esto, la Aplicación proporciona la opción de encriptación de mensajes -cifrado de extremo a extremo- para una mayor protección a esta intimidad mencionada).

En segundo lugar, la red social Facebook proporciona los dos mecanismos de Bloqueo a un perfil y de Denuncia a cierto contenido. No obstante, la denuncia no significa ningún tipo de cooperación con las autoridades para ofrecer cierta protección, así como tampoco aseguran que el contenido se elimine de la red social.

Aun así, es interesante que la misma aplicación proporciona información para que la víctima pueda ejercer las acciones oportunas y protegerse⁴⁶. Por ejemplo, si alguien controla o supervisa la actividad en Facebook, se disponen de varias opciones. Dependiendo de las circunstancias, se puede cambiar la configuración de privacidad de la cuenta de Facebook para que esa persona agresora no pueda acceder a la información.

Si se trata de alguien con quien se mantiene una relación estable, podría ser indicio de abuso. Se proporciona la línea de ayuda de *National Domestic Violence* y la red estadounidense para poner fin a la violencia doméstica para obtener más información.

Además, si el agresor amenaza a la víctima con compartir imágenes de carácter sexual sin consentimiento, se dan una serie de pasos a seguir para que la víctima pueda ejercer las acciones legales oportunas⁴⁷, así como la asistencia de asociaciones estatales.

En tercer lugar, Instagram⁴⁸ desde un primer momento advierte que los mensajes directos son conversaciones privadas y la plataforma no puede entrar a controlar la conversación entre dos personas, por lo que no garantizan que las personas no reciban mensajes ofensivos o hirientes. No obstante, para controlar, prevenir y proteger del abuso *online*, presentan las típicas medidas de Bloqueo al perfil y Denuncias al mismo.

⁴⁶ Servicio de ayuda de Facebook -¿Qué puedo hacer si mi novio, novia o cónyuge actuales o anteriores controlan o supervisan lo que hago en Facebook? (n.d.). Facebook FAQ. https://es-la.facebook.com/help/131920223550312/?helpref=uf_share

⁴⁷ Servicio de ayuda de Facebook - ¿Qué debo hacer si alguien me pide que comparta en Facebook una foto o un video donde aparezco sin ropa o en actitud provocativa, o si me amenaza con compartir una foto que ya envié? (n.d.). Facebook FAQ. https://es-la.facebook.com/help/1381617785483471/?helpref=uf_share

⁴⁸ *Actualización sobre el trabajo que hacemos para abordar el abuso en Instagram | Blogs de Instagram*. (2021, February 11). Instagram. <https://about.instagram.com/es-la/blog/announcements/an-update-on-our-work-to-tackle-abuse-on-instagram>

Sin embargo, se presentan las particularidades de que la misma empresa es consciente que con los mensajes privados no pueden actuar de la misma manera que con los comentarios públicos, por ello cuando detectan lenguaje que incita al odio en los mensajes directos (mensajes privados), utilizan nuevas medidas para prevenir este tipo de comportamiento, como por ejemplo: la eliminación de las cuentas de las personas que envían estos mensajes, así como la creación de nuevas tecnologías para reducir este abuso.

Además, actualmente si detectan personas que envían este tipo de mensajes abusivos, proceden a desactivar la cuenta por la que envía los mensajes, así como desactivar las cuentas nuevas que puedan crear.

Asimismo, Instagram coopera con las autoridades del Reino Unido (debido a que la sede reside ahí) y responden a las solicitudes legales que requieran de información de su plataforma.

Finalmente, en relación a la protección que pueden tener las víctimas, nos encontramos con que las víctimas pueden usar filtros en los comentarios para evitar que otras personas dejen comentarios ofensivos; además, utilizan inteligencia artificial para avisar a las personas que lo que están a punto de publicar puede ser ofensivo ya que esta red social está muy comprometida con la lucha contra el abuso en su plataforma. Aunque son conscientes que esta problemática excede de su ámbito de aplicación, tienen previsto trabajar con ONGs, asociaciones o gobiernos para mejorar su alcance y protección.

De todas formas, Instagram hace saber que están trabajando una nueva función para tratar de forma más eficiente estos casos, la cual saldrá adelante durante estos meses.

En cuarto lugar, la red social Twitter⁴⁹ no proporciona otros mecanismos de protección y prevención que no sean los habituales. Así, recomiendan que, si alguien se encuentra en situación de abuso, dejen de seguir a la cuenta en cuestión y la bloqueen. Si el comportamiento sigue persistiendo, se puede denunciar a la plataforma esta conducta. Además, informan que, si la víctima recibe amenazas y esta decide denunciar al abusador, se recomienda que se sigan unos pasos especificados en la página web mencionada.

Una vez hecho este pequeño análisis, nos quedamos con la duda de: ¿Por qué los Estados trasladan la decisión de la protección a las plataformas, y estas tienen tan pocos mecanismos de

⁴⁹ *Cómo manejar el abuso de Twitter y cómo podemos ayudar.* (n.d.). Twitter Help Center. <https://help.twitter.com/es/safety-and-security/cyber-bullying-and-online-abuse>

protección (el cual uno de ellos es denunciar a las autoridades estatales)? En esta situación parece ser que se están trasladando la decisión de la protección de la víctima entre ellos. Es una cuestión muy complicada debido a que, entre todo ello, se encuentra la protección de los derechos fundamentales, no solo de la víctima, sino también del abusador.

3.2 El conflicto entre el derecho fundamental de la víctima sobre la intimidad y propia imagen, contra el derecho de la libertad de expresión del agresor

Como se ha mencionado en múltiples ocasiones, hoy en día las redes sociales son el medio de comunicación más común entre las relaciones personales y de pareja. Debido a esto, los delitos de expresión (es decir, aquellos que afectan a la libertad o a la intimidad) se producen más en este medio, lo que conlleva a situaciones de violencia de control y psicológica.

No obstante, somos conscientes que la protección de los derechos fundamentales es cuestión crucial no solo en el ámbito analógico, sino también en el virtual (donde todo lo que ocurre se realiza de forma más discreta). Así, aunque se produzcan estos delitos, ¿cómo hemos de ponderar los derechos fundamentales en el campo tecnológico?

Así, tomamos como referencia un *Issue Discussion Paper*⁵⁰ realizado por el *Comissioner for Human Rights* en 2012. En él se toma consciencia de la relevancia de las redes sociales en nuestro día a día, así como las múltiples vulneraciones de derechos fundamentales que se pueden realizar con este medio, sobre todo en relación al derecho a la libertad de expresión. En este *paper* se informa de la creación de unos principios de *Internet governance* para evitar estas vulneraciones de derechos.

Algunos Estados (sobre todo miembros del Consejo de Europa) han adoptado procedimientos de bloqueo, filtración, eliminación o vigilancia de Internet debido a preocupaciones estatales sobre actividades delictivas *online*, concretamente el intercambio en línea de imágenes de abuso infantil. No obstante, a causa de las limitaciones a estas medidas restrictivas, el bloqueo de Internet no cumple el objetivo de eliminar contenido específico de Internet. Es muy intrusivo e ineficaz para evitar que determinados usuarios accedan a contenidos ilegales; inevitablemente

⁵⁰Internet Governance Forum, & United Nations. (n.d.). the charter of human rights and principles for the internet. *Internet Rights & Principles Coalition*. <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>

European Comission. (n.d.). EUROPEAN COMMISSION Brussels, 25.1.2012 SEC(2012) 72 final COMMISSION STAFF WORKING PAPER Impact Assessment Accompanying the document Regulation of the European Parliament and of t. https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf

bloquea el contenido legal; y a veces puede beneficiar a aquellos contra quienes se usa. Además, a menudo se basa en leyes vagas y arbitrarias (o en ninguna ley). Por lo general se basa en listas secretas, desconocidas para el público y elaboradas por organismos que no rinden cuentas; y carece del debido proceso, tanto cuando se aplica como prevención o después de la comisión del hecho.

Como consecuencia, el ordenamiento jurídico europeo ha incluido una serie de principios que pretenden orientar la legislación de los Estados Miembros. Algunos de estos principios son⁵¹: Derecho de expresión y asociación, accesibilidad, Derecho a la vida, libertad y seguridad e igualdad en la red.

De esta forma, así quedarían las fuentes del derecho comunitario: Los nuevos principios de gobernanza de Internet, el Convenio Europeo de Derechos Humanos (ECHR) y la jurisprudencia (desarrollada sobre todo para el mundo analógico) y otros convenios y resoluciones (incluido el Convenio del Consejo de Europa sobre la Ciberdelincuencia).

En lo que atañe a la temática de este trabajo sobre redes sociales, el derecho fundamental que se suele vulnerar con más frecuencia es el derecho a la libertad de expresión.

Sobre ello, la *Global Network Initiative*⁵² ha elaborado unos principios sobre Libertad de expresión y privacidad. Exactamente, recuerdan la necesidad de cumplir con los estándares internacionales de libertad de expresión y privacidad y de cumplir con el Estado de Derecho en asuntos que afectan a la libertad de expresión en Internet. Además, es importante remarcar que han incluido específicamente a las entidades del sector privado en estas recomendaciones que emanan de los principios. Expresan que las empresas TIC “*tienen la responsabilidad de respetar y proteger la libertad de expresión y los derechos de privacidad de sus usuarios*” y que “*el desarrollo de estrategias colaborativas que involucren a empresas, asociaciones industriales, organizaciones de la sociedad civil, inversionistas y académicos será fundamental para el logro de estos principios*”.

⁵¹ Internet Governance Forum, & United Nations. (n.d.). the charter of human rights and principles for the internet. *Internet Rights & Principles Coalition*. <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>

⁵² Global Network Initiative. (n.d.). GNI PRINCIPIOS DE LIBERTAD DE EXPRESIÓN Y PRIVACIDAD. <https://globalnetworkinitiative.org/wp-content/uploads/2018/03/GNI-Principles-SP.pdf>

Además, la Recomendación CM/Rec (2008)6 del Consejo de Europa añade nuevos e importantes detalles a los principios básicos del CEDH sobre transparencia, garantías procesales y participación del sector privado. En este se establecen pautas sobre el uso de filtros que suelen utilizar las empresas TIC en sus plataformas. Se remarca la protección de la libertad de expresión y la privacidad; requisitos para que el filtrado sea proporcionado y únicamente sea realizado por organismos públicos por las razones expuestas en el artículo 10.2 de la CEDH; y que las decisiones de bloqueo sean revisables por un tribunal independiente.

Estos nuevos principios expresan que los principios básicos del CEDH (o su jurisprudencia) pueden no estar regulados. Es decir, estos novedosos principios no han de transponerse obligatoriamente a una normativa estatal y únicamente se centran en expresar que todas las restricciones deben basarse en criterios claros, específicos y de acuerdo a una ley estatutaria accesible. Que las autoridades reguladoras que aplican las leyes que restringen la libertad de expresión deben ser totalmente independientes, responsables y aplicando las debidas garantías establecidas para evitar la arbitrariedad. Además, se requiere mayor transparencia y proporcionalidad en el bloqueo de Internet, y este debe efectuarse con notificación efectiva de la conclusión del debido proceso, y las partes interesadas deben tener la oportunidad de impugnar la decisión en procedimientos judiciales públicos.

Estos principios también tratan de la protección de los intermediarios de responsabilidad, además de la imposición de deberes a entidades del sector privado (como tales intermediarios) para defender la libertad de expresión, y, sobre todo tratan de garantizar el acceso ilimitado de Internet para todos los usuarios.

Sin embargo, ha habido dificultades para aplicar estos principios emergentes ya que, al no ser vinculantes, ningún Estado Miembro tiene la obligación de aplicarlos ni introducirlos en sus ordenamientos jurídicos, quedando su mención relegada a pocas declaraciones.

Esta problemática podría resolverse mediante cambios menores en las normas existentes sobre responsabilidad de los intermediarios. De esta forma, estos principios emergentes de gobernanza de Internet se volverían legalmente exigibles.

Dicho esto, es relevante remarcar que lo mencionado anteriormente es realizado desde una perspectiva europeísta. Mientras que en la Unión Europea se intenta regularizar todo el proceso de protección de los derechos fundamentales desde la raíz (entrando en el funcionamiento de las políticas de las redes sociales), pasando el charco nos encontramos con una visión diferente.

Desde la perspectiva del *Common Law*, exactamente norteamericana⁵³, propugnan una reforma de la legislación sobre la privacidad *online*, y exclaman que la confianza y seguridad del consumidor es indispensable para que las redes sociales sigan siendo rentables. Por ello, piensan que lo ideal sería una legislación que imite los principios de la Declaración de Derechos de Privacidad del Consumidor porque así mejorará la confianza del consumidor. Además, se equilibraría de forma flexible la necesidad de innovación económica y la necesidad social de protección de la privacidad. Por lo tanto, ellos propugnan una regulación básica de la protección de la Privacidad, relegando el resto de cuestiones al ámbito privado y confiando en el transcurso natural de las relaciones y los negocios.

Finalmente, se ha comprobado que la Unión Europea es consciente de la importancia de una buena regulación e instauración clara de Derechos digitales. Así lo expresan en el proyecto de Declaración de Derechos digitales⁵⁴; en ella mencionan los derechos y principios de solidaridad e inclusión, la ampliación de seguridad y el desarrollo de la sostenibilidad. Y sobre la materia que atañe a este trabajo sobre violencia de control: el empoderamiento de los usuarios, el carácter céntrico de las personas y sus derechos y la garantía de la libertad de elección *online*. Con rasgos semblantes se encuentra también la propuesta de Carta de Derechos Digitales⁵⁵ del Gobierno de España, donde propugnan por mantener la cultura arraigada de los derechos fundamentales que tanto caracteriza al ordenamiento jurídico español, pero completándola en los espacios y entornos digitales.

3.3 Posibilidades que tienen las mujeres de prevención y protección ante el abuso online

Una vez analizada la amalgama de legislación vigente, nos encontramos con la incógnita que aún no está resuelta: en el caso de ser una víctima de control *online*, ¿qué posibilidades de protección tiene? Normalmente se aconseja que se evite la comunicación con los acosadores mediante redes sociales o teléfono móvil y se denuncie. No obstante, ha quedado acreditado que no es suficiente al no haber una protección integral de la víctima en el ámbito de redes sociales.

⁵³ Rizk, H. (2013). Fundamental right or liberty: online privacy's theory for co-existence with social media. *Howard Law Journal*, 56(3), 951-982.

⁵⁴ *Declaration on digital rights and principles*. (2022, January 26). European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452

⁵⁵ Gobierno de España. (n.d.). Carta de Derechos Digitales. *Plan de Recuperación, Transformación y Resiliencia*. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

A lo largo del trabajo se han proporcionado diferentes vías de protección, así como de prevención sobre estas conductas controladoras (ya sea a través de la típica denuncia a las autoridades o mediante las mismas plataformas de las redes sociales, así como a través de asociaciones civiles o gubernamentales).

A estos efectos, considero relevante proporcionar en conjunto todas estas vías para que las posibles personas que estén leyendo este trabajo y se encuentren en esta situación, sepan exactamente dónde informarse y qué hacer exactamente. De esta forma y resumidamente:

- Por parte del Estado nos encontramos con la denuncia que puede interponer la víctima ante las autoridades policiales y las siguientes medidas cautelares y de protección que puede adoptar el juez en virtud de la Ley Orgánica 1/2004 y el artículo 544 de la Ley de Enjuiciamiento Criminal. Aunque ya hemos visto que estas medidas de protección no son eficientes para el abuso y control *online*.
- Todas las plataformas online acreditadas (incluidas Facebook, Instagram y Twitter) presentan políticas estrictas contra el acoso y el abuso *online* y permiten denunciar contenido o usuarios abusivos/ofensivos. El objetivo no es solo eliminar el contenido ofensivo, sino también garantizar que se desactiven las cuentas de usuario abusivas. Desafortunadamente, estas plataformas no siempre responden rápidamente, por lo que vale la pena considerar emprender acciones legales al mismo tiempo. Los links de interés ante el abuso online sobre las redes sociales más usadas son las siguientes:
 - <https://www.whatsapp.com/legal/privacy-policy-eea#privacy-policy-working-with-authorities>
 - <https://faq.whatsapp.com/general/security-and-privacy/unauthorized-use-of-automated-or-bulk-messaging-on-whatsapp>
 - https://es-la.facebook.com/help/1381617785483471/?helpref=uf_share
 - https://es-la.facebook.com/help/131920223550312/?helpref=uf_share
 - <https://help.twitter.com/es/safety-and-security/cyber-bullying-and-online-abuse>
- Además, encontramos Instituciones, asociaciones y páginas web que proporcionan información o ayudas, como pueden ser:
 - Desde el Gobierno de España, concretamente la Delegación del Gobierno contra la Violencia de Género: <https://violenciagenero.igualdad.gob.es/profesionalesInvestigacion/asistenciaSocial/recursos/orden/home.htm>
 - Desde la Agencia Española de Protección de Datos: <https://www.aepd.es/es/areas-de-actuacion/recomendaciones>

- Una de las pocas asociaciones sin ánimo de lucro en España que tratan la Violencia de Género online: <https://stopviolenciadegenerodigital.com/>
- Si vives en Estados Unidos, una de las asociaciones más relevantes e influyentes (y muy completa) es: <https://www.womenslaw.org/about>
- En cambio, si vives en Reino Unido, encontramos una asociación muy similar y útil: <https://www.womensaid.org.uk/>

4. CRÍTICA ANTE LA SITUACIÓN ACTUAL Y POSIBLES SOLUCIONES

Se ha constatado mediante el análisis del ordenamiento jurídico español que, aunque exista cierta regulación que ampare los derechos de las mujeres ante cualquier tipo de abuso *online*, la protección que proporciona la misma no es suficiente ni integral. Esta regulación ineficiente conlleva a perpetuar este subtipo de violencia de género y continuar con la misma problemática inicial: no se garantiza ni la seguridad ni la protección adecuada de la víctima de violencia de control en el campo virtual.

A continuación, se pretenden proporcionar posibles soluciones ante las problemáticas que se han ido abarcando. El orden que se seguirá está basado en el mismo patrón que se ha seguido para presentar el trabajo: primero, se tratará la situación comunitaria; segundo, la situación estatal; y en último lugar, la situación del sector privado y las plataformas de redes sociales.

En relación a la situación general de la Unión Europea, no encontramos una regulación uniforme ni específica. Sobre el campo tecnológico, la regulación base sería el *Convenio sobre la Ciberdelincuencia del 2001*, pero no trata exactamente ni pone un especial interés en la situación de las mujeres cuando son víctimas de abuso *online*.

Sobre la situación de las mujeres, la regulación que se acerca más a su realidad es el *Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica de 2011*, aun así, no mencionan en ningún momento alguna protección específica ante las conductas reprochables en Internet. Esta regulación ha servido de base para que los Estados miembros regulen estas conductas que tanto preocupan, pero perpetúan el mismo problema que nos encontramos con la regulación comunitaria: concretamente, el abuso *online* sobre las mujeres no es tratado en ninguna disposición, lo que provoca un vacío legal ante tal problema.

La posible solución que se ha ideado frente a este asunto puede ser, en primer lugar, la complementación⁵⁶ de estas dos normas base, con la finalidad de que los Estados Miembros legislen sobre la violencia de control *online*, colmando esta laguna. Esto se puede conseguir de una forma muy sencilla ya que solo requiere la pronunciación de los legisladores comunitarios mediante un informe sencillo.

De una forma más utópica y típica, la segunda solución que se puede proponer es que el legislador comunitario ponga esta problemática sobre la mesa y así se empiece a debatir una nueva regulación a nivel comunitario sobre las conductas tecnológicas que quedan impunes y que tantos problemas causan. Así, las múltiples regulaciones quedarían comprendidas de forma unitaria y sistemática y se condenarían las conductas que hasta ahora no se castigan debido a que no se incardinan en un tipo penal, como podría ser el delito de odio (desde la perspectiva de las regulaciones europeas)⁵⁷.

En relación a la situación estatal, nos encontramos que en España la regulación vigente es extensa: se ha redactado una Ley Orgánica unitaria sobre la protección de las víctimas de violencia de género, así como una disposición específica en la Ley de Enjuiciamiento Criminal para garantizar los derechos de las partes en el proceso judicial. Se ha demostrado que estas regulaciones proporcionan únicamente soluciones para el campo analógico, ninguna para el ámbito tecnológico, lo que conlleva a la misma solución mencionada anteriormente: no existe protección eficiente para las víctimas de control y abuso *online*.

En relación a la actividad gubernamental y asociaciones civiles, nos encontramos con que estas actuaciones son muy dispares y no están conectadas ni coordinadas entre sí. Mientras que la Delegación del Gobierno contra la Violencia de Género no enfoca (ni menciona) ninguna medida de protección *online*, la Agencia Española de Protección de Datos únicamente se limita a no intervenir desde su ámbito de actuación, así, ante cualquier intervención, se limitan a remitir a los links de las plataformas de las redes sociales para que las víctimas se informen mediante estos.

⁵⁶ Esta idea ha sido también apoyada por el Consejo de Europa, y encontramos esa fundamentación en las opiniones expresadas en: Van der Wilk, A. (2021). The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. *PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE*. <https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44>

⁵⁷ Esta solución también se ha expresado en Barker, K., & Jurasz, O. (2020). Online violence against women as an obstacle to gender equality: A critical view from Europe. *European Equality Law Review*, 2020(1), 47-60.

En el caso de las regulaciones dispares y anticuadas, una solución factible sería la actualización y/o renovación⁵⁸ de la legislación (tanto la Ley Orgánica como la Ley de Enjuiciamiento Criminal). Es decir, no basta con emitir una guía práctica (como la del 2016 del CGPJ) que tenga la finalidad de utilizar la tecnología como un instrumento agilizador del proceso judicial. La agilización es muy necesaria, pero lo preciso para la protección integral y real de la víctima sería esta nueva regulación a fin de actualizar los conceptos y adaptarse a los nuevos tiempos que estamos viviendo donde hemos dejado claro que las redes sociales son un pilar fundamental de nuestra comunicación, y a la vez un peligro si no se tratan con cautela.

Sobre la actuación gubernamental, una solución plausible es la cooperación⁵⁹ real entre la Delegación del Gobierno contra la Violencia de Género y la Agencia Española de Protección de Datos, con la finalidad de dar una protección efectiva a las mujeres víctimas de violencia de género y de control dentro del campo de Internet. Esta cooperación es ideal ya que la Agencia Española tiene su ámbito de actuación dentro del plano tecnológico y trata uno de los bienes que son más perjudicados ante estas actuaciones tecnológicas que constituyen el abuso *online*: los datos personales de las víctimas de violencia de control.

Asimismo, siguiendo con la actuación gubernamental y sus posibles soluciones, vemos correcta la creación de una asociación civil que esté constituida con ayudas gubernamentales⁶⁰. De esta forma, la asociación y sus actuaciones serían llevadas a cabo por profesionales privados de diferentes ámbitos que se encargarían de la protección, seguridad y otros actos *ex ante* y *ex post* sobre la víctima. No obstante, es ideal que, a la vez, la Delegación del Gobierno mantenga el

⁵⁸ Esta solución también ha sido propuesta en: Merino Sancho. (2019). La (a)simetría de género en el concepto de violencia: una propuesta de reforma de la Ley Orgánica 1/2004 tras el Convenio de Estambul. *Anuario de filosofía del derecho*, 35, 93–126.

⁵⁹ Este razonamiento indicando la necesidad de cooperación entre organismos para una mayor eficiencia a la hora de abordar la problemática de violencia de género y control se encuentra (desde el ámbito sociosanitario, aunque indicando la misma problemática y solución): Germán Calvo González, & Rafaela Camacho Bejarano. (2014). La violencia de género: evolución, impacto y claves para su abordaje/Gender violence: trends, impact and keys for approach. *Enfermería global*, 13(1), 424–.

Asimismo, encontramos esta solución ya implementada en España con el *Convenio de colaboración entre Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad y la Agencia Española de Protección de Datos*. No obstante, la ineficiencia de este Convenio ante la protección *ex post* de la víctima ha de sugerir un nuevo replanteamiento del Convenio.

⁶⁰ La solución ha sido inspirada por el interés que tiene la asociación inglesa *Women's Aid* en recibir ayudas gubernamentales para así fomentar la cooperación con el Gobierno y además profesionalizar el trato que realizan a las víctimas. Así lo han expresado en: Hadley, L. (n.d.). *Tackling domestic abuse in a digital age*. Women's Aid. <http://www.womensaid.org.uk/wp-content/uploads/2015/04/APPGReport2017-270217.pdf>

contacto con esta asociación para así, por ejemplo, cuando se presente una denuncia a las autoridades, el caso sea llevado a cabo de forma conjunta entre la asociación y las autoridades.

De esta forma, opino que la carga de trabajo se compensa entre las autoridades estatales y la asociación y las actuaciones son más eficientes porque cada persona trabaja sobre su ámbito especializado y todas las necesidades estarían cubiertas entre estas dos entidades. O si el caso no llega a ser denunciado, que al menos la Delegación mantenga una revisión periódica de los casos con la asociación. Así, desde el Gobierno se toma consciencia de las necesidades reales de las víctimas en cada momento y en base a ello se podrá legislar teniendo en cuenta estos datos.

En relación a la situación actual del sector privado, se ha visto cómo cada una de las plataformas de cada red social es una empresa privada, las cuales tienen su regulación y sus políticas internas propias. En base a estas mismas regulaciones, cada empresa decide qué medidas de protección cree oportunas ante el abuso *online*. Se ha comprobado que hay multiplicidad de opciones, pero la mayoría utilizan el mecanismo del bloqueo o la denuncia del perfil abusador, lo cual se ha demostrado que no neutralizan completamente la conducta abusadora, y ante ello, la víctima no tiene ulteriores mecanismos de protección además de la denuncia analógica (la cual ya hemos contemplado que no protege integralmente a la víctima ante ataques *online*).

Con ello, una solución ante esta problemática sería que las plataformas revisaran sus políticas internas y se enfocaran más en actualizarlas desde una perspectiva protectora hacia las víctimas de este tipo de abuso. No obstante, esta idea ha quedado obsoleta viendo los resultados de Facebook, los cuales proclamaron la revisión de sus políticas para mejorar esta problemática, pero la Revista de Wall Street ha constatado que en la práctica estos cambios han sido muy poco eficientes⁶¹.

Acorde a lo anterior, considero que la opción más eficiente sería aquella que respetase la idea de que las entidades deben desempeñar un papel clave en la protección de los Derechos Fundamentales no solo de la víctima, sino también del abusador. Por lo que opino que la cooperación entre empresas y autoridades estatales de cada país debe de ser vital para asegurar

⁶¹Información extraída de la página web: Goujard, C. (2021, September 30). *Advocates have a message for social media platforms: Protect women*. POLITICO <https://www.politico.eu/article/advocates-have-a-message-for-social-media-platforms-protect-women/>

la protección eficiente de la víctima de violencia de control y la garantía de los derechos de todos los usuarios de Internet.

No obstante, al ser conscientes de la heterogeneidad de herramientas virtuales y de regulaciones (así como de pautas éticas no vinculantes utilizadas en las mismas regulaciones de plataformas de redes sociales), puede plantearse la posibilidad de reincorporar en el Derecho existente (tanto comunitario, como estatal o internacional) la figura del Defensor del Pueblo u *Ombudsperson*⁶² (*Ombudsman* o Defensor del Pueblo de Internet). Actualmente, numerosos países han sugerido la introducción de este instrumento con la finalidad de que este sirva como un mecanismo de rendición de cuentas de organizaciones e instituciones privadas, públicas y gubernamentales en sus actuaciones relativas a la protección *online*.

Además, para materializar lo mencionado sobre el *Ombudsperson*, considero que lo más correcto sería la creación de una entidad privada independiente que proteja los intereses de los usuarios de Internet, y a la vez los intereses de las empresas.

La idea ha sido inspirada no solo por la figura del Defensor del Pueblo de Internet (*Ombudsperson*), sino también por la figura de la Comisión Nacional de Mercados y la Competencia. Esta Comisión ejerce la labor de supervisión, análisis y regulación de la competencia que actúa sobre múltiples mercados y ámbitos. Está adscrita al Ministerio de Asuntos Económicos y Transformación Digital, tiene personalidad jurídica propia y plena capacidad pública y privada. Con esta forma, es un organismo público, independiente del Gobierno y que además está sometido al control parlamentario y judicial.

Opino que la creación de una Comisión semejante a la CNMC⁶³ sería muy eficiente debido a que esta Comisión ya existente se encarga de supervisar un ámbito que tiene unas características muy parecidas al ámbito tecnológico: varía rápidamente y es muy volátil pero a la vez siempre deja una huella en el campo donde se desarrolla. Por ello considero que la creación de una Comisión⁶⁴ que se encargase de la regulación y control de las conductas de los usuarios en

⁶² Daskal, Wentrup, R., & Shefet, D. (2020). Taming the Internet Trolls With an Internet Ombudsperson: Ethical Social Media Regulation. *Policy and Internet*, 12(2), 207–224. <https://doi.org/10.1002/poi3.227>

⁶³ (n.d.). Comisión Nacional de los Mercados y la Competencia | CNMC. <https://www.cnmc.es/node>

⁶⁴ Esta idea sobre crear una Comisión para solventar los problemas que hemos ido mencionando no solo se inspira en la figura de la Comisión Nacional de los Mercados y la Competencia, sino también en la figura de la Junta de Supervisión de Facebook e Instagram:

Klonick, K. (2020). The facebook oversight board: creating an independent institution to adjudicate online free expression. *Yale Law Journal*, 129(8), 2418-249

Internet promovería un mejor funcionamiento del ámbito tecnológico en nuestro país ya que la problemática de la falta de específica regulación se solventaría con la actuación de esta porque parte de la actuación del poder judicial se trasladaría a esta. Además, al tener personalidad jurídica propia podría estar facultada a emitir las sanciones pertinentes y estaría controlada tanto judicialmente como parlamentariamente.

También, la coordinación entre asociaciones y Gobierno (que citábamos antes) se realizaría de una forma más fehaciente porque ya estaría esta Comisión supervisaría y analizaría las actuaciones que se hacen en la red de Internet y que constituyen un daño/abuso hacia los usuarios, además de realizar la pertinente cooperación entre el sector privado y las autoridades estatales.

En este caso la Comisión no se limitaría a las actuaciones sobre las mujeres usuarias, sino también hacia los hombres que no hemos de negar que también sufren abusos y control; pero sí es cierto que habría un enfoque importante a aquellos actos que promuevan la violencia hacia la mujer en este ámbito.

CONCLUSIONES:

Con este análisis se ha concluido, además de existir muchos estudios⁶⁵ sobre ello, que la violencia psicológica o de control es de las más habituales en el ámbito de las relaciones de pareja y tiene graves consecuencias en las víctimas. Resulta muy difícil de detectar y se manifiesta mediante amenazas, intimidación, aislamientos, actuaciones que pretenden confundir a la víctima o la utilización de la denominada violencia por poderes. Esta violencia es conocida como violencia controladora coactiva o “terrorismo íntimo”, y tiene una especial repercusión en el ciberespacio⁶⁶, donde los usuarios controladores pueden alcanzar su objetivo dañino con mayor facilidad que en el campo analógico. Este tipo de violencia está relacionada con situaciones de afectación psíquica y de lesión al honor, a la intimidad y a la integridad moral, lo que conlleva a una violencia simbólica. Esta actuación es peligrosa porque se trata de una actuación intensa y continuada, y a través del entorno tecnológico se favorece el mantenimiento y el fomento de la situación de sometimiento y control de la mujer.

Este tipo de violencia en el campo tecnológico tiene una mayor repercusión en las personas que mantienen una relación personal. Así se ha manifestado en los Informes de la Memoria de la Fiscalía del Estado⁶⁷. En ellos se constata que la tecnología genera más relaciones virtuales, y en estas se están percibiendo nuevas formas de control y de acoso que muchas veces no se castigan por la dificultad de subsumir estas acciones en los tipos penales y por no apreciarlas como gravemente lesivas para los bienes jurídicos. Por esto, se está observando un aumento de denuncias de menores por delitos de violencia de género, las cuales se singularizan por ser actos con pautas de control y dominación sobre la mujer.

⁶⁵ Pérez Martínez, V. T., & Hernández Marín, Y. (2009). La violencia psicológica de género, una forma encubierta de agresión. *Revista Cubana de Medicina General Integral*, 25(2), 0-0.

Echeburúa, E., & Muñoz, J. M. (2017). Límites entre la violencia psicológica y la relación de pareja meramente disfuncional: implicaciones psicológicas y forenses. *Anales de Psicología/Annals of Psychology*, 33(1), 18-25.

López Angulo, L., Fundora Quintero, Y., Valladares González, A., Ramos Rangel, Y., & Blanco Fleites, Y. (2015). Prevalencia de la violencia física y psicológica en relaciones de pareja heterosexuales: una explicación necesaria. *Revista Finlay*, 5(3), 161-169.

⁶⁶ Muñoz, J. M., & Echeburúa, E. (2016). Diferentes modalidades de violencia en la relación de pareja: implicaciones para la evaluación psicológica forense en el contexto legal español. *Anuario de psicología jurídica*, 26(1), 2-12.

⁶⁷ FISCAL GENERAL DEL ESTADO EXCMA. SRA. DOÑA CONSUELO MADRIGAL MARTÍNEZ-PEREDA. (n.d.). Memoria. https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/recursos/pdf/MEMFIS16.pdf

Con este reflejo de la situación actual de la sociedad española, nos encontramos con que las víctimas de violencia de género y de control pueden denunciar a las autoridades policiales y se aplicarán las medidas de protección de la Ley Orgánica 1/2004 o el artículo 544 de la Ley de Enjuiciamiento Criminal.

Tristemente, actualmente todas estas medidas son de carácter analógico y no se prevé una actualización de la normativa ni una propuesta de regulación que prevea la renovación de estas medidas de protección y/o cautelares.

Ello provoca una desprotección integral de la víctima en el campo virtual. En consecuencia, la víctima habrá de protegerse por sí misma: buscando ayuda en asociaciones civiles, a la Delegación del Gobierno contra la Violencia de Género, o utilizando los mecanismos que le proporcionan las plataformas digitales de cada red social.

Estos mecanismos de protección que facilita cada red social son muy diversos, pero en general se decantan por elegir el bloqueo de la cuenta abusadora o la denuncia a la propia plataforma de la red social (informando del mismo abuso).

Se puede visualizar cómo estas vías no proporcionan una protección integral a la víctima, ya que el abusador puede seguir creándose cuentas falsas para mantener el control sobre la víctima y seguir comunicándose con la misma. Las propias plataformas presentan limitaciones ante sus propias actuaciones, y ello es debido a que se debe garantizar en todo momento los derechos fundamentales de todos los usuarios. De esta forma, al encontrarnos ante un conflicto de Derechos Fundamentales, la ponderación entre el derecho a la intimidad y la propia imagen de la víctima, y el derecho a la libertad de expresión del abusador finaliza con la conclusión de que se ha de garantizar también el derecho a la libertad de expresión. Por ello y haciendo referencia a los principios de *Internet governance* (cuyo objetivo es evitar estas vulneraciones de derechos), no se puede limitar de forma tan exhaustiva el derecho a la libertad de expresión porque ello conllevaría arrebatar la posibilidad de que un usuario pueda crear una cuenta en cualquier red social, y siempre ha de prevalecer en cualquier caso el acceso ilimitado de Internet para todos los usuarios, sin discriminación.

Con todo ello, nos encontramos ante esta situación tan heterogénea, ambigua y problemática no solo desde el ámbito comunitario, sino también desde el ámbito estatal y desde el sector privado. De esta forma, creemos correcta no solo la implementación de mecanismos eficientes, reales e integrales para las víctimas de violencia de género y de control tecnológico (ya sea en la

actualización de la misma Ley Orgánica 1/2004 o creando nueva regulación), sino también una coordinación y cooperación entre las autoridades estatales y las plataformas de cada red social. Las entidades del sector privado, como controlan gran parte de lo que sucede en Internet también deben desempeñar un papel clave en la protección de las víctimas, y por ello considero que esta cooperación con las autoridades ayudaría en gran medida a realizar una implementación/regulación práctica y eficiente de medidas que ayuden a proteger de forma real e integral a las víctimas de violencia de control en el campo tecnológico.

En definitiva, considero que la solución más eficiente a efectos prácticos sería la creación de una entidad similar, o a la Comisión Nacional de Mercados y la Competencia, o al Defensor del Pueblo de Internet (*Ombudsperson*). Es decir, un organismo público con personalidad jurídica propia, independiente del Gobierno y que además esté sometido al control parlamentario y judicial y cuyo principal objetivo sea la protección de los intereses de todos los usuarios de Internet y los intereses de las empresas. Con ello, la cooperación entre el sector privado y el sector público se realizarían de una forma más sencilla porque la entidad actuaría de intermediario entre ellos.

Así, la protección de las víctimas de violencia de control tecnológico se materializaría de forma correcta, enfocando y atribuyendo la competencia del asunto de violencia de género y de control *online* a esta entidad. De esta forma, la resolución del conflicto se atribuye a esta entidad especializada en el funcionamiento de Internet. Esta, al tener la competencia de control de los comportamientos *online*, se facilitaría la persecución de los mismos que perpetúen un abuso. En consecuencia, se conseguiría la reducción de los casos de desprotección de las víctimas y se impediría la violencia de control que tanto preocupa actualmente en el ámbito de las nuevas tecnologías y redes sociales.

BIBLIOGRAFÍA:

- Ariadna Martín Montilla, María Pazos Gómez, María del Valle Cecilia Montilla Coronado, & Cristina Romero Oliva. (2016). UNA MODALIDAD ACTUAL DE VIOLENCIA DE GÉNERO EN PAREJAS DE JÓVENES: LAS REDES SOCIALES. *Educación XXI*, 19(2), 405–429.
- Barker, K., & Jurasz, O. (2020). Online violence against women as an obstacle to gender equality: A critical view from Europe. *European Equality Law Review*, 2020(1), 47-60.
- Borrajo, E., Gámez-Guadix, M., Pereda, N. y Calvete, E. (2015c). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior*, 48, 358-365
- Chadha, Steiner, L., Vitak, J., & Ashktorab, Z. (2020). Women’s Responses to Online Harassment. *International Journal of Communication (Online)*, 239–.
- Daskal, Wentrup, R., & Shefet, D. (2020). Taming the Internet Trolls With an Internet Ombudsperson: Ethical Social Media Regulation. *Policy and Internet*, 12(2), 207–224. <https://doi.org/10.1002/poi3.227>
- *Declaration on digital rights and principles*. (2022, January 26). European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452
- Echeburúa, E., & Muñoz, J. M. (2017). Límites entre la violencia psicológica y la relación de pareja meramente disfuncional: implicaciones psicológicas y forenses. *Anales de Psicología/Annals of Psychology*, 33(1), 18-25.
- Elmer, Neville, S. J., Burton, A., & Ward-Kimola, S. (2021). Zoom Bombing During a Global Pandemic. *Social Media + Society*, 7(3), 205630512110353–. <https://doi.org/10.1177/20563051211035356>
- European Commission. (n.d.). EUROPEAN COMMISSION Brussels, 25.1.2012 SEC(2012) 72 final COMMISSION STAFF WORKING PAPER Impact Assessment Accompanying the document Regulation of the European Parliament and of t. https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf
- European Parliament, Directorate-General for Internal Policies of the Union, Dizdarevic, I., Cucu, V., Ribeiro Oertel, R. (2020). *Violencia contra las mujeres: violencia psicológica y control coercitivo: síntesis*, European Parliament. <https://data.europa.eu/doi/10.2861/86732>
- Fox, C.L. y Warber, K. (2014). Social networking sites in romantic relationships: Attachment, uncertainty, and partner surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 7(1), 3-7.
- Germán Calvo González, & Rafaela Camacho Bejarano. (2014). La violencia de género: evolución, impacto y claves para su abordaje/Gender violence: trends, impact and keys for approach. *Enfermería global*, 13(1), 424–.

- Goujard, C. (2021, September 30). *Advocates have a message for social media platforms: Protect women*. POLITICO <https://www.politico.eu/article/advocates-have-a-message-for-social-media-platforms-protect-women/>
- Gobierno de España. (n.d.). Carta de Derechos Digitales. *Plan de Recuperación, Transformación y Resiliencia*. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf
- Hadley, L. (n.d.). *Tackling domestic abuse in a digital age*. Women's Aid. <http://www.womensaid.org.uk/wp-content/uploads/2015/04/APPGReport2017-270217.pdf>
- Image-based Abuse: Debate and Reflections on the “Iveco Case” in Spain on Twitter. (2020). *Journal of Interpersonal Violence*, 886260520967143–886260520967143. <https://doi.org/10.1177/0886260520967143>
- Internet Governance Forum, & United Nations. (n.d.). the charter of human rights and principles for the internet. *Internet Rights & Principles Coalition*. <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>
- Keller, Schoch, D., Stier, S., & Yang, J. (2020). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication*, 37(2), 256–280. <https://doi.org/10.1080/10584609.2019.1661888>
- Klonick, K. (2020). The facebook oversight board: creating an independent institution to adjudicate online free expression. *Yale Law Journal*, 129(8), 2418-249
- Lloria García, P. (2020). *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*. Iustel.
- Lloria García, P. (2006). *Aproximación al estudio del delito permanente*. Comares. Pp. 124-126
- López Angulo, L., Fundora Quintero, Y., Valladares González, A., Ramos Rangel, Y., & Blanco Fleites, Y. (2015). Prevalencia de la violencia física y psicológica en relaciones de pareja heterosexuales: una explicación necesaria. *Revista Finlay*, 5(3), 161-169.
- López-Barajas Perea, I. (2017, Febrero). Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos. *Revista de Internet, Derecho y Política*.
- Mansouri, O. (2021). Protection of Personal Data in Social Media (Comparative Analysis). *International Review of Law*, 9(3). <https://doi.org/10.29117/irl.2020.0124>
- McGlynn, C., & Rackley, E. (2016). Not “revenge porn,” but abuse: Let’s call it image-based sexual abuse. <https://inherentlyhuman.wordpress.com/2016/02/15/>

- Merino Sancho. (2019). La (a)simetría de género en el concepto de violencia: una propuesta de reforma de la Ley Orgánica 1/2004 tras el Convenio de Estambul. *Anuario de filosofía del derecho*, 35, 93–126.
- Mery, H. C. (2021). The dangers of doxing and swatting: why Texas should criminalize these malicious forms of cyberharassment. *St. Mary's Law Journal*, 52(3), 905-944
- Muñoz, J. M., & Echeburúa, E. (2016). Diferentes modalidades de violencia en la relación de pareja: implicaciones para la evaluación psicológica forense en el contexto legal español. *Anuario de psicología jurídica*, 26(1), 2-12.
- Pérez Martínez, V. T., & Hernández Marín, Y. (2009). La violencia psicológica de género, una forma encubierta de agresión. *Revista Cubana de Medicina General Integral*, 25(2), 0-0.
- PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE. (n.d.). Coe. <https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44>
- Reed, L. A., Tolman, R. M. y Ward, L. M. (2017). Gender matters: Experiences and consequences of digital dating abuse victimization in adolescent dating relationships. *Journal of Adolescence*, 59, 79-89.
- Reznik M. Identity theft on social networking sites: developing issues of Internet impersonation. *Touro law review*. 2013; 29 (2):455–
- Rizk, H. (2013). Fundamental right or liberty: online privacy's theory for co-existence with social media. *Howard Law Journal*, 56(3), 951-982.
- Rosa María García Sanz. (2011). REDES SOCIALES ONLINE: FUENTES DE ACCESO PÚBLICO O FICHEROS DE DATOS PERSONALES PRIVADOS (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas). *Revista de Derecho Político*, 81, 102–.
- Van der Wilk, A. (2021). The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women.
- Veletsianos, G., Houlden, S., Hodson, J., & Gosse, C. (n.d.). Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame. *SAGE*, 20(12), 4689 –4708.
- *Violencia de género, violencia machista y control coercitivo*. (n.d.). FutureLearn <https://www.futurelearn.com/info/courses/salud-de-la-mujer-en-el-postparto/0/steps/68332>

LEGISLACIÓN:

- Convenio sobre la Ciberdelincuencia, en Budapest el 23 de noviembre de 2001.
- Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica de 11 de mayo de 2011.
- Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género.
- Llei 5/2008, sobre el dret de les dones a erradicar la violència masclista.
- Artículo 544 bis y ter de la Ley de Enjuiciamiento Criminal.
- Código Penal, concretamente, los artículos 172, 197, 284 y 401.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.