

PROTOCOLO GENERAL DE ACTUACIÓN ENTRE LA FISCALÍA GENERAL DEL ESTADO Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PARA LA COLABORACIÓN EN MATERIA DE ATENCIÓN A LAS PERSONAS CUYOS DATOS SE HAYAN OBTENIDO Y DIFUNDIDO ILEGÍTIMAMENTE, ESPECIALMENTE EN CASO DE IMÁGENES, VÍDEOS, O AUDIOS CON DATOS SENSIBLES

En Madrid, a 24 de septiembre de 2019

REUNIDAS

De una parte, la Fiscal General del Estado, **D^a María José Segarra Crespo**, nombrada por Real Decreto 702/2018, de 29 de junio, en nombre y representación de la Fiscalía General del Estado (FGE).

De otra parte, la Directora de la Agencia Española de Protección de Datos, **D^a Mar España Martí**, nombrada por Real Decreto 715/2015 de 24 de julio, en nombre y representación de la Agencia Española de Protección de Datos (AEPD).

Ambas partes comparecen en nombre de las Instituciones a las que respectivamente representan y de modo recíproco se reconocen capacidad para formalizar el presente Protocolo General de Actuación y, por ello,

EXPONEN

Primero.

Conforme al artículo 124 de la Constitución Española, el Ministerio Fiscal tiene por misión promover la acción de la justicia en defensa de la legalidad, de los derechos de los

ciudadanos y del interés público tutelado por la ley, de oficio o a petición de los interesados, así como velar por la independencia de los Tribunales, y procurar ante éstos la satisfacción del interés social.

Entre las funciones que corresponden al Ministerio Fiscal se encuentran las de “velar por el respeto de las instituciones constitucionales y de los derechos fundamentales y libertades públicas con cuantas actuaciones exija su defensa”, de “ejercitar las acciones penales y civiles dimanantes de delitos y faltas u oponerse a las ejercitadas por otras cuando proceda” y de “ejercer en materia de responsabilidad penal de menores las funciones que le encomiende la legislación específica, debiendo orientar su actuación a la satisfacción del interés superior del menor” (artículo 3 de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal).

Que la Fiscalía General del Estado ostenta la jefatura superior del Ministerio Fiscal, órgano de relevancia constitucional con personalidad jurídica propia, integrado con autonomía funcional en el Poder Judicial, y ejerce su misión por medio de órganos propios, conforme a los principios de unidad de actuación y dependencia jerárquica y con sujeción, en todo caso, a los de legalidad e imparcialidad.

Segundo.

Que la Agencia Española de Protección de Datos (AEPD) es una autoridad administrativa independiente, con personalidad jurídica propia y plena capacidad pública y privada, que ostenta las competencias atribuidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos o en adelante, RGPD), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDPGDD). Su principal cometido es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación.

Corresponde a la Agencia Española de Protección de Datos ejercer las funciones establecidas en el artículo 57 del RGPD, entre las que se encuentran controlar la aplicación del Reglamento y hacerlo aplicar (artículo 57.1.a)), promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de los datos (artículo 57.1 b)), promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben (artículo 57.1 d)), facilitar información a cualquier interesado en relación con el ejercicio de sus derechos (artículo 57.1.e)), así como desempeñar cualquier otra función relacionada con la protección de los datos personales (artículo 57.1 v)).

Tercero.

Que, a pesar de sus enormes ventajas, en el ámbito de Internet y de las Tecnologías de la Información y Comunicación (TIC) tienden a reproducirse las estructuras sociales, más amplias, en las que se manifiestan las diversas formas de violencia, especialmente contra la mujer, al tiempo que aparecen otras nuevas, propias del entorno en línea. La extensión y el uso intensivo de dispositivos móviles e Internet, redes sociales y servicios como los de mensajería instantánea o de geolocalización, han servido de cauce para la proliferación de conductas violentas, comprobándose que, en muchas ocasiones, Internet y sus servicios y aplicaciones se han utilizado con la finalidad de controlar, amedrentar, acosar, humillar y chantajear a las víctimas, constituyendo un instrumento cada vez más utilizado para dichos fines.

En este sentido, las características de las TIC han dado lugar a nuevas amenazas para las víctimas de estas conductas de violencia, derivadas, entre otras, de la velocidad con la que la información se difunde en este entorno, la posibilidad de acceder a la información gracias a los motores de búsqueda y las dificultades para su eliminación. La facilidad para viralizar, la perdurabilidad en el entorno en línea entrañan nuevas situaciones de riesgo, como pueden ser el acceso y la divulgación sin consentimiento de información sensible, de fotografías o videos de carácter íntimo; la vigilancia, seguimiento y control de actividades en línea; daños a la reputación de la víctima por las conductas conocidas como "sextorsión" o el acoso sexual en línea.

Las mujeres se ven especialmente afectadas por estos fenómenos de violencia en línea, sufriendo como consecuencia daños físicos, psicológicos y económicos. En su encuesta a escala de la Unión Europea (UE) de 2014, la Agencia de Derechos Fundamentales de la UE reveló que el 23% de las mujeres había manifestado haber sufrido acoso o abuso en línea al menos una vez en su vida y que una de cada diez había sido víctima de violencia en línea.

Con la aplicación efectiva del RGPD desde el 25 de mayo de 2018, se pretende hacer frente a los nuevos retos que para la protección de los datos personales han planteado la rápida evolución tecnológica y la globalización derivados del aumento significativo de la magnitud de su recogida e intercambio, tal y como se expone en su Considerando segundo. En este sentido, el RGPD amplía los derechos de los interesados, como el de supresión, de tal forma que quien haya hecho públicos datos personales y esté obligado a suprimirlos esté obligado asimismo a indicar a los responsables del tratamiento que estén tratando los mismos de la solicitud del interesado de que dichos responsables supriman cualquier enlace a ellos, o las copias o réplicas de tales datos. El principio de integridad y confidencialidad impone que los datos personales deban ser tratados de tal manera que se garantice una seguridad adecuada de éstos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Cuarto.

Los daños que provocan estas conductas contrarias a la Ley no afectan sólo a las mujeres en casos de violencia por razón de género. La grabación y difusión de imágenes personales es uno de los instrumentos más utilizados en los casos de acoso, tanto en el entorno laboral como en el escolar -*bullying* y su versión a través de Internet, *cyberbullying*- y de acoso sexual a menores -*grooming* o *sexting*-.

En último término, toda persona, hombre o mujer, de cualquier edad, puede verse afectada por este problema. Empleando los medios que ofrece Internet han proliferado la

suplantación de identidad -para cometer un fraude, o bien para construir a la víctima una reputación falseada - y el “porno vengativo”.

Igualmente, se ha extendido el conocimiento de las aplicaciones que sirven para localizar a distancia la ubicación de un dispositivo móvil, o para activar su cámara y grabar a otra persona desde otro lugar -y así poder monitorizar y controlar a la persona que lo utiliza-.

La abundancia de medios y sistemas de comunicación ha propiciado, asimismo, que los mensajes potencialmente difamatorios y los que incitan al odio se difundan a gran velocidad, de forma prácticamente instantánea.

En este contexto, es cada vez más frecuente que se publiquen en Internet imágenes (fotografías y vídeos) y audios o documentos privados de las víctimas de violencia por razón de género, sin su consentimiento, o de los menores a su cargo, o que se difundan a través de las redes sociales contenidos de esa naturaleza, con intención vejatoria.

Ambas instituciones son conscientes de la gravedad y persistencia de estas conductas ilícitas, y de la perdurabilidad de los daños que ocasionan a las víctimas, al quedar expuesta su intimidad ante todos.

Por ello, ambas partes coinciden en la necesidad de dar pronta respuesta, cada una en el marco de sus respectivas atribuciones y competencias, a las conductas contrarias a la Ley, y de intentar contener la expansión de esas imágenes y audios a través de Internet, en particular cuando se refieran a datos especialmente sensibles.

Quinto.

Conforme a lo establecido en el RGPD, sólo podrán considerarse lícitos los tratamientos de datos que se fundamenten en alguna de las bases legales definidas en su artículo 6.

Por otra parte, el RGPD, en su artículo 9.1 dispone que determinados tipos de datos personales se consideran integrantes de “categorías especiales”. Son los datos



Fiscalía General del Estado



personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Por su más profunda afectación de la intimidad de las personas, y por la gravedad de los daños que puede ocasionar un tratamiento ilegítimo de estos datos que puede vulnerar otros derechos fundamentales, como el derecho a la integridad física y moral, o el derecho a la no discriminación-, se establece con carácter general la prohibición de su tratamiento, salvo que concurra alguno de los supuestos contemplados en el apartado 2 del artículo 9 del RGPD.

Entre los supuestos que se encuentran exceptuados de esa prohibición, cabe mencionar los siguientes:

- el consentimiento explícito otorgado por el interesado para el tratamiento de dichos datos personales (art. 9.2 a)), y
- cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos (art. 9.2.e)).

La Agencia Española de Protección de Datos es competente para asistir a las personas por falta de atención en el ejercicio de los derechos reconocidos en los artículos 15 a 22 del RGPD, entre los que se encuentra el derecho de supresión (artículo 17). Cuando aprecia la existencia de infracción de la normativa en materia de protección de datos personales, incoa procedimientos sancionadores contra los responsables de tales tratamientos ilícitos de datos.

Sexto.

Las medidas de protección que se pueden adoptar, en el marco de la normativa de protección de datos, se han de dirigir a ayudar a aquellas personas, de cualquier sexo y



Fiscalía General del Estado



edad, cuyos datos personales, especialmente los sensibles, hayan sido tratados ilegítimamente por terceros.

La LOPDGDD dispone, en su artículo 84.2, que “la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor”.

Séptimo.

Toda estrategia de actuación debe aunar prevención y reacción. Por tanto, además de investigar y, en su caso, sancionar, las conductas infractoras, es imprescindible, por una parte, la formación en la normativa y la práctica de la protección de datos personales de todos aquellos que como consecuencia del ejercicio de su función han de tratarlos.

Por otra parte, informar, formar y concienciar de la necesidad de proteger los datos personales a sus titulares, en especial a los menores de edad que realizan un uso intensivo de Internet en el que se tratan con asiduidad datos personales, como imágenes, ya sean fotografías o vídeos, o audios, que en algunos casos pueden llegar a constituir un ilícito penal y/o administrativo.

Con el objetivo de conseguir esa formación, el artículo 83 de la LOPDPGDD, dispone la inclusión en el sistema educativo de la competencia digital que contenga los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red. En concordancia con lo anterior, el profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

Para ayudar a su cumplimiento resulta adecuado elaborar materiales que contribuyan a proporcionar formación y sensibilización a los menores de edad y que se puedan facilitar a las Administraciones educativas.

En ambas perspectivas el Ministerio Fiscal, a través de la Fiscalía General del Estado y de las Fiscalías especializadas de Violencia sobre la mujer, Menores y Criminalidad informática, y la Agencia Española de Protección de Datos ya vienen colaborando desde hace tiempo, tanto en el intercambio de información como en el ámbito de la formación y concienciación de usuarios y titulares de los datos y en la elaboración de materiales destinados a esta última finalidad.

Octavo.

Considerando todo lo anteriormente expuesto ambas partes desean promover una relación intensa de colaboración en la prevención y sensibilización frente a la difusión ilegítima de datos personales, en especial en casos de violencia contra la mujer.

Por lo expuesto, las partes acuerdan suscribir el presente Protocolo General de Actuación, que se regirá por las siguientes

CLÁUSULAS

Primera. Objeto

El presente Protocolo General de Actuación tiene por objeto articular la colaboración entre la Fiscalía General del Estado y la Agencia Española de Protección de Datos para la realización de cuantas actuaciones contribuyan a incrementar la eficacia de las medidas de atención a las personas afectadas en caso de que sus datos se hayan obtenido y difundido ilegítimamente a través de Internet, especialmente en caso de imágenes (fotografías y vídeos) y audios con datos sensibles, y particularmente en los casos de violencia contra la mujer.

A estos efectos, se entenderá por datos especialmente sensibles los descritos en el artículo 9.1 del RGPD.

En este marco de actuación, la FGE y la AEPD se prestarán la colaboración mutua que al efecto precisen y seguirán intensificando, con carácter institucional, sus relaciones, estableciendo iniciativas y actividades comunes dirigidas a promover la garantía de los derechos de las víctimas.

Segunda. *Aportaciones de los firmantes.*

1º. Comunicación de hechos que puedan constituir delito.

Cuando se apreciase por parte de la AEPD la existencia de indicios de la comisión de un ilícito penal, se dará inmediatamente traslado a la FGE de toda la información y documentación que se hubiera recabado a fin de que por ésta se lleven a cabo las actuaciones pertinentes.

2º. Actividades de formación.

Ambas partes llevarán a cabo actuaciones conjuntas de formación, particularmente a través de la celebración de seminarios al objeto de concienciar e informar al Ministerio Fiscal sobre la normativa de protección de datos, en particular del RGPD y por la LOPDPGDD. Igualmente, se realizarán seminarios al objeto de difundir la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, así como la normativa por la que se lleve a cabo su transposición.

3º. Educación digital.

Ambas partes expresan su voluntad de apoyar y facilitar el desarrollo y ejercicio de la educación digital de los menores de edad, mediante acciones como la elaboración de materiales y contenidos que ayuden a la prevención, detección y erradicación de situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red, especialmente cuando éstas puedan constituir un ilícito penal. Dichos materiales se pondrán a disposición de las Administraciones educativas que así lo soliciten, a efectos de colaborar en el cumplimiento por su parte del mandato contenido en el apartado 1 del artículo 83 de la LOPDPGDD, en el plazo de un año establecido en la Disposición adicional vigésima primera. Así mismo, la AEPD ofrecerá estos materiales a la Red Iberoamericana de Protección de Datos.

Tercera. Financiación.

El presente Protocolo General de Actuación no conlleva contraprestación económica para ninguno de los firmantes, los cuales asumirán con sus propios recursos los costes de las actuaciones que, en su caso, propongan realizar, sin que se produzca en ningún caso incremento del gasto público.

Cuarta. Medidas de control y seguimiento.

Para el seguimiento de la ejecución del presente Protocolo General de Actuación se constituye una Comisión de Seguimiento, que estará integrada por representantes de la FGE y de la AEPD de manera igualitaria y hasta un máximo de dos por cada parte, que serán designados en cada caso por las autoridades firmantes del Protocolo.

La Comisión de Seguimiento se reunirá en sesión constitutiva en el plazo de 30 días desde la entrada en vigor del Protocolo General de Actuación y determinará qué parte ejerce la función de Secretaría de la Comisión, que será alterna con carácter anual.

Esta Comisión podrá ser convocada por cualquiera de sus miembros, a efectos del oportuno seguimiento del Protocolo General de Actuación, previa indicación de los asuntos

a tratar. La Comisión se reunirá cuantas veces sea preciso y, al menos, una vez al año. De cada reunión la Secretaría levantará la correspondiente acta.

La Comisión será la encargada de proponer las actuaciones y medidas a adoptar para el cumplimiento de los objetivos del Protocolo General de Actuación, los instrumentos adecuados para su ejecución y llevará a cabo su seguimiento y evaluación, con el fin de lograr las mejores condiciones para su consecución.

La Comisión adoptará los acuerdos por unanimidad, salvo que los firmantes, de común acuerdo, dispongan otra cosa. Tendrá capacidad de proponer la modificación, vigencia o resolución del Protocolo General de Actuación, dentro de lo dispuesto en el mismo. Asimismo, podrá convocar a distintas personas en razón a los asuntos a tratar y crear los grupos de trabajo que fueran necesarios para el buen cumplimiento del fin del presente Protocolo General de Actuación.

Las reuniones y actos de este órgano podrán realizarse telemáticamente.

Quinta. *Confidencialidad y protección de datos de carácter personal*

Los firmantes se comprometen a mantener la confidencialidad de todos los datos e informaciones facilitados por la otra parte y que sean concernientes a la ejecución del objeto del presente protocolo, debiendo ambos mantener dicha información en reserva y secreto y no revelarla de ninguna forma, total o parcialmente, a ninguna persona física o jurídica que no sea parte del mismo, salvo en los casos y mediante la forma legalmente previstos.

Si durante la ejecución del presente convenio los firmantes tratasen datos de carácter personal, éstos se obligan al cumplimiento de lo previsto en el RGPD y en la LOPDPGDD.

Sexta. *Modificación y extinción.*

El presente Protocolo General de Actuación podrá ser modificado por mutuo acuerdo entre los firmantes. La modificación se incorporará como adenda al Protocolo y se considerará parte integrante del mismo.

Serán causas de resolución del presente Protocolo General de Actuación el transcurso de su plazo de vigencia sin haberse acordado su prórroga y, en particular, el incumplimiento por una de las partes de las cláusulas establecidas en él, lo que facultará a la otra parte para instar su resolución. También serán causas de extinción el mutuo acuerdo de las partes, o la concurrencia de causa de fuerza mayor que imposibilite el objeto del Protocolo General de Actuación.

Séptima. Legislación aplicable.

El presente Protocolo se regirá por lo establecido en él, y subsidiariamente, por lo dispuesto en la Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público, en lo que le resulte aplicable.

La resolución de cualquier discrepancia que pudiera surgir en la interpretación, ejecución o cumplimiento del Protocolo General de Actuación se llevará a cabo en el seno de la Comisión de Seguimiento

El presente Protocolo no es jurídicamente vinculante ni supone la formalización de compromisos jurídicos concretos y exigibles entre las partes.

Octava. Inicio de la aplicación y duración.

Este Protocolo General de Actuación resultará eficaz desde la fecha de su firma y su periodo de vigencia será de cuatro años, pudiendo prorrogarse por mutuo acuerdo expreso de las partes antes de su finalización, mediante adenda, por otro período de cuatro años.

Y en prueba de conformidad de cuanto antecede, firman el presente Protocolo General de Actuación en dos ejemplares originales, igualmente válidos, en el lugar y la fecha arriba indicadas.

POR LA FISCALÍA GENERAL
DEL ESTADO

María José Segarra Crespo

POR LA AGENCIA ESPAÑOLA DE
PROTECCIÓN DE DATOS



Mar España Martí