© **Dereito** Vol.28, nº1:147-177 (Xaneiro-Xuño, 2019) • ISSN 1132-9947

AUTORREGULACIÓN DE LOS PRESTADORES DE SERVICIO DE LA INFORMACIÓN

Self-regulation of providers information service

DOI: http://dx.doi.org/10.15304/dereito.28.1.4490

MELANIA PALOP BELLOCH
Doctora en Derecho
Universidad Jaume I de Castellón
melaniapalop@gmail.com

Resumen
ste artículo analiza los sistemas de autorregulación, así como las herramientas tecnológicas disponibles para garantizar la eliminación del material nocivo de la víctima de violencia de género virtual.
La metodología utilizada ha consistido en la consulta de bibliografía, jurisprudencia y la realización de entrevistas a profesionales especializados en la materia.
Los resultados obtenidos demuestran la existencia de herramientas tecnológicas viables para eliminar y no ocultar la información nociva de la víctima de violencia de género y ciberacoso. Pero sin ser aplicado ante una falta de corregulación entre las partes y de exigencia por la propia Ley orgánica.
Palabras clave: Violencia de género; Herramientas tecnológicas; Menor; Datos, autorregulación; Corregulación.

Abstract
This article analyzes the systems of self-regulation, as well as the technological tools available to guarantee the elimination of the harmful material of the victim of violence of virtual gender.
The methodology used consisted in the consultation of bibliography, jurisprudence and the accomplishment of interviews to professionals specialized in the matter.
The results obtained demonstrate the existence of viable technological tools to eliminate and not hide the harmful information of the victim of gender-based violence and cyberbullying, but without operability in the network due to a lack of co-regulation between the parties and a requirement for the Organic Law itself.
Keywords: Gender violence; Technological tools; Minor; Data; Self-regulation; Co-regulation.

SUMARIO

Recibido: 28/09/2018. Aceptado: 15/11/2018.

SUMMARY

1. LA VIOLENCIA DE GÉNERO VIRTUAL

GARCÍA[1] define el concepto de violencia de género entre menores como "todo ataque intencional de tipo sexual, físico o psíquico" respecto del menor hacía la menor en su relación de afectividad consolidada. Este concepto es idéntico al utilizado en las parejas de personas adultas. Estos tipos de violencia: psicológica, física y sexual se pueden realizar de forma autónoma o de forma acumulativa.

La LOMPIVG define el concepto de violencia de género en su artículo 1: "*actuar contra 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, aún sin convivencia*".

Las conductas o acciones violentas del menor hacía su pareja o ex pareja menor en las redes sociales e internet pueden producir casos de violencia de género virtual. A su vez, estas conductas o acciones violentas realizadas en el ciberespacio pueden ser calificadas de ciberacoso.

Los tipos de ciberacosos son: ciberacecho (*ciberstalking),* ciberacoso sexual *(sexting)* y ciberacoso psicológico.

El ciberacoso psicológico es el comportamiento hostil[2], humillante y vejatorio sostenido y repetido en el tiempo realizado por el menor hacía la menor víctima de violencia de género virtual, dotándolo de permanencia en internet a través de las siguientes herramientas digitales: *e-mail* o correo electrónico, mensajes de textos e imágenes digitales, *blogs*, salas de chat o coloquios *online*, páginas *webs* difamatorias y demás tecnologías de comunicación digital para acosar a la menor mediante ataques personales.

El Código Penal español tipifica la conducta del *stalke*r, creando *ex novo* tipo penal contenido en el artículo 172 ter y dice: **"***Será castigado (…) el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:*

***1ª** La vigile, la persiga o busque su cercanía física.*

***2ª** Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.*

---

[1] R. I. CORREA GARCÍA, "Violencia y medios", *Violencia escolar y de género: conceptualización y retos educativos,* con A. D. GARCÍA ROJAS, Servicio de publicaciones de la Universidad de Huelva, 2012, p. 180.

[2] M. PARES SOLIVA, "Ciberacoso". Un tema de reflexión", http://www.visagesoft.com, 2007, p. 1.

> ***3ª*** *Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.*
> ***4ª*** *Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella".*

Estas conductas o acciones se pueden concretar en: cercar, vigilar, perseguir a la menor de forma física u *online*, telefonearla de forma reiterativa, envío de correos electrónicos constantes y repetitivos, mensajes en redes sociales (*Facebook* o *Tuenti*) continuos, conectarse a chats donde la menor es asidua, editar entradas en páginas *web*s personales dirigidas a la menor, interceptar el correo electrónico de la menor, hacer regalos *online* a la víctima sin ella quererlo (puesto que la menor ignora o ha manifestado su negativa ante la recepción del obsequio *online).* También puede hacer pintadas en la vivienda o propiedades de la menor, mostrando su amor hacía ella y colgarlas en internet.
El Código penal español tipifica la figura del *sexting* en el art. 197 apartado 7º. El *sexting* consiste en[3]:
La conducta típica debe ser la de difundir, revelar o ceder a terceros imágenes o vídeos. El autor material del delito es una tercera persona, pudiendo ser pareja o ex pareja de la menor. Esa difusión, revelación o cesión debe realizarse sin el consentimiento de la víctima menor.
Todas estas conductas se caracterizan por la voluntariedad e intencionalidad de producir un daño en la menor por parte de su pareja o ex pareja menor. El daño psicológico debido a las características propias de internet es mayor en la esfera virtual y menor en el ámbito físico.
Las características de internet son: la facilidad en el anonimato del ciberagresor menor, la rápida transmisión de la información de forma instantánea, la viralidad de la red y el gran número de usuarios para ver y compartir la información nociva de la menor víctima de violencia de género virtual.
El menor es menos consciente del daño producido a la menor porque no realiza estas conductas o acciones lesivas cara a cara sino a través de la pantalla de un ordenador. Además, el lenguaje utilizado por el menor suele ser mucho más ofensivo en internet.

2. LOS CÓDIGOS DE CONDUCTA: POSIBLES MEDIDAS DE CONTENIDO PROCESAL

El mundo virtual es un medio en continúa evolución y necesita normas para su regulación. La autorregulación puede ser un medio preventivo ante la comisión del delito mediante la investigación I+D en nuevos métodos tecnológicos para bloquear esas acciones delictivas y evitar la comisión de violencia de género en las redes sociales y su posterior indexación en el buscador *Google.*
Así, pues, el largo proceso de tramitación y promulgación de leyes para la regulación de los problemas existentes en internet sirve para

[3] J. M. MARTÍNEZ OTERO, "La difusión de sexting sin consentimiento del protagonista: un análisis jurídico", *Derecom,* nº. 12, 2013, p. 3.

solucionarlos, pero, a su vez, surgen nuevos conflictos merecedores de regulación[4]. Ante esta vicisitud TERRÁDEZ SALOM dice que: "El Derecho no puede dar las respuestas oportunas"[5].
LÁZARO GONZÁLEZ y BARTOLOMÉ lo ratifican, argumentando que: "los avances tecnológicos son de tal envergadura que el día siguiente apenas nada tiene que ver con el precedente, lo que requiere una capacidad de respuesta y adecuación ágil a los cambios progresivos que se van produciendo.
Por ello, es necesario contar con un marco jurídico general y de principios que sea capaz de adaptarse a los avances tecnológicos; que no esté condicionado por situaciones concretas; que dé respuesta a los problemas y a los retos que la tecnología puede plantear; un marco que pase por el respeto a los derechos fundamentales, y muy especialmente, al derecho a la privacidad y a la dignidad de la persona"[6].
Por este motivo, la oficina ejecutiva del presidente de la Casa Blanca de EEUU elaboró un informe que decía en uno de sus puntos: "ante las cuestiones complejas de internet, su alcance global y la constante evolución se requieren políticas a tiempo, escalables y que permitan la innovación. El objetivo primordial del plan de acción de la administración estadounidense es crear el marco o entorno necesario para que las partes interesadas, colaborando entre sí, desarrollen códigos de conducta voluntarios, de obligado cumplimiento"[7].
BELTRÁN CASTELLANOS da un paso más y explica la importancia de la autorregulación: "Un eficaz sistema de protección de datos en el ámbito de las comunicaciones electrónicas exige rebasar incluso la solución estrictamente jurídica, para abrazar cualesquiera medidas e iniciativas que coadyuven a encauzar el problema. Las implicaciones técnicas de las comunicaciones electrónicas, en este caso, de las redes sociales y la dimensión extraterritorial de internet, representan tales obstáculos para la protección de la vida privada, que impiden renunciar a nuevas vías como la autorregulación y autocontrol de los sectores implicados"[8].

[4] I. SERRANO MAÍLLO, "El derecho a la imagen de los menores en las redes sociales. Referencia especial a la validez del consentimiento", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013, p. 437.
[5] D. TERRÁDEZ SALOM, "Formaciones políticas racistas y xenófobas: aproximación al uso de las redes sociales. Libertad de expresión versus abuso de derecho", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales,* con I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios políticos y constitucionales, Madrid, 2013, pp. 275-278.
[6] I. E. LÁZARO GONZÁLEZ, Y A. BARTOLOMÉ, *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, Aranzadi, Madrid, 2015, p. 276.
[7] M. RECIO GAYO, *Protección de datos personales e innovación: ¿(in)compatibles?,* Reus, Madrid, 2016, pp. 72-75.
[8] J. M. BELTRÁN CASTELLANOS, "Aproximación al régimen jurídico de las redes sociales", *Cuaderno electrónico de estudios jurídicos*, nº. 2, 2014, p. 69.

Por eso, según VIGURI CORDERO el concepto de autorregulación es[9]:

- "Es una técnica que previene o pospone la legislación.
- En un sentido más positivo, puede ser utilizada como un medio para experimentar y prepararse para la legislación de forma flexible evitando así, la excesiva normatividad en cada uno de los sectores.
- Puede proporcionar soluciones más allá del alcance de la legislación existente, que puede o no dar lugar a un nuevo ciclo de elaboración de políticas a lo largo de las líneas antes mencionadas".

A raíz de la autorregulación surgen los mecanismos de certificación como los códigos de conducta, los sellos y las marcas. Los códigos de conducta son: "los criterios utilizados para otorgar el sello de calidad IQUA, y llevar a cabo las posibles mediaciones o procesos de arbitraje"[10].

La IQUA es una entidad de ámbito estatal sin ánimo de lucro de las Islas Baleares. Fue creada, el 21 de octubre de 2002. La IQUA pretende ser un referente común para la administración, las empresas, los operadores, las asociaciones, los usuarios, tiendas y los técnicos para la mejora y la calidad en internet.

El objetivo principal de IQUA es la confianza y la seguridad en la red mediante la autorregulación[11] y el otorgamiento del sello de calidad IQ. El sello de calidad permite la visualización pública de una correcta aplicación por parte de la empresa tecnológica de los códigos de conducta y de la vinculación de la empresa con la responsabilidad social en sus prácticas.

Sus funciones son las siguientes[12]:

1) "Velar por la calidad de internet.
2) Desarrollar la sociedad de la información.
3) Promover la autorregulación en internet.
4) Otorgar un sello que acredite la calidad de las páginas *web*.
5) Defender los derechos de los usuarios de la red.
6) Realizar estudios e informes sobre los contenidos de la red.
7) Actuar como plataforma de debate y reflexión.
8) Tramitar quejas y sugerencias.
9) Resolver extrajudicialmente conflictos relacionados con internet.
10) Actuar como plataforma de mediación y arbitraje".

---

[9] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime, con A. RALLO LOMBARTE, y R. GARCÍA MAHAMUT, Valencia, Tirant lo Blanch, 2015, p. 902.

[10] http://www.iqua.es/

[11] Como señala FERNÁNDEZ ESTEBAN "frente a la autorregulación (…) presenta ciertas ventajas que la hacen especialmente apropiada para algunos de los aspectos jurídicos de Internet: es una alternativa flexible, eficaz y rentable a la regulación, ya que consigue los mismos efectos que la regulación sin la lentitud que conllevan los procesos regulatorios" M. L. FERNÁNDEZ ESTEBAN, "Internet y los derechos fundamentales", *Internet, una profecía,* Ariel, Barcelona, 2002, p.126.

[12] http://www.iqua.es/

El código deontológico de IQUA es el cumplimiento de unos principios generales[13] para la defensa del interés general y de los derechos de los ciudadanos. Hay diferentes modelos de códigos de conducta[14]:

1) "Los códigos de organización: Estos códigos han sido desarrollados por grandes organizaciones (…) han sido objeto de inspección (…) o han recibido un elevado volumen de quejas por parte de los consumidores.
2) Los códigos sectoriales: Los sectores están ya regulados legal o reglamentariamente y lo que se pretende a través de ellos es adaptarse de un modo sencillo, ágil y eficaz.
3) Los códigos funcionales: están enfocados (…) al ejercicio de sus funciones. Su ejemplo se encuentra en el *marketing* directo y en el *telemarketing*.
4) Los códigos profesionales: se crean por los profesionales a los que se les aplicará el código.
5) Los códigos tecnológicos: se definen las prácticas tecnológicas intentando hacer frente a problemas específicos de privacidad. Son instrumentos enormemente dinámicos como se requiere en el campo de las nuevas tecnologías".

Este trabajo se centra más en el modelo de código tecnológico en busca de la medida tecnológica para hacer viable un derecho al olvido eficaz.
Según VIGURI CORDERO: "Los códigos de conducta constituyen: prácticas, principios o derechos para ser respetado"[15]. Es necesaria su aprobación por parte de la AEPD.
Este autor añade: "son instrumentos que van más allá de un simple compromiso de privacidad. Están compuestos por un conjunto de reglas que complementan a la legislación y una vez la organización se someta a ellos, les resultará vinculante en toda su extensión"[16].
Existen dos modelos de autorregulación[17]:

1) La autorregulación pura.
2) La corregulación o autorregulación mixta.

La autorregulación pura es utilizada en EEUU. Las empresas privadas tienen plena libertad para establecer sus principios y normas, dejando en

[13] Si se quiere conocer estos principios veáse el anexo XI: Principios IQUA.
[14] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 913.
[15] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 912.
[16] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 917.
[17] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 908.

un segundo plano a las administraciones públicas. Los principios a tener en cuenta son[18]:

1) "La privacidad por diseño (*PbD*) que consiste en adoptar medidas de privacidad en todas las fases de desarrollo del producto.
2) Se ofrece a los consumidores la capacidad de tomar decisiones respecto a sus datos personales de un modo simple, entendible e inteligible por un consumidor medio.
3) La recopilación y el uso de información personal de un modo transparente".

Las ventajas de este tipo de autorregulación son[19]:

1) "La voluntariedad: facilita la aplicación práctica de estos mecanismos y su cumplimiento sin necesidad de intervención e imposición de poderes públicos.
2) La eficiencia: es un sistema eminentemente práctico para la descongestión del sector público, ahorrando tiempo en recursos jurídicos y económicos.
3) La flexibilidad: los instrumentos utilizados son modificables de un modo rápido y relativamente sencillo.
4) La especialización: permite adaptarse perfectamente a un sector de actividad específico.
5) La trasparencia: proporciona publicidad e información a terceros sobre el funcionamiento interno de una organización.
6) La proactividad: previene daños e infracciones futuras mediante la puesta en práctica de actuaciones que salvaguardan la protección de los datos personales".

Sin embargo, VIGURI CORDERO considera no apropiado este sistema de autorregulación porque "debido al gran desarrollo de los productos y servicios resulta necesario que la administración adquiera progresivamente mayores competencias en la materia para proteger la privacidad de los consumidores, así como el establecimiento de un control eficaz, independiente e imparcial que genere confianza en la economía a través de las nuevas tecnologías"[20].

Por eso, la autorregulación mixta o corregulación surge como consecuencia de los inconvenientes derivados de la aplicación del sistema de autorregulación pura. Estos países regulan la protección de datos mediante la creación de principios mínimos y mecanismos técnicos apropiados para cumplir lo manifestado en las legislaciones, y, además, esto proporciona una mayor garantía de privacidad de la establecida en la

[18] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 909.
[19] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 910.
[20] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., pp. 910-911.

Ley, complementando la legislación sobre datos personales. Esto constituye una manifestación de la responsabilidad social corporativa[21]. Asimismo, la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, relativa a determinados aspectos jurídicos de los servicios de la información, donde en su considerando 49 recoge que: *"Los Estados miembros y la Comisión fomentarán la elaboración de códigos de conducta, ello no irá en perjuicio del carácter voluntario de dichos códigos ni de la posibilidad de que las partes interesadas decidan libremente la adhesión a los mismos"*[22]. Por tanto, son las propias empresas las que se adhieren libre y voluntariamente.

En la Directiva 95/46CE los códigos de conducta se encuentran regulados en el artículo 27 y dipone:

"1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.

Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Este se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo".

La Directiva 95/46CE establece "que todas los prestadores de servicio de la información[23] encargados de elaborar, modificar o prorrogar códigos de

[21] http://www.lssi.gob.es/la-ley/aspectos-basicos/Paginas/autorregulacion.aspx

[22] A. ROJAS, "La responsabilidad de los PSSI y la libertad de expresión. Jurisprudencia reciente", *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías*, con COTINO HUESO, L., Servei de publicaciones de la Universidad de Valencia, 2010, p. 284.

[23] En adelante ISP's.

privacidad podrán ser sometidas a examen de las autoridades nacionales a fin de que se adecuen a las disposiciones nacionales"[24].

El último párrafo otorga potestad al GT29 para examinar los proyectos de los códigos de conducta comunitarios y pronunciarse sobre su conformidad. También, las APD comunitarias tendrán la legitimación para examinar la adecuación de los códigos de conducta a las disposiciones legales y reglamentarias de los Estados miembros[25].

A su vez, el GT29 elaboró un documento DG XV D/5004/98 con el procedimiento para la presentación de códigos de conducta comunitarios. En su artículo 4 estableció:

> *1) "Si se atenían o no a lo dispuesto en las Directivas y las disposiciones nacionales adoptadas en cumplimiento de las mismas.*
> *2) Si reunían las oportunas condiciones de calidad y coherencia interna.*
> *3) Si ofrecían un valor añadido suficiente con respecto a las Directivas y otras normas sobre protección de datos aplicables, evaluando en particular, si el proyecto de código se centraba suficientemente en los problemas de protección de datos.*
> 4) *Si aportaban soluciones suficientemente claras a dichos problemas*".

Así, el art. 30 párrafo 1º de la Directiva 95/46CE ratifica lo anterior:

> *"1. El Grupo tendrá por cometido:*
> *a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;*
> *b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;*
> *c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;*
> *d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria".*

A su vez, la LOPD regula los códigos de conducta en el artículo 32 y dice:

---

[24] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 917.

[25] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., pp. 918-920.

"1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.
En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el registro general de protección de datos y, cuando corresponda, en los creados a estos efectos por las comunidades autónomas, de acuerdo con el artículo 41. El registro general de protección de datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el director de la agencia de protección de datos requerir a los solicitantes para que efectúen las correcciones oportunas".

De esta manera, la AEPD realiza una labor de supervisión, trasparencia, calidad e inspección del funcionamiento y organización de los códigos de conducta en vigor. También, los Códigos de conducta están regulados en el art. 18 de la LSSICE[26]:

"1. Las administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La administración general del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.
Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.
2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

[26] https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias.
Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.
3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión".
De esta forma, el art. 18 de la LSSICE insta a la administración a impulsar códigos de conducta para la autorregulación del propio sector, regulando cuestiones referentes a: procedimientos para la detección y retirada de contenidos ilícitos, el establecimiento de procedimientos extrajudiciales para la resolución de conflictos y medidas al respecto para la protección de las menores y su dignidad humana.
La LSSICE faculta la potestad al sector público para controlar todo el proceso desde la promoción en la elaboración de los códigos hasta su efectivo control[27]. Según LÁZARO GONZÁLEZ y BARTOLOMÉ: los códigos de conducta son una forma de regulación interna que funciona como un contrato entre los proveedores del servicio y sus usuarios"[28].
Los códigos de conducta no son normas orgánicas u ordinarias con rango de ley sino son consideradas costumbres. La costumbre es una fuente de derecho[29]. Por tanto, los códigos de conducta se regirán por la autonomía de la voluntad entre los *ISP's* intervinientes en la creación y regulación de las bases constituyentes de los códigos de conducta y otros operadores de internet como el sector público.
PIÑAR MAÑAS ratifica esta argumentación, diciendo: "tales manifestaciones de autorregulación deben ser bien acogidas, pero siempre y cuando los principios esenciales del derecho fundamental estén clara e imperativamente recogidos en las normas jurídicas. Ningún derecho fundamental se deja sólo en manos de la autorregulación"[30].
A su vez, LÁZARO GONZÁLEZ y BARTOLOMÉ coinciden con las argumentaciones anteriores: "las manifestaciones sobre autorregulación necesitan de un apoyo normativo que esté recogido por una legislación de

[27] J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime*,* op. cit., p. 928.
[28] I. E. LÁZARO GONZÁLEZ, Y A. BARTOLOMÉ, *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, op. cit, p. 279.
[29] C. J. MALUQUER DE MONTES I BERNET, "Códigos de conducta y buenas prácticas en la gestión de datos personales", *Protección de datos personales en la sociedad de la información y la vigilancia,* con Mª. R. LLÁCER MATACÁS, Wolters Kluwer, 2011, p. 128.
[30] J. L. PIÑAR MAÑAS, "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales", *Redes sociales y privacidad del menor*, CON J. L. PIÑAR MAÑAS, S. RODOTA, P. L. MURILLO DE LA CUEVA, K. BENYEKHLEF, C. G. DE GREGORIO, P. FLEISHER, REUS, Madrid, 2011, p. 83.

protección de datos, honor, intimidad e imagen, que posteriormente, sea desarrollado por códigos de conducta y/o políticas de privacidad"[31].
Por eso, como consecuencia del constante proceso de evolución de los medios tecnológicos y la proliferación de nuevas formas de atentado a los derechos fundamentales y a la protección de los datos personales de las menores víctimas de violencia de género es necesario la creación de códigos de conducta para prevenir y luchar contra este vacío legal existente en las leyes mediante la creación por parte de los *ISP's* de las medidas tecnológicas eficaces, viables y suficientes para dotar de seguridad a la red y evitar la existencia de cualquier forma de agresión a la menor víctima de violencia de género en las redes sociales e internet.
Así, pues, LESSIG dice que: "El ciberespacio requiere una regulación más amplia y lo que es más importante, el reconocimiento de un regulador de singular importancia. El ciberespacio, hemos de comprender cómo regulan un código diferente, esto es, cómo el software y el hardware, que hacen del ciberespacio lo que es, constituyen su código"[32].
Por eso, solamente conociendo cómo funcionan los instrumentos tecnológicos se podrán aplicar y crear unas normas con rango de ley y normas de autorregulación oportunas al ciberespacio. Si el legislador entiende las normas de exclusión de contenidos, los códigos abiertos y los distintos sistemas tecnológicos y herramientas operantes en internet, se regulará el robot existente en internet, pero de forma adecuada.
El 10 de febrero de 2008 el Comité de ministros del Consejo de Europa propuso una serie de iniciativas mediante un programa para "proteger la dignidad, la seguridad y la privacidad de los menores en internet". Este programa entró en vigor en el año 2009[33] y se adhirieron diecisiete operadores.
Su finalidad era proteger concretamente la intimidad del menor y sus datos personales. Para ello, puso en marcha una serie de acciones de concienciación. Estas acciones consiguieron la concienciación de los menores mediante la comprensión de los riesgos asociados a su conducta en internet[34].
Por otra parte, la Comisión Europea elaboró unos principios para la autorregulación de la actuación de las redes sociales llamado: "*Principios de redes sociales*" y son[35]:

> "*Principio 1: Aumentar los mensajes para hacer más segura la red y elaborar políticas de uso aceptables para los usuarios,*

[31] I. E. LÁZARO GONZÁLEZ, Y A. BARTOLOMÉ, *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, op. cit, p. 276.
[32] L. LESSIG, *El Código 2.0*, Traficantes de sueños, 2009, p. 37
[33] G. BUTTARELLI, "Los menores y las nuevas tecnologías", *Redes sociales y privacidad del menor*, CON J. L. PIÑAR MAÑAS, S. RODOTA, P. L. MURILLO DE LA CUEVA, K. BENYEKHLEF, C. G. DE GREGORIO, P. FLEISHER, REUS, 2011, p. 141.
[34] G. BUTTARELLI, "Los menores y las nuevas tecnologías", *Redes sociales y privacidad del menor*, op. cit., p. 141.
[35]
http://ec.europa.eu//information_society/activities/social_networking/docs/sn_principles.pdf

padres, profesores y estudiantes de una forma destacada, clara y adaptada a cada edad.
Principio 2: Garantizar la adopción de los servicios prestados a la edad de sus usuarios.
Principio 3: Otorgar poder a los usuarios a través de herramientas y tecnología.
Principio 4: Proveer de mecanismos sencillos de reporte de conductas o de violaciones de los términos de uso.
Principio 5: Facilitar y animar a los usuarios a hacer una aproximación segura en relación con su privacidad y datos personales.
Principio 6: Revisión de contenidos o conductas ilegales o prohibidas".

La aplicación en las redes sociales de este último principio sería importante para detectar los delitos derivados de casos de violencia de género en menores.

En cuanto a la aplicación de estos principios se han adherido veinte redes sociales en toda Europa. Estas redes sociales son sometidas a examen por parte de expertos independientes de la Comisión Europea para valorar el grado de *compliance*. Los resultados han sido positivos[36].

Su objetivo fue proporcionar medios a los adolescentes para enfrentarse a los potenciales riesgos derivados de la navegación en internet y estableció estos mínimos:

1º. La posibilidad del usuario de acudir a los propios canales de denuncia "botón de denuncia de abusos" de las redes sociales o de los sitios *web* para hacer desaparecer una intromisión ilegítima de los derechos de la persona.

2º. Asegurarse de que todos los perfiles y listas de contactos en línea de los usuarios de los sitios *webs* registrados como menores de 18 años estén predeterminados como "privados".

3º. Asegurarse de que los perfiles privados de los usuarios de 18 años no puedan buscarse (ni en sitios *web* ni a través de motores de búsqueda).

4º. Garantizar la visualización accesible y destacada de las opciones de privacidad para que los usuarios puedan averiguar fácilmente quién puede ver sus publicaciones en el muro: sólo sus amigos o todo el mundo.

5º. Impedir a los menores de 13 años de edad la utilización de sus servicios.

6º. Los sitios de redes sociales adheridos a un código de conducta informarán a la Comisión sobre las políticas de seguridad adoptadas a título particular y sobre cómo pondrán en práctica los principios enunciados.

[36] N. MARTOS DÍAZ, "Políticas de privacidad, redes sociales y protección de datos. El problema de la verificación de edad", *Derecho y redes sociales*, con A. RALLO LOMBARTE, y R. MARTÍNEZ MARTÍNEZ, Civitas, Navarra, 2010, p. 157.

3. HERRAMIENTAS TECNOLÓGICAS DE AUTORREGULACIÓN

Las principales iniciativas de autorregulación y corregulación hasta el momento son[37]:

1. "Líneas de denuncia (conocidas internacionalmente como *hotlines*): constituyen mecanismos para la notificación a las autoridades sobre contenidos ilegales o dañinos existentes en internet por parte de los usuarios. Muchas de estas líneas están basadas en la idea de colaboración entre los particulares" al denunciar, y los poderes públicos, persiguiendo el delito acontecido".

Se realizan a través de formularios en las propias redes sociales. También, mediante llamada telefónica o envío de correo electrónico.

Su procedimiento es el siguiente: una vez recibida, el *ISP* lo comunicará al resto de intermediarios y a la policía para el estudio del caso y, llegado el caso, la retirada del contenido ilícito de violencia de género virtual. "Estas líneas de denuncia son un ejemplo paradigmático de la eficacia de la corregulación: los usuarios denuncian, los *ISP's* tramitan la queja, y los poderes públicos intervienen en la aplicación del Derecho"[38].

2. El etiquetado de contenidos significa: aparecerá el titular del comentario o imagen perfectamente identificable. La AEPD propone "limitar la posibilidad de etiquetado de los usuarios dentro de la red para que cualquier persona etiquetada con su nombre reciba automáticamente una solicitud de aceptación o rechazo, impidiendo en este caso la publicación y tratamiento de datos no autorizados"[39].

Actualmente, *Facebook* no ofrece al usuario la opción de impedir esta actividad. Es más, el usuario es etiquetado sin su consentimiento previo y, posteriormente recibe la notificación de su etiquetado por la propia red social. Entonces, el usuario deberá proceder a desetiquetarse foto por foto, eliminando su nombre en las imágenes de su titularidad compartidas sin poder eliminar la propia imagen[40] porque está publicado en otros muros de usuarios.

Por eso, desde *Facebook* recomiendan a sus usuarios solicitar permiso al titular de la imagen o comentario de su publicación. Recomendación no realizada por ningún usuario de las redes sociales. Esto queda manifestado en la propia red social en su "*Decálogo de condiciones*" y

---

[37] J. M. MARTÍNEZ OTERO, *La protección jurídica de los menores en el entorno audiovisual,* Aranzadi, Pamplona, 2013, pp. 237-238.

[38] J. M. MARTÍNEZ OTERO*, La protección jurídica de los menores en el entorno audiovisual,* op. cit., p. 245.

[39] R. M. ORZA LINARES, "El derecho al olvido en internet: algunos intentos para su regulación legal", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013, p. 487.

[40] A. NIETO MARTÍN, Y M. MAROTO CALATAYUD, "Redes sociales en internet y "data mining" en la prospección e investigación de comportamientos delictivos", *Derecho y redes sociales*, con A. RALLO LOMBARTE, y R. MARTÍNEZ MARTÍNEZ, Civitas, Navarra, 2010, p. 240.

pone: "*no será en ningún caso responsable de las interacciones entre los usuarios. Los únicos responsables serán los propios usuarios*"[41].
Esta situación demuestra la inoperancia de las redes sociales en aplicar eficaces sistemas tecnológicos para impedir la vulneración de la intimidad y la protección de datos personales de los usuarios.
3. Filtro de contenidos. Limitan el acceso a sitios *web* con contenido nocivo. Pueden funcionar de muy diversas maneras: con sistemas de listas blancas donde solo se admite el acceso a los sitios *web* consignados en la lista, o con listas negras donde sólo se limita el acceso a los sitios *web* de la lista. También cabe aplicar un filtro a través de *software* donde se detecte determinadas palabras o expresiones y limite el acceso a las páginas con contenido no adecuado.
4. Señalización: Antes de ofrecer el contenido de la *web* se advierte al usuario sobre el tipo de contenido a encontrar. Sólo cuando el usuario reconoce haber leído la advertencia y manifiesta su voluntad de visitar el sitio, se le permite el acceso a la *web* o al servicio.
5. Códigos de conducta de los *ISP's*. Distintas asociaciones de *ISP's* han desarrollado códigos tendentes, entre otras cosas, a proteger a los menores en internet. Estos códigos, de muy diversa naturaleza, señalan qué contenidos son permitidos y las vías para denunciar la forma de actuar de los *ISP's* ante esto.
6. Estándares de la comunidad en páginas con contenido generado por los usuarios. Algunas comunidades han desarrollado su propio código de contenidos y los medios para denunciar y retirar contenidos ilegales o inadecuados[42].
Estas iniciativas de autorregulación y corregulación propiciarán la iniciación de las diligencias previas de investigación por parte de los cuerpos de seguridad del estado para detectar al responsable (a la pareja o ex pareja de la menor) o responsables (a los ciberacosadores) del contenido ilícito.
La LECrim autoriza en su artículo 264 a cualquier persona con conocimiento sobre casos de violencia de género la comunicación a los cuerpos y seguridad del Estado para proceder a iniciar la fase de investigación del delito y tomar las medidas pertinentes. Sin embargo, es la propia menor o sus representantes legales los denunciantes de su situación y la red social solo facilita los contenidos y otras informaciones para investigar el posible delito cuando se les requiere.
También, pueden ayudar a frenar la expansión de los contenidos ilícitos de la menor víctima de violencia de género virtual. Pero, la mayoría de estas medidas no impiden la difusión de los datos personales de la menor víctima y, si sus datos personales han formado parte de otro muro personal de otro usuario, la menor no podrá controlar su difusión por no

[41] A. NIETO MARTÍN, Y M. MAROTO CALATAYUD, "Redes sociales en internet y "data mining" en la prospección e investigación de comportamientos delictivos", *Derecho y redes sociales*, op. cit., p. 241.
[42] R. M. ORZA LINARES, "El derecho al olvido en internet: algunos intentos para su regulación legal", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, op. cit., p. 487.

tener herramientas para frenar la viralidad de sus datos entre los usuarios de la red social.

Al respecto, deberían usarse las oportunas técnicas tecnológicas para impedir y bloquear de forma automática la difusión de contenidos ilícitos mediante técnicas de rastreo y localización de la información nociva para su posterior eliminación. El objetivo es luchar contra la apología de la violencia hacía las mujeres y, de momento no se han puesto en marcha ninguna iniciativa eficaz para cumplir con este objetivo.

Otra medida a tener en cuente sería la aplicación de herramientas tecnológicas para impedir la indexación de contenidos ilícitos. *Google* debería proporcionar la debida seguridad en la red, y más, tratándose de menores.

Así lo estima el Consejo, Parlamento y Comisiones europeos y del GT29, diciendo: "Los usuarios menores deberían tener unos perfiles privados que no deberían ser indexados por buscadores"[43]. Esto ocurre así, pero, cuando el menor es citado en un muro de una persona adulta aparece su información en *Google*.

Ante todo lo expuesto, es necesario imponer una política preventiva para la protección de los datos personales de la menor víctima de violencia de género virtual. Esto puede ser posible mediante los llamados: *privacy by design*.

Los *PbD* "es una filosofía surgida en los años 90 promovida por la Dra. Ann Cavoukian, comisionada de privacidad de Ontario (Canadá). Cavoukian propuso una reformulación de los sistemas de protección de los datos personales en entornos tecnológicos para la construcción de sistemas de información, procesos de negocio y sistemas físicos respetuosos con la privacidad.

En el *PbD* se parte del hecho de que todos los requisitos relacionados con el tratamiento de datos personales y privacidad se deben identificar de forma integrada y sistemática en las especificaciones iníciales del nuevo sistema. Para ello, es necesario evaluar todos los procesos y flujos de información previstos en el sistema, analizando sus implicaciones en privacidad desde un punto de vista holístico, preventivo y con un foco más allá del marco jurídico vigente"[44].

De este modo, "el operador de la red deja de tener un papel pasivo, limitándose a aplicar las medidas legalmente establecidas para asegurarse el cumplimiento de la normativa de protección de datos, y se convierte en un actor (…), para asegurar unos niveles máximos de protección de los datos que vayan a recogerse y/o tratarse en la red social"[45].

---

[43] I. E. LÁZARO GONZÁLEZ, Y A. BARTOLOMÉ*, Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, op. cit, p. 278.

[44] J. MEGÍAS TEROL, "Privacy by design, construcción de redes sociales garantes de la privacidad", *Derecho y redes sociales*, con A. RALLO LOMBARTE, Y R. MARTÍNEZ MARTÍNEZ, Navarra, Civitas, 2010, p. 320.

[45] A. TOURIÑO, *El derecho al olvido y a la intimidad en Internet*, Los libros de la catarata, 2014, p. 23.

El sistema *PbD* está inspirado en siete principios[46]:

1. "Proactividad (no retroactividad) y prevención (y no corrección): Esta basado en medidas proactivas, es decir, anticipándose y previendo incidencias y problemas que puedan poner en riesgo los datos personales al ser recogidos y tratados por la red.
2. Privacidad como configuración predeterminada: Los datos personales se protegerán de forma automática en el sistema técnico o en los procesos asociados al mismo. Por ello, no hará falta que la persona usuaria realice cualquier acción para proteger sus datos, automáticamente quedan protegidos y asegurará su privacidad.
3. Privacidad incrustada en el diseño: La privacidad se convertirá en la raíz y esencia del proceso de diseño.
4. Funcionalidad total: Tanto la seguridad como la privacidad están garantizadas por igual.
5. Seguridad extremo a extremo: Los sistemas de recogida y tratamiento de datos asegurarán unos niveles máximos de protección de la información tanto en su recogida como en las posteriores fases de las que se componga el ciclo de vida de tales datos en los citados sistemas. De este modo, los datos se recogerán, tratarán y finalmente se destruirán, asegurando su plena seguridad.
6. Visibilidad y trasparencia: La explotación de los sistemas técnicos que vayan a utilizarse para el tratamiento de datos personales deberán estar estructurados y funcionar conforme a su diseño original, garante de unos niveles óptimos de protección de tales datos. Así, sus componentes y operaciones deberán ser trasparentes para sus usuarios, de modo que éstos tengan una imagen fiel en todo momento del *status* de cumplimiento de los niveles de protección de datos personales.
7. Enfoque centrado en el usuario: Los intereses del usuario deberán configurar los sistemas mediante configuraciones predefinidas de privacidad alta, sistemas adecuados de notificaciones así como establecer medios de opciones para los perfiles de usuario de fácil gestión"[47].

En cuanto a la aplicación de estos principios en el diseño, construcción y operación de redes sociales significa: el usuario es dueño de sus datos personales e información contenida en su muro, por tanto se deben reforzar y mantener estos derechos. También, se debe tener conocimiento de las leyes reguladoras de la protección de datos personales y a partir, de estas perfeccionarlas para conseguir la ansiosa protección.

Por otro lado, a la gestión del procedimiento de crear un eficaz *PbD* se le aplica un "análisis de impacto de privacidad". El PIA "es un estudio que

[46] A. TOURIÑO, *El derecho al olvido y a la intimidad en Internet*, op. cit., p. 23.

[47] Si se quiere profundizar sobre el sistema de gestión veáse: Anexo XI: Gestión del diseño.

describe los flujos de información privada dentro de un sistema o proyecto y analiza los posibles impactos de dichos procesos en la privacidad de sus usuarios. Su objetivo es identificar y recomendar alternativas para gestionar, minimizar o erradicar completamente impactos en la privacidad de los individuos usuarios del sistema" antes de empezar la creación del diseño de la red social[48].

Esto supone adoptar una estrategia en el diseño de la red social mediante la "seguridad informática". La seguridad informática consiste en "proporcionar integridad, disponibilidad y confidencialidad de la información"[49]. La seguridad informática evita la intromisión por parte de terceros a los datos personales de sus titulares. Con esto, se conseguiría proteger los derechos fundamentales de la menor víctima de violencia de género y la protección de sus datos personales. Hoy en día es una utopía, pero puede ser una realidad.

El *PbD* implica la protección de la intimidad, y de la reputación a lo largo de todo el ciclo de vida de las tecnologías, es decir, desde su concepción hasta su despliegue, utilización y eliminación final. El último avance en relación con la positivización del principio de privacidad en el diseño se ubicó en la citada propuesta europea del Reglamento (UE). El art. 23 de la propuesta estableció las obligaciones del responsable del tratamiento que emanen de los principios de la protección de datos desde el diseño y por defecto[50].

Sin embargo, actualmente la menor víctima de violencia de género virtual no puede configurar su privacidad respecto a las fotos publicadas por su pareja en su muro personal, y que posteriormente son compartidas con otros usuarios con comentarios nocivos hacía ella.

Ante este hecho, a la menor víctima de violencia de género se le asocian todas las consecuencias negativas derivadas de la acción de un tercero. Solamente se produce este hecho porque la red social no pone en práctica técnicas visibles y eficaces para compartir datos personales de terceros sin el consentimiento expreso e inequívoco y previo del propio titular de los datos. Sin embargo, este derecho está regulado en la LOPD y en la Directiva 95/46 CE, así como en el Reglamento (UE), y sin embargo, nada se hace al respecto.

Otra iniciativa de códigos de conducta relevante es la propuesta realizada en Francia destinada a fomentar la protección del derecho al olvido. Este código de conducta establece tres niveles diferentes para los sitios *webs*[51]*:*

1) No podrán recopilar datos.

---

[48] J. MEGÍAS TEROL, "Privacy by design, construcción de redes sociales garantes de la privacidad", *Derecho y redes sociales*, op. cit., p. 322.

[49] I. E. LÁZARO GONZÁLEZ, Y A. BARTOLOMÉ*, Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, op. cit, p. 278.

[50] A. TOURIÑO, *El derecho al olvido y a la intimidad en Internet*, op. cit., p. 23.

[51] K. BENYEKHLEF, P. A. COUTURE-MÉNARD, E. PAQUETTE BÉLANGER, "Menores, redes sociales y el derecho al olvido", *Redes sociales y privacidad del menor*, CON J. L. PIÑAR MAÑAS, S. RODOTA, P. L. MURILLO DE LA CUEVA, K. BENYEKHLEF, C. G. DE GREGORIO, P. FLEISHER, REUS, 2011, p. 214.

2) Podrían recopilar un número limitado de datos.
3) Podrán recopilar una amplia gama de datos de sus usuarios.

Otros autores han aconsejado probar otras medidas técnicas mediante un sistema de encriptación de los datos cuya función sea la autodestrucción de los mismos pasado un determinado período de tiempo como es el caso del proyecto Vanish[52].

En la misma línea, otra técnica propuesta por MAYER- SCHÖNBERGER es la fijación de un período de caducidad[53] en la información recopilada por parte del propio usuario. Sin embargo, esta iniciativa no soluciona la eliminación del material nocivo circulante en internet, puesto que la propia ex pareja y ciberacosadores pondrían una fecha muy extensa.

Sin embargo, JARAMILLO dice que: "la autorregulación debe ser realizada por los propios usuarios, debido a que son ellos quienes confeccionan y suben los contenidos de las redes sociales"[54].

En cambio, GALÁN MUÑOZ constata que "no parece que la solución se pueda dejar en manos de la autorregulación que se pudiesen dar los propios usuarios, los intermediarios de la red ni los tribunales, hecho que ha llevado a que se hayan ido paulatinamente creando diversas normativas nacionales que han tratado de concretar y de delimitar cuándo y bajo qué condiciones se podría llegar a atribuir responsabilidad jurídica a los proveedores por los contenidos ajenos que ayudasen a difundir"[55].

LÁZARO GONZÁLEZ y BARTOLOMÉ fundamentan una propuesta conciliadora: "porque la búsqueda del necesario equilibrio entre la naturaleza abierta de internet y la protección de datos personales, la intimidad, el honor y la imagen de sus usuarios (…) se piensa la regulación para lo esencial, los principios y la configuración del derecho y la autorregulación, para adecuar la normativa a las particularidades del

---

[52] P. SIMÓN CASTELLANO, "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013, p. 102.

[53] El estudio de ENISA demuestra que existen ya tecnologías (Vanish, X-pire, EpfCOM) que posibilitan la destrucción de información personal (fotografías, etc.) cuando el usuario fija una fecha de caducidad (ENISA (Network and Information Securite Agency): The right to be forgotten) (http: //www.enisa.europa.eu/activities/identity-and-trust/library/deliberables/the-right-to-be-forgotten). El propio V. MAYER SCHÖNBERGER, válida la aplicabilidad de esta modalidad de derecho al olvido en los buscadores de internet: "*google and other search engines may have to change their practices as well. No longer would they be able to store search queries forever. They would have to be deleted forgotten over time*". A. RALLO LOMBARTE, *El derecho al olvido en Internet: **Google versus España***, op. cit., p. 32.

[54] O. JARAMILLO CASTRO, "El futuro de la vida pública y privada en las redes sociales", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013, p. 411.

[55] A. GALÁN MUÑOZ, *Libertad de expresión y responsabilidad penal de contenidos ajenos en internet,* Tirant lo Blanch, Valencia, 2010, p. 79.

sector, y, en particular, al uso de las nuevas tecnologías por parte de los menores"[56].

En mi opinión se está totalmente conforme con la aplicación de los códigos de conducta en el sistema mixto y no puro, porque debe haber una cooperación coordinada de todos los agentes intervinientes en la lucha de la violencia de género y, puesto que como se dijo anteriormente, la regulación de la Ley al caso concreto siempre suele ir un paso atrás para combatir la delincuencia en la red. Además, se necesitan nuevas técnicas de investigación tecnológica para dotar de seguridad a la red en temas de violencia de género virtual.

Por otro lado, internet constituye un medio global. Los conflictos y delitos surgidos en la *web* pueden ser entre nacionales de un mismo país o entre usuarios de distintos países, siendo importante la aplicación de las normas de autorregulación o corregulación para mejorar la cooperación entre países por medio de técnicas extrajudiciales de mediación, conciliación o arbitraje siempre que no se tenga la necesidad de acudir a los tribunales y solicitar el auxilio de cooperación internacional de la justicia mediante rogatorias, donde siempre surgen problemas a pesar de su regulación en la Ley.

En Alemania utilizaron el sistema de bloqueo de páginas *webs* para imposibilitar o dificultar el acceso del menor a determinadas páginas a través de los mecanismos técnicos respectivos: el instrumento de bloqueo de páginas webs[57]. Es un sistema de vigilancia estatal. Esta medida tiene un carácter preventivo. Es realizado por un funcionario alemán. Se realiza un bloqueo con el proveedor de acceso y surte sus efectos solo en Alemania. Está regulado en la legislación nacional Alemana[58].

Exportar este sistema a España no soluciona el problema porque el acoso de la menor víctima de violencia de género virtual seguiría produciéndose y virilizándose fuera de nuestras fronteras sin ninguna garantía para detenerlo al ya haberse producido.

También, Australia pretendía tomar medidas nacionales mediante la creación de un muro de fuego o firewall cuyo objetivo sería aislar al país de todos los contenidos de violencia de género virtual procedentes de otros países. A este fenómeno se le denomina: *zonificar* la red. De esta forma, el usuario solo podría navegar por una especie de intranet o internet de carácter nacional.

---

[56] I. E. LÁZARO GONZÁLEZ, Y A. BARTOLOMÉ, *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, op. cit, p. 277.

[57] R. SÄNGER, "El bloqueo de páginas web en el Derecho alemán, a través del ejemplo de la ley para dificultar el acceso a páginas web", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013, pp. 191-192.

[58] R. SÄNGER, "El bloqueo de páginas web en el Derecho alemán, a través del ejemplo de la ley para dificultar el acceso a páginas web", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, op. cit., p. 194.

Además, se guardaría el registro de cada una de las actividades realizadas por los usuarios en la *web* a través de códigos identificatorios, es decir, se le asignaría una *IP* específica y el *ISP* estaría obligado a guardar registro de cada una de las actividades en línea, además de filtrar los puertos para evitar la conexión a redes *P2P* y compartir archivos de cualquier otro tipo no autorizados.

Se proseguiría, ejerciendo un control sobre los servidores de alojamiento y de los buscadores para que los usuarios sólo pudieran acceder a los contenidos aprobados por el gobierno. "Este modelo está en discusión en Australia y se emplea en Corea del Norte y China"[59].

En mi opinión no es aceptable esta medida. Esto supondría una restricción de la libertad de información por parte de todos los usuarios de internet y un control abusivo sobre el contenido, monopolizándolo por parte del Estado. Además, al igual que Alemania no sirve de nada impedir la entrada y la viralidad de contenido ilícito propio del delito de violencia de género realizado a través de las *Tic's*, si este contenido sigue siendo visible y compartido por usuarios de otros países al ya haberse producido.

Algunos autores también han señalado la posibilidad de utilizar otras medidas técnicas como el uso de determinadas medidas tecnológicas: la etiqueta meta[60], en vez del uso de robots.txt[61].

GARRIGA destaca la tecnología *PET* o tecnologías de protección de la intimidad: "un sistema de medidas que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin el menoscabo de la funcionalidad del sistema de información. La aplicación de *PET* puede ayudar a diseñar sistemas y servicios de información y comunicación que reduzcan al mínimo la recogida y el empleo de datos personales y faciliten el cumplimiento de la normativa sobre protección de datos"[62].

En el mismo sentido, LESSIG, dice: "La tecnología *PET* permitirá que los usuarios de internet controlen de forma más efectiva los datos personales que revelan y también contarán con una identidad seudónima fiable. Así, si un sitio *web* necesita corroborar la mayoría de edad del usuario la tecnología pueda certificar estos datos sin revelar nada más"[63].

Este autor prosigue diciendo: "la segunda opción sería el uso del protocolo *P3P* para un mayor control sobre el uso de los datos personales. Este

---

[59] O. JARAMILLO CASTRO, "El futuro de la vida pública y privada en las redes sociales", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales,* op cit., p. 411.

[60] Las meta etiqueta que se añaden en la sección de las páginas web HTML constituyen el modo a través del cual los *webmaster* facilitan a los motores de búsqueda información sobre sus sitios *web*, y normalmente se utilizan para ofrecer información a todo tipo de clientes.

[61] Éstos restringen el acceso y rastreo de un sitio *web* por parte de los motores de búsqueda. Cabe aclarar que rastrear no es lo mismo que indexar. El *robots.txt* impide al robot de los buscadores buscar en determinados sitios de las páginas *web* y escarbar para conseguir nuevos contenidos a indexar, cumple con esa función pero ninguna otra.

[62] A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, Dykinson, Madrid, 2015, p. 245.

[63] L. LESSIG, *El Código 2.0*, op. cit., p. 364.

sistema permitirá al usuario darle la información sobre las normas de privacidad de un determinado sitio *web*, reconociendo de manera automática si ese sitio *web* cumple con las preferencias de privacidad del usuario. De esta forma la tecnología ya nos avisa sobre la existencia de un conflicto, siendo la mejor forma para poderlo proteger a través de una regulación"[64].

También, caben adoptar medidas como: la transformación de la información personal recopilada del perfil del usuario, normalmente datos sensibles, (nombre, apellidos, estado civil, imágenes) en marcas de agua[65].

Otra de las posibles medidas adoptables propuestas desde este estudio es la aceptación de un derecho al olvido preventivo. Se ha obtenido la información en las entrevistas realizadas que los *ISP's* tienen las herramientas precisas y sofisticadas para poder hacer realidad este tipo de derecho al olvido.

Este consistiría en informar al titular del comentario realizado o de las imágenes subidas, copiadas y/o difundidas por terceros, aunque sea tras la publicación inicial de dicho comentario u imagen por ella misma, para que pueda decidir la aceptación o denegación de datos publicados sobre ella. Así, se evitaría su falta de control y viralidad en la red, además del daño psicológico producido a la menor víctima de violencia de género virtual.

Este acontecimiento cambia totalmente la posible vulneración de los derechos fundamentales de la menor víctima de violencia de género virtual, pudiendo adelantarse a la posible puesta en peligro de sus bienes más íntimos y a la protección de datos personales. Pero, esto produce un problema para los *ISP's* en cuanto a la implantación de esta tecnología porque supone un aumento del coste respecto a los beneficios.

Quizás por ello, se siga debatiendo, creando y aplicando leyes y todo ello, a pesar del fallo de la sentencia, 13 de mayo del 2014 del TJUE, ya mencionada, donde se debe primar la protección de los derechos fundamentales de los usuarios frente a la ganancia económica de los *ISP's,* aunque parece ser que esto no se cumple del todo. "*La tutela judicial comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y restablecer al perjudicado en el pleno disfrute de sus derechos, así como para prevenir o impedir intromisiones ulteriores".*

En las redes sociales los prestadores de servicios pueden poner en marcha este tipo de normas de autorregulación para garantizar un clima de respeto y paz entre los usuarios. Por otra parte, interesa a los *ISP's* crear este clima para no ahuyentar a sus usuarios y poderles vender publicidad y comercializar con sus datos personales a otras empresas interesadas, pudiendo hacerlo de una forma trasparente a través de estas medidas de autorregulación.

---

[64] L. LESSIG, *El Código 2.0*, op. cit., p. 364.

[65] J. MEGÍAS TEROL, "Privacy by design, construcción de redes sociales garantes de la privacidad", *Derecho y redes sociales,* op. cit., p. 332.

Ante todo esto, la menor podrá optar por la técnica del posicionamiento positivo mientras espera un verdadero derecho al olvido. Es una técnica que consiste en crear reputación positiva, dejando en las últimas páginas los comentarios nocivos de los ciberacosadores.

4. NOTAS DEL REGLAMENTO (UE) 2016/679 RESPECTO A LA AUTORREGULACIÓN

Otra forma de regular el cumplimiento de los *ISP's* es mediante la adhesión a códigos de conducta tal y como dispone el artículo 24 apartado 3º del Reglamento (UE). Los códigos de conducta están contenidos en el artículo 40 del Reglamento (UE) y dice:

> *"1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.*
>
> *2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:*
>
> *a) el tratamiento leal y transparente;*
>
> *b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;*
>
> *c) la recogida de datos personales;*
>
> *d) la seudonimización de datos personales;*
>
> *e) la información proporcionada al público y a los interesados;*
>
> *f) el ejercicio de los derechos de los interesados;*
>
> *g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;*
>
> *h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;*
>
> *i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;*
>
> *j) la transferencia de datos personales a terceros países u organizaciones internacionales, o*
>
> *k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79".*

De esta manera, los Estados miembros, las autoridades de control, el Comité y la Comisión elaborarán códigos de conducta para la efectividad del cumplimiento de los objetivos y finalidades adquiridas en la elaboración de este Reglamento (UE). Además, las asociaciones y organismos representativos podrán elaborar, modificar o ampliar estos códigos de conducta.

El artículo 41 del Reglamento (UE) nombra a un controlador para las obligaciones adquiridas en los códigos de conducta y dispone:

> "*1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente (…).*
>
> *6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos*".

Con esto, el Reglamento (UE) pone a disposición de los usuarios de internet mecanismos de protección de datos mediante el órgano supervisor del contenido contemplado en el código de conducta elaborado u modificado por las diversas partes adheridas o contratantes para su cumplimiento y trasparencia en las decisiones.

Lo mismo ocurre en el ámbito de la cooperación internacional sobre la protección de datos personales regulado en el artículo 50 del Reglamento (UE): "*En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:*

> *a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;*
>
> *b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales; (…)*
>
> *d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países*".

Este artículo presenta un contenido muy ambicioso de cooperación entre las autoridades judiciales, policiales y demás agentes sociales en aras a unificar el tratamiento de la protección de datos personales mediante la figura de la autoridad de control, siendo necesario puesto que hay una gran deficiencia técnica y organizativa en la cooperación internacional

entre Estados, ya que solamente la traducción de la documentación para su envío desde España tarda seis meses en su realización[66].
El artículo 60 del Reglamento (UE) contiene las funciones de la autoridad de control y son:

> "*1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.*
> *2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.*
> *3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista (…).*
> *11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.*
> *12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado*".

Se verá su verdadera factibilidad y aplicabilidad con la entrada en vigor del Reglamento (UE) el 25 de mayo del 2018. En resumen, en él se dispone que: los *ISP's* adoptarán medidas más oportunas, viables y eficaces para conseguir un derecho al olvido, pero sin olvidar, como se comentaba anteriormente, conforme a la "*tecnología disponible*" y "*no sea imposible o exija un esfuerzo desproporcionado*".

5. CONCLUSIÓN

Los derechos fundamentales de la víctima de violencia de género virtual son vulnerados en internet, acentuando su revictimización puesto que la información nociva publicada sobre ella por parte de su ex pareja y, que posteriormente es compartida de forma viral por otros usuarios de la red social, produciendo ciberacoso, e indexada en *Google* está presente en la red, no ha desaparecido, siguiendo sufriendo la violación constante e

[66] Entrevista realizada a la jueza de menores de valencia el 20 de abril del 2017.

ininterrumpida de sus derechos fundamentales y la desprotección de sus datos personales.

Ante esto, el *ISP* aconseja a la menor que denuncie estos hechos. Sin embargo, los *ISP's* ignoran la obligación contenida en el artículo 264 de la LECrim de proceder a denunciar por parte de cualquier persona con conocimiento sobre casos de violencia de género a los cuerpos y seguridad del Estado para proceder a iniciar la fase de investigación del delito y tomar las medidas pertinentes.

También le da recomendaciones cívicas, destacando: la solicitud del borrado de la información nociva sobre ella en cada uno de los perfiles de los usuarios dónde aparezca. Estos tendrán la potestad para borrar esa información de forma voluntaria puesto que los datos publicados en sus muros son propiedad de ellos y no de la menor, aunque sean datos personales sobre ella. A su vez, el *ISP* no podrá hacer nada sin la autorización judicial.

Sin embargo, entiendo que la menor no tiene la tecnología adecuada para poder comprobar en qué muros están publicados sus datos personales puesto que, aunque sea facilitado por el *ISP* en un primer momento mediante las herramientas de rastreo y localización como robots.txt y etiqueta meta, la viralidad de la red desfasa pronto la información obtenida.

Con estas tecnologías las propias redes sociales han evitado la indexación de los perfiles de los usuarios menores de edad en *Google* pero lo compartido a través de un muro de una persona calificada como mayor de edad se indexa en el buscador, aunque se refiera a información de menores.

Por eso, desde *Facebook* recomiendan a sus usuarios solicitar permiso al titular de la imagen o comentario de su publicación. Recomendación no realizada por ningún usuario de las redes sociales. Esto queda manifestado en la propia red social en su "*Decálogo de condiciones*" y pone: "*no será en ningún caso responsable de las interacciones entre los usuarios. Los únicos responsables serán los propios usuarios"*.

Esta situación demuestra la inoperancia de las redes sociales en aplicar eficaces sistemas tecnológicos para impedir la vulneración de la intimidad y la protección de datos personales de los usuarios. Y eximirse de responsabilidad ante la no aplicación en su plataforma virtual de la tecnología estudiada en este artículo y ante la falta de exigencia para su aplicación en la Ley.

Creo que el *ISP* debiera establecer algún tipo de filtro para verificar la titularidad de la información compartida en las redes sociales, ya que solamente facilita a la menor agredida una línea de denuncia; a pesar de estar lucrándose de toda la información que se genera en los muros.

Así pues, el mundo virtual es un medio en continúa evolución y necesita normas generales para su regulación con el apoyo de los códigos actuales. Las leyes reguladoras sobre protección de datos personales suelen quedar obsoletas con rapidez y necesitan ser modificadas en un futuro a través de los sistemas de autorregulación o corregulación. En el caso de la autorregulación pura son acuerdos alcanzados por los propios *ISP's*. En el

caso de la corregulación son pactos realizados por los *ISP's*, el Estado y agentes operantes en internet. Estos acuerdos se llaman normas de conducta.
Por eso, creemos que la corregulación puede dar buenos resultados porque supone la intervención y el control de lo pactado por todas las partes de forma neutra y equilibrada al haber diversos intereses contrapuestos en juego para adoptar propuestas favorables para el usuario y no en virtud del criterio económico de los *ISP's*. Los códigos de conducta no son normas orgánicas u ordinarias sino son consideradas costumbres, pero necesitan del apoyo de la LOPD, la Directiva 95/46CE y otras en su vinculación para prevenir y luchar contra este vacío legal existente en las leyes.
También la autorregulación o corregulación pueden mejorar la cooperación entre países por medio de técnicas extrajudiciales de mediación, conciliación o arbitraje y siempre que no se tenga la necesidad de acudir a los tribunales y solicitar el auxilio de cooperación internacional de la justicia mediante la comisión rogatoria.
De momento, se han planteado los siguientes códigos de conducta, pero sin llegar a un acuerdo entre las partes:
1. Poner plazo de caducidad a los datos publicados o un sistema de encriptación de los datos personales cuya función sea la autodestrucción de los mismos pasado un determinado período de tiempo como es el caso del proyecto *Vanish*.
Sin embargo, la desaparición de la publicación depende de la voluntariedad y decisión del editor. Además, si dependiera del menor infractor o del ciberacosador no es de extrañar la programación de períodos muy extensos. Según esta configuración la menor víctima adopta una actitud pasiva respecto a la publicación de sus datos personales por parte de terceros sin poder decidir sobre ellos.
Además, no soluciona la permanencia de la publicación en la red, es más, la puede agravar al generar más datos con otra fecha de caducidad. Todo esto puede provocar vulnerabilidad y revictimización en la menor víctima ante cada comentario nocivo sobre la publicación.
2. Adoptar filtro de contenidos ante las publicaciones. Estos sirven para limitar el acceso a sitios *web* con contenido nocivo. Considero una buena opción para impedir la viralidad de los datos personales de la menor víctima.
3. La señalización es otra técnica que advierte al usuario sobre el contenido de la *web*. No considero que sea muy eficaz para los casos de violencia de género o ciberacoso puesto que se pretende mostrar al mayor público posible y, además carece de aplicación sobre una información que no debería estar publicada en internet.
4. La etiqueta meta y el uso de robots *txt* evitan la búsqueda, ocultándola y la indexación de la información. Puede resultar muy beneficioso para acabar con la viralidad, aunque ha dado problemas; mostrando lo ocultado.
5. La utilización de la tecnología *PET* o tecnologías de protección de la intimidad es un sistema de medidas que protege el derecho a la intimidad

suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin el menoscabo de la funcionalidad del sistema de información. La aplicación *PET* puede ayudar a diseñar sistemas y servicios de información y comunicación que reduzcan al mínimo la recogida y el empleo de datos personales y faciliten el cumplimiento de la normativa sobre protección de datos.
La considero la mejor tecnología para conseguir un derecho al olvido eficaz.
6. El protocolo *P3P* permite al usuario darle la información sobre las normas de privacidad de un determinado sitio *web*, reconociendo de manera automática si ese sitio *web* cumple con las preferencias de privacidad del usuario. Este sistema sería muy apropiado para aplicar en las redes sociales, sobretodo ante usuarios menores.
Creo que la utilización de la tecnología *PET* posibilita la eliminación de la información nociva de la víctima mediante la aplicación de normas de privacidad de diseño y por defecto, logrando la creación de un verdadero código informático. Sin embargo, nos llama la atención la espera en su aplicación. Además, la sentencia 805/2013 del TS nos dice: que las redes sociales ya disponen de las suficientes herramientas tecnológicas para conseguirlo.
Pero, el contenido del art. 17 del futuro Reglamento favorece la inoperancia de las redes sociales al exigirles la adopción de medidas, pero, eximiéndolas de responsabilidad si estas son: "*medidas razonables, sea imposible o exija un esfuerzo desproporcionado".*
Esto es trasladable a los casos de violencia de género virtual en cuanto a la publicación de material nocivo de la menor víctima por parte de su ex pareja, y su posterior efecto viral entre los usuarios de las redes sociales, siendo una tarea arduosa para la red social su notificación a cada uno de los usuarios implicados; aunque con el enumerado de medidas citadas vemos que es posible.
Una vez más, el legislador, en este caso europeo, no ha concretado ni detallado el grado de exigencia al *ISP* sobre las medidas técnicas y tecnológicas para la viabilidad de la eliminación de la información nociva, abriendo una puerta a la exoneración de responsabilidad de los *ISP's*.
Por tanto, el *ISP* adoptará medidas más oportunas, viables y eficaces para conseguir la eliminación de la información nociva, pero sin olvidar, conforme a la "*tecnología disponible*" y "*no sea imposible o exija un esfuerzo desproporcionado*".
Considero necesario invertir en I+D para incorporar nuevos sistemas tecnológicos para seguir bloqueando los ataques al sistema operativo, es decir, a internet. Es preciso conocer las normas de funcionamiento del *hardware* y *software,* los códigos abiertos, los canales cerrados, los distintos sistemas tecnológicos y herramientas operantes en internet para poner en funcionamiento un sistema tecnológico viable y eficaz tanto para comentarios como par imágenes. Sin olvidar que internet es una verdadera máquina de copiar.
Pero, mientras se crean y se regulan estas nuevas herramientas tecnológicas para eliminar de raíz toda la información de la menor, ella

podrá optar por crear reputación positiva en la red mediante el posicionamiento positivo, introduciendo contenido positivo y posicionarlo en las primeras hojas mediante la técnica SEM y SEO y; de este modo, conseguirá desplazar los mensajes negativos a las últimas páginas del buscador.

Considero que no se trata de una técnica ilegal, puesto que no se trata de modificar la información contenida en internet sobre ella sino crear información positiva sobre ella, además constituye una forma de protegerse.

En definitiva, ante todo esto se necesita ciberseguridad y ciberprotección y también, es recomendable la realización de campañas para concienciar, prevenir, educar y enseñar a los menores cómo actuar ante este tipo de casos.

6. BIBLIOGRAFÍA

J. M. BELTRÁN CASTELLANOS, "Aproximación al régimen jurídico de las redes sociales", *Cuaderno electrónico de estudios jurídicos*, nº. 2, 2014.

K. BENYEKHLEF, P. A. COUTURE-MÉNARD, E. PAQUETTE BÉLANGER, "Menores, redes sociales y el derecho al olvido", *Redes sociales y privacidad del menor*, CON J. L. PIÑAR MAÑAS, S. RODOTA, P. L. MURILLO DE LA CUEVA, K. BENYEKHLEF, C. G. DE GREGORIO, P. FLEISHER, Reus, Madrid, 2011.

G. BUTTARELLI, "Los menores y las nuevas tecnologías", *Redes sociales y privacidad del menor*, CON J. L. PIÑAR MAÑAS, S. RODOTA, P. L. MURILLO DE LA CUEVA, K. BENYEKHLEF, C. G. DE GREGORIO, P. FLEISHER, Reus, Madrid, 2011.

R. I. CORREA GARCÍA, "Violencia y medios", *Violencia escolar y de género: conceptualización y retos educativos,* con A. D. GARCÍA ROJAS, Servicio de publicaciones de la Universidad de Huelva, 2012.

M. L. FERNÁNDEZ ESTEBAN, "Internet y los derechos fundamentales", *Internet, una profecía,* Ariel, Barcelona, 2002.

A. GALÁN MUÑOZ, *Libertad de expresión y responsabilidad penal de contenidos ajenos en internet,* Tirant lo Blanch, Valencia, 2010.

A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, Dykinson, Madrid, 2015.

O. JARAMILLO CASTRO, "El futuro de la vida pública y privada en las redes sociales", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I, CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013.

I. E. LÁZARO GONZÁLEZ, y A. BARTOLOMÉ, *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, Aranzadi, Navarra, 2015.

L. LESSIG, *El Código 2.0*, Traficantes de sueños, 2009.

C. J. MALUQUER DE MONTES I BERNET, "Códigos de conducta y buenas prácticas en la gestión de datos personales", *Protección de datos personales en la sociedad de la información y la vigilancia,* con Mª. R. LLÁCER MATACÁS, Wolters Kluwer, 2011.

J. M. MARTÍNEZ OTERO, "La difusión de *sexting* sin consentimiento del protagonista: un análisis jurídico", *Derecom,* nº. 12, 2013.

J. M. MARTÍNEZ OTERO, *La protección jurídica de los menores en el entorno audiovisual,* Aranzadi, Pamplona, 2013.

N. MARTOS DÍAZ, "Políticas de privacidad, redes sociales y protección de datos. El problema de la verificación de edad", *Derecho y redes sociales*, con A. RALLO LOMBARTE, Y R. MARTÍNEZ MARTÍNEZ, Civitas, Navarra, 2010.

J. MEGÍAS TEROL, "Privacy by design, construcción de redes sociales garantes de la privacidad", *Derecho y redes sociales*, con A. RALLO LOMBARTE, Y R. MARTÍNEZ MARTÍNEZ, Civitas, Navarra, 2010.

A. NIETO MARTÍN, Y M. MAROTO CALATAYUD, "Redes sociales en internet y "data mining" en la prospección e investigación de comportamientos delictivos", *Derecho y redes sociales*, con RALLO LOMBARTE, Y R. MARTÍNEZ MARTÍNEZ, Civitas, Navarra, 2010.

R. M. ORZA LINARES, "El derecho al olvido en internet: algunos intentos para su regulación legal", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I, CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013.

M. PARES SOLIVA, "Ciberacoso. Un tema de reflexión", http://www.visagesoft.com, 2007.

J. L. PIÑAR MAÑAS, "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales", *Redes sociales y privacidad del menor*, CON J. L. PIÑAR MAÑAS, S. RODOTA, P. L. MURILLO DE LA CUEVA, K. BENYEKHLEF, C. G. DE GREGORIO, P. FLEISHER, Reus, Madrid, 2011.

M. RECIO GAYO, *Protección de datos personales e innovación: ¿(in)compatibles?,* Reus, Madrid, 2016.

A. ROJAS, "La responsabilidad de los PSSI y la libertad de expresión. Jurisprudencia reciente", *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías*, con L. COTINO HUESO, Valencia, Servei de publicaciones de la Universidad de Valencia, 2010.

R. SÄNGER, "El bloqueo de páginas web en el Derecho alemán, a través del ejemplo de la ley para dificultar el acceso a páginas web", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I, CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013.

I. SERRANO MAÍLLO, "El derecho a la imagen de los menores en las redes sociales. Referencia especial a la validez del consentimiento", *Libertad de expresión e información en internet. Amenazas y*

protección de los derechos personales, con Madrid, Centro de estudios Políticos y Constitucionales, Madrid, 2013.

P. SIMÓN CASTELLANO, "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, con I, CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013.

D. TERRÁDEZ SALOM, "Formaciones políticas racistas y xenófobas: aproximación al uso de las redes sociales. Libertad de expresión *versus* abuso de derecho", *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales,* con I, CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, Centro de estudios Políticos y Constitucionales, Madrid, 2013.

A. TOURIÑO, *El derecho al olvido y a la intimidad en Internet*, Los libros de la catarata, 2014.

J. VIGURI CORDERO, "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo derecho europeo de protección de datos*: towards a new european data protection regime, con A. RALLO LOMBARTE, y R. GARCÍA MAHAMUT, Tirant lo Blanch, Valencia, 2015.