FORO JURÍDICO

Cuestiones procesales acerca de la e-violencia de género

"(...) podríamos definir al agente encubierto en Internet como un empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la Red, que causen una gran repulsa y alarma a nivel social, tales como la e-violencia de género".

Federico Bueno de Mata*

Resumen: El constante cambio tecnológico en los medios de comunicación ha generado muchas particularidades de interés para los casos de violencia de género, o como Federico Bueno de Mata denomina: "e-violencia de género". Es así que identifica ciertas modalidades de este tipo de violencia, características del uso de las Tecnologías de la Información e Internet, para luego evaluar el aspecto procesal a seguir, donde la principal arista que se debe evaluar es si la violencia sucedió en un entorno virtual abierto o cerrado. Finalmente, da cuenta de la controversial tarea del "agente encubierto en Internet", funcionario público que deberá utilizar el "engaño" a fin de identificar las prácticas de e-violencia de género.

Palabras clave: Violencia de género, e-violencia, agente encubierto en Internet, ciberacoso, "sextorsión", TIC.

Abstract: The constant technological change in the media has generated a particular interest in many cases of gender-based violence, or as Federico Bueno de Mata says: "E-gender violence". First, it is identified certain forms of violence generated due the use of information technology and Internet, and then is analyzed the procedural aspect to follow, where the principal edge should be that whether the violence happened in an open virtual environment or a closed one. Finally realizes the controversial task of the "undercover online agent", public official who must use "deceit" to identify E-gender violence practices.

* Profesor Ayudante Doctor en el Área de Derecho Procesal de la Universidad de Salamanca.

Keywords: e-gender violence, e-violence, undercover online agent, stalking, bullying, sexting, information technology.

Sumario: 1. Las comunicaciones digitales y la violencia de género. 2. Tipos de violencia de género a través de Internet. 3. Tratamiento procesal de la violencia de género a través de Internet: 3.1. Mecanismo para iniciar el procedimiento; 3.2. Competencia; 3.3. Investigación policial y e-violencia de género: realidad actual y propuestas de futuro. 4. Reflexiones finales.

1. Las comunicaciones digitales y la violencia de género

En primer lugar, debemos ofrecer un concepto de esta nueva forma de ejercer la violencia de género y ver si la misma puede encuadrarse dentro del objeto de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género; o si, por el contrario, debemos modificar dicho texto legal para que contemple esta nueva realidad(1). De esta forma, al utilizar una vía electrónica como medio para desplegar el tipo delictual, dicha violencia nunca podría manifestarse de forma física al encontrarnos en un terreno propiamente virtual, por lo que descartaríamos el medio físico como forma de ejercicio y nos centraríamos en delimitar estos ataques como una nueva modalidad de ejercer violencia psicológica sobre las víctimas.

Así, todas estas conductas sí serían encuadrables dentro del artículo 1.3 de la citada Ley, pues entrarían dentro de su objeto de aplicación. Aun así, pensamos que sería conveniente, para mayor claridad, una reforma del precepto tendente a ampliar la extensión del objeto de aplicación, para que el mismo abarque también las nuevas manifestaciones delictuales que las tecnologías u otros recursos pudieran generar. Esta discusión, creemos, se zanjaría incorporando un apéndice a la redacción de este tercer punto del artículo 1°, quedando redactado de la siguiente manera: "(…) la presente Ley comprende todo acto de violencia física y psicológica, incluidas las agresiones a la libertad sexual, las amenazas, las coacciones o la privación arbitraria de libertad, con independencia del cauce, medio o instrumento utilizado para ejercerla". Con ello, ampliamos el objeto del articulado, adaptando la legislación a los tiempos actuales y garantizando la no obsolescencia del texto legal respecto al desarrollo futuro de la ciencia y la tecnología.

En segundo lugar, debemos delimitar quiénes podrían ejercer concretamente esta forma de violencia, ya que si seguimos analizando el texto legal, la ley regula las conductas de los hombres sobre las mujeres "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"(2). Debido a esto, solo se podrían considerar como tales, únicamente, a las agresiones de los mencionados sujetos en un espacio que conlleva unas posibilidades de anonimato exponencialmente mayores que el terreno físico como es el Internet. Así, quedarían fuera del mismo aquellos ataques anónimos o cuyo autor no se hubiera podido identificar de forma veraz y exacta, o incluso, aquellos que, una vez

(1) La última revisión de la LO 1/2004 está vigente desde 1 de enero de 2008, por lo que han pasado varios años sin actualizar dicho texto legal a la nueva realidad tecnológica y social.

(2) Así se muestra en el artículo 1.1. de la LO 1/2004 donde se regula el objeto de dicho texto legal.

identificados los autores, no mantengan o hubieran mantenido relaciones afectivas con las personas agraviadas por dichas conductas.

Esta sería una cuestión que dejaría sin sanción todas las conductas perpetradas por usuarios de chats, foros o redes sociales bajo perfiles falsos, a no ser que tras una denuncia se lograra identificar de forma fehaciente la autoría y que la misma estuviera relacionada con cualquiera de los sujetos contemplados en el art. 1.1 de la Ley 1/2004. Se parte, así, de que necesitaríamos tener controlada una dirección IP, fija o variable, de los presuntos autores en el caso de que no estuvieran localizados, ya que solo podríamos atribuir la autoría, y no con todas las garantías, a ataques realizados bien desde perfiles de Internet en redes sociales, correos electrónicos o foros debidamente autenticados; o bien a través de otras vías tecnológicas de comunicación como puede ser el envío de SMS, MMS, o Whatsapp desde números y terminales móviles atribuidos a dichas personas irrefutablemente.

Todos los ataques de este tipo inferidos por personas que no se encuadren dentro de este marco subjetivo seguirían siendo tipificados como delitos de amenazas, acosos, coacciones, extorsiones, etcétera, pero no como delitos de violencia de género realizados a través de las nuevas tecnologías.

Lo afirmado previamente nos lleva a ofrecer una definición de este nuevo tipo de violencia, tomando el concepto original de violencia de género, a la que denominaríamos "e-violencia de Género". Esta se podría definir como aquella violencia psicológica ejercida sobre la mujer por quien esté o haya estado ligado a ella por análoga relación de afectividad, aun sin convivencia, a través de cualquier medio tecnológico o electrónico, mediante conductas en el plano virtual consistentes en amenazas, humillaciones o vejaciones, exigencias de obediencia o sumisión, coerción, insultos, aislamiento o limitaciones de su ámbito de libertad, produciendo en la mujer desvalorización o sufrimiento[3].

2. Tipos de violencia de género a través de Internet

Una vez formulado el concepto de e-violencia de género y haber visto su alcance y extensión, debemos identificar la tipología de ataques que se encuadrarían dentro de este tipo delictual con el fin de demarcar y focalizar dichas actuaciones. De esta forma, las conductas más relevantes vinculadas a este tipo de violencia serían: el *ciberbullying*, el *stalking*, el *sexting* y la "sextorsión", palabras anglosajonas que cada vez son más oídas y utilizadas en España para denominar estas actuaciones, y que, al día de hoy, no tienen su denominación equivalente en castellano. Por lo tanto, vamos a analizar en qué consiste cada una de estas prácticas y ver si se contemplan o no en el Código Penal de nuestro país.

En primer lugar, la más conocida es el *ciberbullying*[4], lo que traducido al español sería algo así como el "acoso en línea" o el "ciberacoso". Este consiste en una agresión psicológica, sostenida y repetida en el tiempo, perpetrada por los sujetos del art. 1.1 de la LO 1/2004 contra su pareja o ex pareja, utilizando para ello las nuevas tecnologías. En este sentido, la conducta

(3) Adaptamos al terreno virtual la definición original dada de violencia de género en la Declaración sobre la Violencia Contra la Mujer (Resolución 48/104) aprobada en 1994 por Naciones Unidas, en Manual de legislación sobre la violencia contra la mujer, Nueva York, 2010, p. 5 y ss. Disponible en: https://www.un.org/womenwatch/daw/vaw/handbook/Handbook%20for%20legislation%20on%20VAW%20%28Spanish%29.pdf (Fecha de consulta 10 de noviembre de 2015).

(4) GUNDÍN, F. "Ciberbullying o ciberacoso: el oscuro lado criminal de las redes sociales", *Revista de Derecho Penal*, LexNova, Valladolid, Junio 2012, p. 4 y ss.

se podría realizar a través de cualquier plataforma o escenario virtual tales como el correo electrónico, los SMS, whatsapps, redes sociales, blogs o foros.

Pensamos que el término en castellano más acertado para referirnos a esta conducta de e-violencia de género es el de "ciberacoso", pues deja de ser un hostigamiento basado en una relación amorosa, debido a que el *ciberbullying* está más ligado socialmente a otro tipo de ámbitos como el escolar. Las víctimas de "ciberacoso", como las de acoso en la vida real, pueden llegar a sufrir diversos problemas de estrés, ansiedad, depresión, fatiga, perdiendo así la confianza en sí mismas, al sentirse, en determinadas ocasiones, vejadas o humilladas, dependiendo del comportamiento del ciberacosador; lo que constituye claramente una forma de violencia psíquica especialmente grave[5].

Este acoso está íntimamente relacionado con el resto de conductas que vamos a estudiar, aunque aparece especialmente vinculada con una de ellas, el *stalking* o acecho[6], que es una forma de acoso que consiste en la persecución ininterrumpida e intrusiva a un sujeto con el que se pretende restablecer un contacto personal en contra su voluntad, sirviéndose para ello de las Tecnologías de la Información y Comunicación[7]. Debemos tener en cuenta que este es un fenómeno que se recrudece según avanza la tecnología, al tener nuevas aplicaciones que permiten saber el tiempo que tarda en entrar una persona en una red social, o saber si los mensajes que se reciben en su móvil han sido leídos a través de determinadas *APPs*, lo que puede provocar consecuencias negativas a nivel psicológico muy parecidas a las producidas por el ciberacoso, ya que no deja de ser una derivación de la conducta anterior que puede afectar plenamente a las víctimas de violencia de género.

En tercer lugar, aparece una conducta que ha cobrado gran relevancia en España tras el mediático caso de la edil Olvido Hormigos[8] y que se conoce internacionalmente con la palabra *sexting*. Un vocablo, también tomado del inglés, que une "sex" (sexo) y "texting", que se vincula al envío de mensajes de texto vía SMS, MMS o similares, de imágenes de carácter sexual tomadas por el agresor o grabados por la protagonista de los mismos desde dispositivos móviles de comunicaciones, con el fin de dañar el honor e imagen de la mujer[9].

Por tanto, observamos que para que se genere este tipo de conducta delictual debe existir siempre una voluntariedad inicial de la propia víctima, debido a que, por regla general, dicho material con cierto contenido sexual es generado libremente por las propias mujeres o con su consentimiento en un momento anterior a la situación de conflicto, motivadas por la atracción o el "flirteo", por lo que no mediaría aquí coacción, miedo o cualquier elemento que vicie dicho consentimiento. Es decir, generalmente, la propia protagonista es la productora y primera difusora de estos contenidos.

(5) CHACÓN MEDINA, A. "Una nueva cara de Internet: el acoso". *Revista Ética-Net*, Granada, 2003, pp. 4-6.

(6) TAPIA, E. "Consecuencias y libertades de Internet", *Memorias del XIII Congreso Iberoamericano de Derecho e Informática, Versión CD*, Lima, Noviembre 2009.

(7) Folletos de la Serie Ayuda del Centro Nacional para Víctimas del Crimen *(National Center for Victims of Crime)*, Nueva York, 2002, disponible en el sitio web siguiente: http://www.ojp.usdoj.gov/ovc/foreignlang/spanish/help_series/pdftxt/StalkingVictimization_sp.pdf (Fecha de consulta 10 de noviembre de 2015).

(8) En esta web encontramos un gran reportaje sobre el sexting, relacionándolo con el caso de la edil, disponible en la web: http://www.eitb.com/es/noticias/sociedad/detalle/995082/sex-texting-que-es-sexting--envio-fotos-eroticas-movil/ (Fecha de consulta: 06 de noviembre de 2015). Olvido Hormigos es una concejal del PSOE víctima a finales del año 2012 de un delito de *sexting*.

(9) La plataforma española www.pantallasamigas.net/. es una de las páginas pioneras que explica qué es el sexting y la "sextorsión", las formas de producirlo, y cómo combatirlo. Dicha asociación tiene varios videos explicativos en Internet y en la plataforma Youtube explicando detalladamente de qué estamos hablando.

El problema se presenta cuando la pareja se separa y se utiliza ese material por parte de la ex pareja como un elemento para extorsionar, vejar o, incluso, chantajear a la mujer protagonista de las imágenes, con lo que nos encontraríamos ante una nueva conducta derivada del *sexting*, denominada "sextorsión". Por tanto calificaríamos de "sextorsión" al chantaje en el que alguien utiliza estos contenidos para obtener un retorno amoroso o sentimental de la víctima, o ejerciendo una situación de control o dominio sobre ella, amenazándola con la publicación de los mismos. De nuevo, tendremos que matizar que esta conducta se situaría dentro del fenómeno de la e-violencia de género, cuando los sujetos entren dentro del ámbito de aplicación del art. 1.1 de la Ley de Violencia de Género.

3. Tratamiento procesal de la violencia de género a través de Internet

3.1 Mecanismos para iniciar el procedimiento

Al encontrarnos dentro del orden jurisdiccional penal, las partes podrían iniciar el procedimiento a través de una denuncia o una querella, dependiendo de la naturaleza y alcance que hubiera tenido el delito. En este sentido, realizaremos aquí una diferenciación sobre si este tipo de conductas constituyen delitos públicos o privados.

¿Cómo haríamos para diferenciar el alcance de estas conductas? Todo depende del plano virtual en el que se cometa el delito. De esta forma, cuando éste hubiera tenido lugar dentro de un escenario virtual "abierto" como un foro, chat, red social, etcétera; es decir, en lugares donde dichas actuaciones podían ser vistas por parte de otros usuarios en la Red, se podría interponer denuncia del afectado o de cualquier persona que hubiera leído tales comentarios ofensivos o hubiera percibido cualquiera de las conductas descritas anteriormente. Al mismo tiempo, la víctima puede denunciar los hechos de las formas habituales, es decir, denunciando ante un órgano jurisdiccional o ante una comisaría. Sin embargo, también existe la posibilidad adicional de que las afectadas denuncien a través de las propias redes sociales, ya que en las más populares existe un "botón de pánico" que sirve para denunciar estos hechos y trasladar dicha información directamente a los Cuerpos y Fuerzas de Seguridad del Estado creados a tal efecto, los cuales mencionaremos a continuación.

Por otro lado, si los delitos de e-violencia de género se hubiesen cometido en un entorno virtual cerrado, tal como la mensajería instantánea a través de móviles o los mensajes privados de una red social, cabría la querella por parte de la propia víctima de estos delitos. En otras palabras, en estos casos, la investigación se iniciaría a instancia de la propia víctima.

Así, vemos que debido a las especiales características que ofrece Internet, el primer problema procesal que se nos plantea es el de diferenciar los espacios virtuales abiertos y cerrados, pues el instrumento para iniciar el procedimiento será diferente según cada caso.

3.2 Competencia

Siempre que se considere esta serie de conductas como delitos de violencia de género, tendríamos que remitirnos a lo regulado en el artículo 87.ter. de la Ley Orgánica 6/1985 del Poder Judicial del 1 de julio, por el que se modifica la LO 1/2004[10]. En el mismo, se indica que "los Juzgados de Violencia de la Mujer serán los encargados de instruir los procesos para exigir responsabilidad penal por delitos cometidos con violencia o intimidación contra quien sea o haya sido su esposa, o mujer que esté o haya estado ligada

(10) Boletín Oficial del Estado, núm. 313 de 29 de diciembre de 2004, pp. 42166 - 42197.

al autor por análoga relación de afectividad, aun sin convivencia; mientras que el fallo corresponderá a los juzgados de lo penal".

En el caso de que algunas de las conductas anteriormente señaladas se tipificaran como faltas, "el conocimiento y fallo de las mismas se atribuye también al juzgado de violencia sobre la mujer, siempre que sean cometidas contra las personas o contra el patrimonio cuando la mujer afectada esté o haya estado vinculada afectivamente al agresor, aún sin convivencia".

No obstante lo anterior, debemos hacer una reflexión previa y madurar la cuestión que en el caso de que tipificásemos estas conductas como faltas, se estarían asimilando estos hechos como vejaciones de carácter leve, cuestión que nos resultaría completamente desafortunada, debido a que tanto el *ciberbullying* como el *sexting* son actuaciones que se suelen repetir en el tiempo, es decir, tienen un bagaje temporal en el que se va dañando psíquica y gravemente a las personas ofendidas, de modo tal que se vulnera el honor e imagen de las mujeres agraviadas si las conductas se hacen en un entorno virtual público. De esta manera, creemos que toda conducta de violencia de género a través de Internet, por la propia naturaleza y características de estos delitos, nunca podrían ser consideradas como faltas y deberían ser tipificadas única y exclusivamente como delitos, tal y como ocurre con los delitos cometidos en el plano físico o real.

"La violencia de género a través de Internet suscita una serie de problemas en el plano procesal, aunque sustancialmente no deje de equipararse a cualquier otra acción de violencia de género […] Así, para iniciar el procedimiento a través de denuncia o querella, la particularidad consiste en diferenciar si las conductas se producen en un entorno virtual abierto o cerrado, optando por interponer una u otra según estemos en una de esas dos modalidades".

3.3 Investigación policial y e-violencia de género: realidad actual y propuestas de futuro

La investigación de los delitos de violencia de género cometidos a través de Internet corre a cargo de los Cuerpos y Fuerzas de Seguridad del Estado. Concretamente, se encargan de su investigación la Brigada de Investigación Tecnológica (BIT[11]) de la Policía Judicial y el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil[12].

La misión y fin de estos colectivos consiste en obtener las pruebas electrónicas oportunas para poder acusar y perseguir a los delincuentes y ponerlos a disposición judicial. De acuerdo a lo enunciado en sus páginas webs, las herramientas usuales que utilizan para descubrir a los autores son una cantidad de personal altamente preparado y la colaboración con instituciones públicas y privadas con alto impacto académico y profesional.

(11) La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales. <http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html>.

(12) El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet. Actualmente es miembro y participa activamente en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen, y en Europol. <https://www.gdt.guardiacivil.es>.

En los casos en los que los delitos estuvieran practicados en escenarios virtuales cerrados, solo cabría la investigación policial si hubiera existido previamente una querella. Sin embargo, si imaginamos que estos ataques se producen en escenarios virtuales públicos tales como chats o perfiles de redes sociales públicos, queremos proponer la adopción de una nueva y novedosa figura de la que se podría valer la investigación policial en los casos de e-violencia de género, siempre que se le dote de una regulación específica y particularizada: la figura del agente encubierto en Internet. Este agente podría presenciar virtualmente dichos actos, pudiendo así llegar a ser una figura nueva que superaría a los "ciberrastreos", y que cumpliría la función principal de estos cuerpos, consistente en velar por la seguridad de los internautas y de los ciudadanos en general. Los "ciberrastreos" estaban pensados para investigar intercambio de archivos en redes P2P, como *Emule, Kaaza* o *Elephant,* pero ahora necesitamos otro tipo de investigación más personal y directa, valiéndonos de las ventajas aportadas por la figura de los agentes encubiertos en Internet[13].

La figura del agente encubierto para infiltraciones en terrenos físicos, encuentra su regulación en el artículo 282.bis. de la Ley de Enjuiciamiento Criminal, gracias a una reforma en materia de perfeccionamiento de la actividad investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, efectuada por Ley Orgánica 5/1999 del 13 de enero. El problema con el que nos topamos aquí y que nos lleva a una situación de vacío legal, es que dicho artículo establece un *numerus clausus*[14] o enumeración tasada de delitos. Esto impide la investigación encubierta en otros tipos delictivos existentes y llevados a cabo por la criminalidad organizada, lo cual resulta muy poco operativo, preocupante y crea dificultades prácticas innecesarias. Aun así, a finales del mes de marzo de 2011, el Senado aprobó regular la figura del agente policial encubierto en Internet en investigaciones contra la pornografía infantil y la pedofilia[15], por lo que ya se utilizaría esta figura para combatir el delito de *grooming*, visto anteriormente, y abriríamos el debate de si debemos o podríamos ampliar sus competencias para intentar combatir otras conductas tales como el *ciberbullying*, el *sexting* o el *stalking*.

Por todo ello, con el avance constante que tiene la tecnología, consideramos un error realizar una lista tasada de delitos a los que hacer frente con esta figura y nos decantaríamos más por establecer aquí un sistema de *numerus apertus* basado en categorías de delitos y no en figuras concretas; por lo que estaríamos hablando siempre de "compartimentos abiertos", para evitar, de este modo, clasificaciones que queden rápidamente desfasadas. Por todo ello, si extrapolamos el concepto del agente encubierto en el terreno físico y lo llevamos al plano virtual, podríamos definir al agente encubierto en Internet como un empleado o funcionario público[16] que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de

(13) BUENO DE MATA, F. "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia", *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal (I Internacional) A Coruña, 2 y 3 de junio de 2011,* PÉREZ-CRUZ MARTÍN, A. (dir)., FERREIRO BAAMONDE, X. (dir). A Coruña: Universidade, 2012, pp. 295-306.

(14) Vid. RIFÁ SOLER, J. M. se cuestiona si el listado recoge numerus apertus o clausus, en "El agente encubierto o infiltrado en la nueva regulación de la LECrim"., Poder Judicial, núm. 55, p. 161. Nosotros entendemos que es una lista cerrada y tasada.

(15) Vid. <http://www.tecnoupdate.com.ar/2011/03/21/espana-agentes-encubiertos-en-internet-contra-la-pedofilia/> (fecha de consulta: 13 de Abril de 2011).

(16) Concretamente, podrán infiltrarse: miembros de la Policía Nacional, miembros de la Guardia Civil y agentes de policías autonómicas si tienen competencias como Policía Judicial. Esto, con la salvedad de que éstos últimos no podrán participar en investigaciones encubiertas con implicaciones internacionales, puesto que no son funcionarios de Policía a efectos del Convenio de Schengen.

obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la Red, que causen una gran repulsa y alarma a nivel social, tales como la e-violencia de género.

Su función consistiría en ocultar su verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los "ciberdelincuentes" actúan, con la finalidad primordial, igualmente oculta, de obtener la información necesaria para descrubrir a los supuestos criminales. Pero, ¿cómo actuaría realmente este agente en los casos de e-violencia? En estos casos, su función específica sería la de infiltrarse en escenarios virtuales públicos, como chats o foros, en los que el agresor arremeta contra su potencial víctima, y adoptar una actitud cómplice con el agresor, ganándose su confianza a través de comportamientos de apoyo hacia el mismo o comentarios misóginos que puedan atraer la atención del maltratador, para así constatar fielmente la autoría real de estos hechos e, incluso, la confesión paralela de agresiones o maltratos en el plano físico por el propio agresor.

Lo que resulta realmente polémico de esta figura policial es su forma de actuación, la cual está basada en el engaño como instrumento principal a la hora de poner en manos de la justicia a los criminales, por lo que roza el tema moral y ético. Aquí entrarían dos valores en juego: por una parte, la licitud de los medios utilizados por un Estado de Derecho; y por otra, la eficacia para combatir un delito que tan graves daños ocasiona y tanta repulsa provoca a la sociedad. Este es un tema peliagudo debido a que el Estado se vale de un medio inmoral en la represión de un delito, esto es, a través de una figura que utiliza en un primer momento el engaño como medio para cumplir su función y la traición a los criminales investigados a *posteriori*.

La justificación del engaño usado por el agente encubierto radica en una cuestión de política criminal[17], la cual llega a justificar las consecuencias desvaliosas que su utilización implica. La solución viene dada por una ponderación de valores, en el que se acaba por dar preponderancia al valor "eficacia", en el sentido de que si se quiere luchar eficazmente contra este delito tan oculto, la mejor manera y la opción idónea es infiltrar a la persona para llegar a una situación más favorable para la sociedad. Estamos eligiendo, así, una solución que reporta más seguridad y bienestar al conjunto de la sociedad y que logra la justicia, objetivo capital en un Estado de Derecho[18].

Sin embargo, debemos matizar que no puede existir un engaño a cualquier precio, por lo que se deben tener siempre presentes los principios de necesidad y proporcionalidad. Además, se debe garantizar el respeto de los principios y las garantías procesales y los derechos fundamentales de cualquier persona, incluso los de los presuntos autores.

4. Reflexiones finales

La lacra de la violencia de género se vuelve a recrudecer debido a que los maltratadores, valiéndose del poder instantáneo, controlador y automático que ofrecen las nuevas tecnologías, ejercen un nuevo tipo de violencia psicológica sobre sus víctimas para las que el Derecho, como medio de defensa, ha llegado tarde. Esta es la razón por la que nuestro legislador debe reconocer legalmente esta nueva problemática, con el fin de

(17) DELGADO MARTÍN, J., "La criminalidad organizada" *Comentarios a la LO 5/99, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilícito de drogas y otras actividades ilícitas grave*, Barcelona, J. M. Bosch, 2001, p. 4 y ss.

(18) Vid. DEL POZO PÉREZ, M., "El agente encubierto como medio de investigación procesal en el ámbito de la cooperación internacional", *Constitución Europea: aspectos históricos, administrativos y procesales*, Tórculo, Santiago de Compostela, 2006, pp. 267-310.

ofrecer penal y procesalmente una regulación novedosa y detallada al respecto, otorgando la cobertura legal necesaria a unas víctimas tan desprotegidas, y especialmente vulnerables, como lo son las víctimas de violencia de género, con independencia del canal o medio utilizado por los maltratadores para provocar dicho terror.

Desde una perspectiva actual y conectada a la presente globalización, la sociedad en la que nos encontramos concede a las TICs el poder de convertirse en los nuevos motores del desarrollo y del progreso de nuestro sistema judicial. Aun así, las nuevas tecnologías también aparecen como un nuevo cauce para la comisión de delitos al ser un escenario que se enmarca dentro de un plano de alegalidad, sobre el que existe el anonimato y gran incertidumbre jurídica, creando así enormes dificultades en el terreno investigativo y judicial.

La violencia de género a través de Internet suscita una serie de problemas en el plano procesal, aunque sustancialmente no deje de equipararse a cualquier otra acción de violencia de género ejercida en el plano físico, a tenor de seguir una serie de particularidades propias del mundo tecnológico. Así, para iniciar el procedimiento a través de denuncia o querella, la particularidad consiste en diferenciar si las conductas se producen en un entorno virtual abierto o cerrado, optando por interponer una u otra según estemos en una de esas dos modalidades.

En cuestión de competencia, se mantendría lo establecido para el resto de delitos y faltas de violencia de género, aunque la cuestión suscitada es si realmente las conductas anteriormente vistas deberían calificarse como delitos o cabrían también dentro de la categoría de faltas. Tal y como hemos argumentado, pensamos que, debido a la propia naturaleza de las acciones ejercidas y a las características particulares que poseen este tipo de conductas, calificaríamos todas ellas como delitos de forma generalizada, por lo que la instrucción correspondería a los Juzgados de Violencia de la Mujer, y el posterior fallo al Juzgado de lo Penal.

En el plano investigativo, vemos cómo existen dos cuerpos plenamente especializados, que se ayudan de las informaciones suministradas por los demás usuarios y por las propias víctimas, para los que proponemos usar una nueva figura ya contemplada para supuestos tan graves como la pedofilia y la pornografía infantil: el agente encubierto en Internet. Una figura originalmente no pensada para resolver este tipo de situaciones, pero que puede resultar muy útil y beneficiosa si se produce una detallada y correcta adaptación de su *modus operandi* a los casos de e-violencia de género, intentando superar los debates sobre la confrontación de su uso con el plano ético, atendiendo a la ponderación que debemos realizar entre las cualidades desvaliosas de esta figura con los resultados y la eficacia conseguidas, teniendo siempre presente la seguridad de todos los ciudadanos y, en concreto, de las mujeres víctimas de esta violencia.

Por todo ello, vemos cómo se abre un nuevo horizonte en el plano procesal que deberá ser reforzado gracias a una cobertura legal sólida y moderna, que guarde respeto a los principios y a las garantías procesales, teniendo en cuenta, al mismo tiempo y como último objetivo, una eficaz protección hacia las víctimas de violencia de género a través de Internet.