PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Manual para periodistas

Autores: Iñigo de Miguel Beriain, Lorena Pérez Campillo (UPV/EHU)

Editor: Federico Caruso (OBC Transeuropa)

Este proyecto ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención nº 788039. Este documento refleja únicamente la opinión del autor y la Agencia no se responsabiliza del uso que pueda hacerse de la información que contiene.

Tabla de contenidos

1. Introducción

El mundo del periodismo es un microcosmos particular en materia de protección de datos. A pesar de que el periodismo implica la recopilación y el almacenamiento de enormes cantidades de información personal en forma de entrevistas, registros de empresas, fotografías y películas, así como su difusión, su marco normativo nunca ha destacado por su claridez. Así, no es de extrañar que cuando se trata de la actividad de los medios de comunicación existan serias preocupaciones relacionadas con la protección de datos (Erdos, 2015, p.8), pues publicar información relacionada con una persona identificada o identificable puede constituir un grave atentado contra su intimidad.

Por otra parte, es innegable que la labor del periodismo es esencial para construir una opinión pública bien informada. De hecho, los miembros de los medios de comunicación son considerados a menudo como guardianes del debate público, con un papel vital en una sociedad democrática. Los periodistas tienen el deber de difundir información e informar al público sobre todos los asuntos de interés público, informaciones que el público también tiene derecho a recibir (Directrices sobre la protección de la intimidad en los medios de comunicación, p.6). Por lo tanto, los medios de comunicación tienen el deber de informar adecuadamente sobre los acontecimientos que puedan ser de interés público, aunque esto pueda poner en riesgo los derechos de las personas afectadas por su publicación.

Consiguientemente, hay dos derechos fundamentales, la libertad de expresión y la intimidad, que a veces entran en colisión en este contezto. Esta colisión sólo puede resolverse mediante su adecuada ponderación en cada caso concreto. ¿Cuándo prevalece el derecho a la protección de datos personales frente al derecho a la libertad de expresión e información y viceversa? Desde el punto de vista jurídica, esta cuestión ya ha sido estudiada con profundidad. Sin embargo, la aprobación del 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 estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD), abre la puerta a nuevos debates.

Creemos que los periodistas y las organizaciones de medios de comunicación deben ser conscientes de esta situación.

Este Manual no pretende centrarse en los aspectos teóricos de esta cuestión, sino proporcionar a los profesionales de la información -periodistas, editores de información, directores de medios de comunicación, etc. - los mecanismos adecuados para garantizar el cumplimiento de las normas mínimas legales y éticas en materia de protección de datos, asegurando al mismo tiempo un adecuado ejercicio de su profesión. En concreto, este Manual está enfocado a cualquier persona que trabaje en un medio de comunicación, ya que todos ellos podrían beneficiarse de las exenciones o excepciones derivadas del artículo 85.2 del RGPD.

Los contenidos de este Manual mezclan varios marcos normativos diferentes: por un lado, la normativa de la UE, principalmente el RGPD; por otro, la regulación del Consejo de Europa a través del Convenio Europeo de Derechos Humanos y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108). Estas fuentes se complementan con la jurisprudencia del TEDH y del TJUE. Como declaró el Grupo de Trabajo del Artículo 29, "un elemento importante que se desprende de la actual situación legislativa de los Estados miembros es que los medios de comunicación, o al menos la prensa, están obligados a respetar ciertas normas que, aunque no forman parte de la legislación sobre protección de datos en sentido propio, contribuyen a la protección de la intimidad de las personas. Dicha legislación y la a menudo rica jurisprudencia en la materia confieren formas específicas de reparación que a veces se consideran un sustituto de la falta de recursos preventivos en virtud de la legislación sobre protección de datos" (A29WP, p. 7). Por lo tanto, las orientaciones que se ofrecen en este Manual pretenden seguir la reglamentación proporcionada por todas las instituciones mencionadas.

El Manual está dividido en varias partes. En sus primeras secciones, expone el marco legal sobre periodismo y cuestiones de protección de datos en el ámbito de la UE. Las secciones cuarta y quinta, en cambio, se centran en cómo abordar las principales cuestiones éticas que deben ser tratadas por un periodista o un medio de comunicación en el marco del RGPD y la normativa del Consejo de Europa. Por último, los anexos

ofrecen información detallada sobre la prueba de equilibrio y el marco normativo a nivel de los Estados miembros.

DESCARGO DE RESPONSABILIDAD: Este documento tiene por objeto ayudar a los periodistas a enfrentarse al reglamento de protección de datos. Sin embargo, su contenido no constituye un asesoramiento jurídico, no pretende sustituir el asesoramiento jurídico y no debe ser considerado como tal. Debe buscar asesoramiento jurídico u otro tipo de asesoramiento profesional en relación con cualquier asunto particular que usted o su organización puedan tener.

2. El marco jurídico relativo a la libertad de expresión y la protección de datos en el ámbito de la UE

El marco normativo relativo al derecho a la libertad de expresión y al régimen de protección de datos en Europa está vinculado principalmente a los ordenamientos jurídicos del Consejo de Europa y de la Unión Europea. En el caso del Consejo de Europa, la regulación es doble. Por un lado, los principales derechos en juego, el derecho a la libertad de expresión y el derecho a la intimidad, forman parte del Convenio Europeo de Derechos Humanos. Su artículo 10.1 establece que “Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa". Este derecho no tiene un carácter absoluto, y puede encontrarse sujeto a limitaciones en los términos que prevé el apartado segundo del artículo 10. El artículo 8, en cambio, se centra en la defensa de la intimidad, estableciendo que:

> "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Por otro lado, el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), también aprobado por el Consejo de Europa, regula el derecho a la protección de datos. De hecho, en la actualidad es el único acuerdo internacional jurídicamente vinculante en esta materia. Sin embargo, el Tribunal Europeo de Derechos Humanos no conoce de las presuntas violaciones de este Convenio, pues el instrumento jurídico con el que trabaja es el Convenio Europeo de Derechos Humanos.

En el contexto de la UE, el derecho a la libertad de expresión se incluyó en el artículo 11 de la Carta de los Derechos Fundamentales de la UE, que dice

> "1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades pœblicas y sin consideración de fronteras.
>
> 2. Se respetan la libertad de los medios de comunicación y su pluralismo".

Por su parte, los artículos 7 y 8 de la Carta incluyen el derecho a la intimidad y el derecho a la protección de los datos personales. En la actualidad, el marco jurídico de la protección de datos está trazado principalmente por el Reglamento (UE) 2016/679 del RGPD. El Tribunal de Justicia de la Unión Europea (TJUE) conoce de las presuntas infracciones de la legislación de la UE. No existe un instrumento equivalente de legislación secundaria global y exhaustiva sobre la libertad de expresión y la libertad de los medios de comunicación, principalmente debido a la posición de la Comisión de que la UE no tiene autoridad para legislar en este ámbito (Biriukova, 6).

El RGPD se aplica siempre que alguien procese (recoja, conserve, utilice o divulgue, por ejemplo) cualquier información sobre una persona viva. Como señala la OIC, "no impide el periodismo responsable, ya que los principios fundamentales son lo suficientemente flexibles como para adaptarse a las prácticas periodísticas cotidianas (...) Sin embargo, los medios de comunicación no están automáticamente exentos y tendrán que asegurarse de tener en cuenta los derechos de protección de datos de las personas. La responsabilidad legal suele recaer en la organización de los medios de comunicación en cuestión y no en los empleados individuales, aunque es probable que los periodistas autónomos tengan sus propias obligaciones por separado". Sin embargo, es bueno tener siempre presente que los empleados de las organizaciones de medios de comunicación deben ser conscientes de sus responsabilidades legales, sobre todo de cómo encarar su cumplimiento cotidiano, cuando trabajan para su empleador.

3. La "exención periodística" en el RGPD

3.1 Introducción y antecedentes

El RGPD es el principal instrumento jurídico en materia de protección de datos a nivel de la UE. Contiene los principios y normas generales que se aplican a todo tratamiento de datos personales en la UE o que implique a ciudadanos de la UE. Dentro de sus disposiciones, es posible encontrar una referencia específica al tratamiento de datos en el ámbito periodístico. Nos referimos a la llamada "exención periodística", tal y como establece el artículo 85 del RGPD, que se muestra en el cuadro siguiente.

Esta cláusula se incluyó en el RGPD como solución para aliviar las tensiones entre la libertad de expresión y el derecho a la protección de datos. De hecho, pretendía codificar la necesidad general de equilibrar estos dos derechos fundamentales. A primera vista, simplemente dejó en manos de los Estados miembros la posibilidad de eximir a quienes ejercen su libertad de expresión con "fines periodísticos" de las normas y obligaciones específicas del RGPD (Biriukova, 14).

Esta exención periodística no era una novedad en la normativa de la UE. El artículo 9 de la Directiva de Protección de Datos de 1995, predecesora del RGPD, ya incluía una disposición similar, lo que supuso cierta divergencia en la regulación de esta cuestión en

los Estados miembros de la UE. Una Recomendación del Grupo de Trabajo del Artículo 29 [1]resumió la situación dividiendo a los Estados miembros en tres grupos principales:

> "a) En algunos casos, la legislación sobre protección de datos no contiene ninguna exención expresa de la aplicación de sus disposiciones a los medios de comunicación. Esta es la situación actual en Bélgica, España, Portugal, Suecia y el Reino Unido.
>
> b) En otros casos, los medios de comunicación están exentos de la aplicación de varias disposiciones de la legislación sobre protección de datos. Esta es la situación actual en el caso de Alemania, Francia, los Países Bajos, Austria y Finlandia. El proyecto de legislación italiana prevé excepciones similares.
>
> c) En otros casos, los medios de comunicación están exentos de la legislación general de protección de datos y están regulados por disposiciones específicas de protección de datos. Este es el caso de Dinamarca para todos los medios de comunicación y de Alemania en relación con los organismos públicos de radiodifusión, que no están cubiertos por las leyes de protección de datos federales o de los Estados federados, sino que están sujetos a disposiciones específicas de protección de datos en los tratados entre Estados federados que los regulan".

El RGPD sólo introdujo cambios menores en este escenario. De hecho, el artículo 85 del RGPD proporciona un marco de actuación muy amplio a los Estados miembros. Deben determinar el alcance de la exención periodística y las circunstancias en las que se aplica. Sin embargo, para que sus desarrollos normativos sean válidos, deben ajustarse a las disposiciones del RGPD y del Convenio Europeo de Derechos Humanos (CEDH). Por tanto, hay que pensar en las normas a seguir en el ámbito periodístico desde una doble perspectiva. Por un lado, hay que tener siempre presente una serie de normas que se recogen en el RGPD y/o en el CEDH y en la jurisprudencia del TJUE y del TEDH. Éstas

1 Sin embargo, el Grupo de Trabajo también informó de que "las diferencias entre estos tres modelos no deberían sobreestimarse. En la mayoría de los casos, independientemente de cualquier excepción expresa que pueda existir, la legislación sobre protección de datos no se aplica plenamente a los medios de comunicación debido al estatus constitucional especial de las normas sobre libertad de expresión y libertad de prensa. Estas normas limitan de facto la aplicación de las disposiciones sustantivas de protección de datos o, al menos, su aplicación efectiva. En cambio, los datos ordinarios". Véase: Grupo de trabajo sobre la protección de las personas en lo que respecta al tratamiento de datos personales, Derecho de la protección de datos y medios de comunicación, Recomendación 1/97, pp. 6-7, en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf.

deben seguirse estrictamente en el ejercicio de esta profesión. Por otro lado, hay que tener en cuenta que pueden existir ciertas diferencias entre los Estados miembros, en función del marco normativo concreto. En cualquier caso, no deben ser excesivas, ya que siempre deben respetarse los principios y normas del RGPD y del CEDH.

No obstante, es importante destacar que algunos Estados miembros no se han adherido plenamente a estas normas. En Bulgaria, por ejemplo, el Tribunal Constitucional ha declarado recientemente inconstitucional el enfoque nacional de la aplicación del artículo 85. Esto se debió a la inclusión de un artículo en la Ley de Protección de Datos Personales que establecía 10 criterios para decidir si los periodistas habían cumplido con el equilibrio entre el derecho a la información y el de la protección de datos personales. El Tribunal consideró que dichos criterios eran demasiado vagos y podían crear un riesgo de interpretaciones arbitrarias, circunstancia que abría el camino para que la Comisión de Protección de Datos tuviera un poder imprevisible para interpretar no necesariamente en el interés público la información plural sobre las políticas y actividades del gobierno[2].

Además, en Rumanía, el regulador de la protección de datos ha sido criticado por utilizar el RGPD para silenciar las voces críticas de los medios de comunicación nacionales. En noviembre de 2018, se informó de un caso en Rumanía que podría servir para reflejar la tensión entre la protección de datos y la libertad de expresión. Estaba relacionado con un artículo sobre un escándalo de corrupción que implicaba a un político y su estrecha relación con una empresa investigada por fraude que se publicó en la página de Facebook de Rise Project, con sede en Bucarest. Tiempo después de la publicación, la autoridad rumana de protección de datos (ANSPDCP) envió una serie de preguntas a los periodistas autores del artículo.

En teoría, esto se debía a la necesidad de garantizar un equilibrio entre el derecho a la protección de los datos personales, la libertad de expresión y el derecho a la información. La autoridad sostuvo que los periodistas de Rise habían violado el RGPD al publicar los vídeos, las fotos y los documentos -en esencia, los datos privados de los ciudadanos rumanos- para apoyar las alegaciones de los reporteros. A los periodistas se

2 El Tribunal Constitucional de Bulgaria rechaza la cláusula de la ley de protección de datos, 17 de noviembre de 2019, https://sofiaglobe.com/2019/11/17/bulgarias-constitutional-court-rejects-data-protection-law-clause-on-media/#:~:text=El%20TribunalConstitucional%20deBulgaria%20ha%20dictaminado,que%20de%20datospersonales%20protección.

les pidió información que pudiera revelar las fuentes del artículo, bajo el anuncio de que, si no cooperaban, podrían enfrentarse a una sanción de hasta 20 millones de euros (Warner, 2019).

Un grupo de doce organizaciones de derechos humanos y de medios de comunicación reaccionó a esta petición enviando una carta abierta a la ANSPDCP en la que se pedía que ésta analizara detenidamente los casos en los que el RGPD pudieran poner en peligro la libertad de expresión. También exigía que se pusiera en marcha un mecanismo urgente y transparente para evaluar las reclamaciones relacionadas con las operaciones de tratamiento de datos con fines periodísticos. Al mismo tiempo, dieciséis ONG de derechos digitales enviaron una carta al Consejo Europeo de Protección de Datos, con la ANSPDCP y la Comisión Europea en copia, pidiendo que el GDPR no sea mal utilizado para amenazar la libertad de los medios de comunicación en Rumania (Benezic, 2018). Más tarde, algunos eurodiputados en Bruselas criticaron el caso contra el Proyecto Rise y cuestionaron la interpretación rumana de la aplicación del GDPR. Finalmente, todo esto dio lugar a advertencias de la Comisión Europea (Nielsen, 2018). Sin embargo, en el momento actual es difícil saber lo que podría ocurrir finalmente, ya que el caso está actualmente en curso.

Hay otros Estados miembros que han tomado un planteamiento totalmente distinto. Por ejemplo, Suecia consideró que el artículo 85 del RGPD daba un mayor espacio para las exenciones a los Estados miembros que la Directiva de protección de datos, entre otras cosas porque no exige que el tratamiento se realice "únicamente" con fines periodísticos (una redacción que se incluía en la Directiva). Además, el Gobierno sueco alegó que el considerando 153 del RGPD establece que el concepto de libertad de expresión debe interpretarse de forma amplia. Sobre esta base, la nueva Ley de Protección de Datos incluye exenciones o excepciones más amplias que la Ley de Datos Personales de 1998 (McCullagh, 45).

3.2 El ámbito personal de la exención

¿Qué significa "fines periodísticos"? ¿Qué significa "periodismo"? No hay nada parecido a una definición de periodismo en el Reglamento, ya que se eliminó de los primeros

borradores del RGPD[3]. Algunos Estados miembros han creado sus propias definiciones. La mayoría de ellas son bastante abiertas, con la principal excepción de Austria, que reservó la exención exclusivamente a "las empresas de medios de comunicación, los servicios de medios de comunicación y sus empleados" (Cullagh, 2019, p.5).

Sin embargo, parece bastante claro que el RGPD opta por un significado abierto e inclusivo del término, que podría ser aplicable, aunque la normativa nacional no lo refleje. De hecho, en el caso Buivids[4], el TJUE aceptó que la excepción de periodista era aplicable a un ciudadano que publicó una grabación de vídeo en Youtube, demostrando que el objeto de la grabación y la publicación de la misma era la divulgación de información, opiniones o ideas al público. Del mismo modo, en el caso[5] Satamedia, el TJUE dictaminó que las actividades de recopilación y difusión de datos también podían considerarse "periodísticas", si su objetivo era revelar al público información, opiniones o ideas, independientemente de los medios empleados. El hecho de que el controlador fuera una organización sin ánimo de lucro se consideró irrelevante para estos fines.

No está claro qué ocurriría si una organización austriaca que pudiera considerarse una empresa de medios de comunicación o un servicio de medios de comunicación aplicara alguna de las derogaciones o excepciones previstas en el artículo 85. De alguna manera, esto crearía un conflicto entre la normativa austriaca y el RGPD, que pide explícitamente una ampliación del concepto de periodismo. En nuestra opinión, es probable que prevalezca la interpretación del GDPR.

Teniendo esto en cuenta, parece que una definición amplia del periodismo tiene mucho más sentido que una más limirada. Natalija Bitiukova ha defendido que "el periodismo se refiere a la producción y distribución de información y noticias a un número indeterminado de personas en busca del interés público y la contribución al debate público" (Bitiukova, p.4). En nuestra opinión, su definición encaja perfectamente con el RGPD.

3 En efecto, el proyecto decía: "Los Estados miembros deben clasificar las actividades como "periodísticas" a efectos de las exenciones y excepciones que se establezcan en virtud del presente Reglamento si el objeto de estas actividades es la divulgación al público de informaciones, opiniones o ideas, independientemente del medio que se utilice para transmitirlas. No deben limitarse a las empresas de medios de comunicación y pueden realizarse con fines lucrativos o no" (Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), COM/2012/011, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52012PC0011).

4 TJUE, Sergejs Buivids contra Datu valsts inspekcija, C-345/17, 14 de febrero de 2019.

5 TJUE, Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy, C-73/07, 16 de diciembre de 2008

El periodismo, por tanto, debe definirse como una actividad que abarca toda la producción de noticias, asuntos de actualidad, consumo o deportes[6]. Esto es así porque la exención cubre la información procesada sólo para realizar actividades periodísticas. El concepto también puede incluir a los editores de blogs o páginas web de Internet, ya que los comentarios realizados en estas plataformas deben considerarse como una manifestación de su propia libertad de expresión. Por supuesto, esto no significa que todos los blogs o comentarios publicados en Internet deban considerarse una actividad periodística, ya que algunos blogueros simplemente pretenden participar en interacciones sociales comunes o en otro uso recreativo de Internet. Además, los motores de búsqueda están expresamente excluidos del concepto y, por tanto, de la excepción[7].

3.3 Tratamiento de datos personales: ámbito de aplicación material

Como se ha visto, el artículo 85 especifica que las exenciones o excepciones pueden ser aplicables a todos los que pretendan divulgar al público información, opiniones o ideas. Sin embargo, ¿qué tipo de datos pueden considerarse como tales? ¿Qué datos personales pueden tratarse con fines periodísticos sin tener que cumplir el RGPD? De nuevo, no hay una respuesta sencilla a esta pregunta. En principio, los Estados miembros tienen voz y voto sobre el alcance material de la exención para periodistas y sus políticas no son siempre las mismas. Por ejemplo, el artículo 7 de la ley rumana nº 190/2018, que introduce excepciones para el tratamiento de datos personales con fines periodísticos, ofrece solo tres escenarios alternativos en los que los datos personales pueden ser tratados con fines periodísticos[8]:

6 Según el ICO, "junto con el arte y la literatura, consideramos que es probable que cubra todo lo que se publica en un periódico o revista, o se emite en la radio o la televisión, es decir, toda la producción de los medios de comunicación impresos y audiovisuales, con la excepción de la publicidad de pago (...) Implicaría una amplia gama de actividades, agrupadas de forma general en la producción (incluyendo la recopilación, la redacción y la verificación del material), la redacción, la publicación o la emisión, y la gestión de las normas (incluyendo la formación, la gestión y la supervisión del personal). En resumen, la exención puede cubrir potencialmente casi toda la información recopilada o creada como parte de la producción diaria de los medios de comunicación de la prensa y la radiodifusión, y de los medios de comunicación comparables en línea de noticias o asuntos de actualidad. Sin embargo, los ingresos publicitarios, la gestión de la propiedad, la deuda financiera, la circulación o las relaciones públicas no suelen considerarse periodismo" (ICO, 29).

7 TJUE, Google Spain SL y Google Inc. v Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, C-131/12, 13 de mayo de 2014, par. 81

8 Denuncia a la Comisión de la UE por parte de La Asociación para la Tecnología e Internet (ApTI), 2018, en: https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

1) si se trata de datos personales que fueron claramente hechos públicos por el interesado;

2) si los datos personales estuvieran estrechamente relacionados con la calidad de persona pública del interesado; o

3) si los datos personales están estrechamente relacionados con el carácter público de los actos en los que participa el interesado. Si se da alguna de estas tres situaciones, el RGPD (excepto el capítulo de sanciones) queda totalmente excluido de su aplicación.

Estos tres escenarios alternativos son extremadamente limitados en comparación con la jurisprudencia actual, tanto del Tribunal de Justicia de la Unión Europea como del Tribunal Europeo de Derechos Humanos. Ambos tribunales consideran que hay varios factores que deben sopesarse antes de un análisis, siendo los más importantes la contribución a un debate de interés público, por un lado, y el daño a la vida privada de los interesados, por otro. Por lo tanto, la ley rumana no parece realizar una conciliación adecuada entre el derecho a la protección de datos personales y el derecho a la libertad de expresión e información.

El Reino Unido adoptó un enfoque totalmente diferente. Su Ley de Protección de Datos de 2018 considera que la excepción del periodista se aplica al tratamiento de datos personales cuando se cumplen tres condiciones acumulativas:

- los datos en cuestión deben ser tratados con vistas a la publicación de material periodístico,
- el responsable del tratamiento debe creer razonablemente que, teniendo en cuenta la especial importancia del interés público en la libertad de expresión, la publicación será de interés público,
- y el responsable del tratamiento debe creer razonablemente que la aplicación de la disposición del RGPD enumerada sería incompatible con su finalidad periodística.

Este enfoque parece mucho más acorde con el marco normativo europeo en materia de libertad de expresión y privacidad.

3.4. La condición para la exención

Las exenciones o excepciones previstas en el artículo 85 sólo son aplicables "si son necesarias para conciliar el derecho a la protección de datos personales con la libertad de expresión e información". ¿Cuándo se aplica esta necesidad? El considerando 153 del RGPD proporciona una valiosa información para responder a esta pregunta:

> *El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.*

Así, el RGPD está dispuesto a garantizar un equilibrio adecuado entre la protección de datos y el derecho a la libertad de expresión e información, consagrado en el artículo 11

de la Carta[9]. Por ello, *las excepciones o exenciones a determinadas disposiciones del RGPD* sólo se aplican *si son necesarias para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión e información*. Esta idea de equilibrar ambos derechos ha sido respaldada por la jurisprudencia del TEDH y del TJUE, que exige que se ponderen caso por caso siempre que exista un conflicto real entre dichos derechos. El punto clave, sin embargo, es cómo proceder para hacerlo. El ICO afirma que, para hacerlo adecuadamente, las organizaciones deben tener en cuenta:

- el interés público general en la libertad de expresión,
- cualquier interés público específico en la materia,
- el nivel de intrusión en la vida privada de un individuo, incluyendo si la historia pudiera ser perseguida y publicada de una manera menos intrusiva, y
- el daño potencial que podría causarse a los individuos. Las orientaciones existentes en los códigos de prácticas del sector pueden ayudar a las organizaciones a reflexionar sobre lo que es de interés[10] público.

En este contexto, la noción de interés público es especialmente relevante, según la jurisprudencia del Tribunal de Justicia de la UE o del Tribunal Europeo de Derechos Humanos, como se menciona en casos como Buivids[11] o Satakunnan contra Finlandia[12]. Sin embargo, es difícil de definir. De hecho, el TEDH se ha abstenido históricamente de dar una definición de "interés público". Sin embargo, declaró, en el contexto de los casos[13] Von Hannover, que "un primer criterio esencial es la contribución de las fotos o artículos de prensa a un debate de interés general". Así, parece que esta noción abarca "el debate público, político e histórico, los asuntos relacionados con los políticos, el comportamiento de los funcionarios, las grandes empresas, los gobiernos, los asuntos relacionados con la delincuencia. Sin embargo, otros asuntos menos aparentes también pueden considerarse de interés público o general" (Biriukova, 21).

9 Artículo 11. Libertad de expresión e información

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y de recibir y difundir informaciones e ideas sin que pueda haber injerencia de la autoridad pública y sin consideración de fronteras.

2. Se respetará la libertad y el pluralismo de los medios de comunicación.

10 ICO, p. 34

11 TJUE, Sergejs Buivids contra Datu valsts inspekcija, C-345/17, 14 de febrero de 2019, par. 60-61.

12 TEDH, Satakunnan Markkinapörssi Oy y Satamedia Oy c. Finlandia, App no 931/13, 21 de julio de 2015.

13 TEDH, Von Hannover c. Alemania (nº 2), Ap. nº 40660/08 y 60641/08, 7 de febrero de 2012, par. 109.

En resumen, hay algunas variables que seguramente estarán presentes en la definición de interés público, que debe implicar "un elemento de proporcionalidad: no puede ser de interés público interferir de forma desproporcionada o irreflexiva en los derechos fundamentales de privacidad y protección de datos de una persona. Si el método de investigación o los detalles que se van a publicar son especialmente intrusivos o perjudiciales para una persona, se requerirá un argumento de interés público más sólido y específico para el caso que lo justifique, por encima del interés público general en la libertad de expresión" (ICO, 33). En efecto, el interés público no puede reducirse a la sed de información del público sobre la vida privada de otros o al deseo de sensacionalismo o incluso de voyeurismo del lector, como la publicación de detalles de las actividades sexuales de un personaje público. Si el único objetivo de un artículo es satisfacer la curiosidad de los lectores sobre los detalles de la vida privada de una persona, no puede considerarse que contribuya a ningún debate de interés general para la sociedad (Directrices para la protección de la intimidad en los medios de comunicación, 12). Por ejemplo, en el caso Standard Verlags GmbH contra Austria (nº 2), se juzgó que un periódico había violado la intimidad de las personas afectadas al publicar un artículo en el que comentaba los rumores de que la esposa del entonces presidente austriaco pretendía divorciarse de él y mantenía estrechos contactos con otro político. En opinión del Tribunal, los periodistas no pueden informar de cotilleos sin sentido sobre los matrimonios de los políticos. Las Directrices sobre la protección de la intimidad en los medios de comunicación destacan que "a la hora de determinar si una persona es una figura pública, tiene poca importancia para los periodistas si una determinada persona es realmente conocida por el público. Los periodistas no pueden verse limitados por las afirmaciones de los interesados de que no son realmente conocidos por el público. Lo que importa es si la persona ha entrado en la escena pública participando en un debate público, siendo activa en un campo de interés público o en un debate público" (Directrices para la protección de la intimidad en los medios de comunicación, 12-20). En la siguiente tabla se ha incorporado un conjunto de ejemplos de sentencias elaboradas por el TEDH y recogidas en las Directrices (las referencias completas se incluyen en la sección Fuentes de información al final de este Manual).

Estas consideraciones abren la puerta a un debate más amplio sobre cómo equilibrar el interés público con el derecho a la intimidad. Esto se analizará en la sección de este

Manual dedicada al interés legítimo como fundamento jurídico del tratamiento de datos personales.

3.5 Alcance material de la excepción

El artículo 85 establece un amplio ámbito de aplicación para las excepciones y exenciones, ya que menciona el capítulo II (principios), el capítulo III (derechos del interesado), el capítulo IV (responsable y encargado del tratamiento), el capítulo V (transferencia de datos personales a terceros países u organizaciones internacionales), el capítulo VI (autoridades de control independientes), el capítulo VII (cooperación y coherencia) y el capítulo IX (situaciones específicas de tratamiento de datos). Por lo tanto, las excepciones y derogaciones podrían abarcar los *principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos.*

Sin embargo, es esencial observar que este amplio alcance no se aplicará necesariamente a todos los Estados miembros de la UE. La cláusula declara explícitamente que los Estados miembros establecerán exenciones o excepciones, pero no enumera dichas excepciones. Sólo declara que *deberán* conciliar por ley el derecho a la protección de los datos personales con el derecho a la libertad de expresión e información, incluido el tratamiento con fines periodísticos y de expresión académica, artística o literaria.

Por lo tanto, la decisión sobre las medidas concretas a adoptar corresponde a los Estados miembros. Se supone que éstos deben desarrollar dicho marco normativo y notificar a la Comisión las disposiciones adoptadas en materia de exenciones o excepciones y, sin demora, cualquier ley de modificación o enmienda posterior que les afecte. En el momento actual (noviembre de 2020), no todos los Estados miembros han desarrollado dicho marco jurídico. En el Anexo II incluimos información sobre la normativa incorporada por los estados miembros de la UE, incluyendo los datos en los que se introdujo la modificación. Sin embargo, puede ocurrir que algunos países hayan modificado su marco legal con posterioridad.

3.6 Normativa aplicable

En general, los periodistas deben tratar de evitar el envío de datos personales fuera del Espacio Económico Europeo (EEE) sin una protección adecuada. Lo que se considere "protección adecuada" dependerá "de la naturaleza de la información, la finalidad de la transferencia y la situación jurídica en el otro extremo, entre otras cosas". Este principio no impedirá la publicación en línea, incluso si esto hace que la información esté disponible fuera del EEE. Si la publicación cumple con la DPA en otros aspectos (o está exenta por ser de interés público), será apropiado publicarla a todo el mundo" (ICO, 26).

¿Qué ocurre si los periodistas tienen su sede en un Estado miembro, pero desean publicar contenidos en otros países o en Internet? El RGPD establece que "cuando esas exenciones o excepciones difieran de un Estado miembro a otro, se aplicará la legislación del Estado miembro al que esté sujeto el responsable del tratamiento". Esto podría tener consecuencias extrañas. Por ejemplo, parece que una publicación de un editor (o bloguero) con sede en España podría beneficiarse de las normas relativamente laxas sobre la privacidad de las "celebridades" de ese país, aunque la publicación en cuestión estaría prohibida si la publicara un editor francés y aunque la publicación española sea fácilmente (y en línea directamente) accesible desde Francia. Es más, incluso podrían beneficiarse de estar radicados en España, aunque la publicación fuera en francés y estuviera dirigida a un público francés. Esta breve sugerencia sobre la ley aplicable es insuficiente para el entorno en línea. A menos que se aborde de forma más específica en el sucesor de la Directiva sobre privacidad electrónica, podría hacer que el entorno jurídico de la libertad de expresión sea muy poco claro, especialmente en el entorno digital en línea (EDRI, 51).

4. El GDPR aplicado al periodismo

4.1 El GDPR en pocas palabras

El RGPD pretende estimular la creación de un espacio de libertad, seguridad y justicia y de una unión económica, el progreso económico y social, el fortalecimiento y la convergencia de las economías dentro del mercado interior y el bienestar de las

personas físicas (considerando 2). Su objetivo es garantizar un equilibrio adecuado entre la protección de datos y la privacidad y algunos otros derechos fundamentales, como la libertad de expresión, por ejemplo.

El Reglamento se centra principalmente en el tratamiento de datos personales, es decir, "cualquier información sobre una persona viva identificable que esté (o vaya a estar) almacenada en un ordenador u otro dispositivo digital, o archivada en un sistema de ficheros organizado donde pueda encontrarse fácilmente" (ICO, 2). Por tanto, se centra en los datos estructurados que revelan información sobre una persona viva. Por ejemplo, las notas escritas a mano no se consideran datos personales. Sin embargo, si alguien transfiere esas notas a un ordenador y las organiza, se convertirán en datos personales.

Del mismo modo, la información anonimizada no es un dato personal, pero no debe confundirse con la información seudonimizada, es decir, aquella que puede estar vinculada a una persona (véase su conceptualización más adelante). La información que se refiere a personas fallecidas tampoco está protegida por el RGPD, aunque su publicación pueda generar problemas relacionados con el derecho al honor o la imagen pública. Por otra parte, el hecho de que un dato sea público o privado no cambia su naturaleza de dato personal. Sin embargo, puede tener consecuencias para la legalidad de su tratamiento.

4.2 Las bases legales para el tratamiento de datos

En general, no se puede tratar ningún dato personal si no existe una base legal para ello. El artículo 6 del Reglamento establece hasta seis fundamentos jurídicos que legitiman el tratamiento, a saber:

1. el interesado ha dado su consentimiento al tratamiento de sus datos personales para uno o varios fines específicos
2. el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para tomar medidas a petición del interesado antes de celebrar un contrato

3. el tratamiento es necesario para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento
4. el tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física
5. el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
6. el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Hay tres bases legales para el tratamiento que suelen aplicarse a los periodistas. Son el consentimiento, el interés público y el interés legítimo. En el apartado 5.3 se analizan en detalle.

4.3 Las categorías especiales de datos

Algunos datos están especialmente protegidos por el RGPD y los periodistas deben ser extremadamente cuidadosos si están dispuestos a tratarlos. Estas categorías especiales comprenden: los datos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la pertenencia a un sindicato, y el tratamiento de datos genéticos, datos biométricos con el fin de identificar de forma única a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Un responsable del tratamiento sólo puede tratar estos datos si tiene un motivo legal para proceder de acuerdo con el artículo 6 del RGPD y se aplica alguna de las circunstancias que alivian la prohibición introducida para su tratamiento por el artículo 9.1. Estas circunstancias se enumeran en el artículo 9.2 del RGPD. En principio, el consentimiento explícito del sujeto que proporciona la información o la divulgación pública por parte de las personas con las que se relaciona la información parecen las

circunstancias más prometedoras. De todos modos, el responsable del tratamiento debe tener siempre en cuenta que, dado que este tipo de datos son especialmente sensibles, sólo debe divulgarlos si existe un interés público sustancial. En el siguiente cuadro se puede encontrar una recopilación del TEDH proporcionada por las Directrices sobre la protección de la intimidad en los medios de comunicación, que recoge la jurisprudencia del TEDH

En relación con esta cuestión, la ICO ha declarado que "si la información es "datos personales sensibles", las organizaciones deben cumplir también una de las siguientes condiciones:

- la persona ha dado su consentimiento explícito
- la información ya se ha hecho pública como resultado de los pasos que una persona ha dado deliberadamente. No basta con que ya sea de dominio público, sino que debe ser la persona en cuestión la que tome las medidas que la hagan pública" (ICO, 41).

4.4 Derechos del interesado y obligaciones del responsable del tratamiento

Por último, es esencial mencionar que el RGPD otorga a los interesados algunos derechos esenciales que deben ser respetados, a menos que se apliquen ciertas excepciones. Entre ellos se encuentran:

- el derecho de acceso. El interesado tendrá derecho a obtener del responsable del tratamiento la confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, el acceso a los datos personales y a la información relativa a cuestiones como los fines del tratamiento, las categorías de datos personales de que se trata, los destinatarios o categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales, etc. (véase el artículo 15 del RGPD).
- Derecho de rectificación. El interesado tendrá derecho a obtener del responsable del tratamiento, sin demora injustificada, la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el

interesado tendrá derecho a que se completen los datos personales incompletos, incluso mediante la presentación de una declaración complementaria.

- Derecho de supresión ("derecho al olvido"). El interesado tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le conciernen sin demora indebida y el responsable del tratamiento tendrá la obligación de suprimir los datos personales sin demora indebida cuando se den las circunstancias enumeradas en el artículo 17 del RGPD.

- Derecho a la limitación del tratamiento. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento cuando el interesado impugne la exactitud de los datos personales, durante un período que permita al responsable del tratamiento verificar la exactitud de los datos personales; o el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; o el responsable del tratamiento ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para el establecimiento, el ejercicio o la defensa de reclamaciones legales; o el interesado se ha opuesto al tratamiento con arreglo al artículo 21, apartado 1, a la espera de que se verifique si los motivos legítimos del responsable del tratamiento prevalecen sobre los del interesado.

- Derecho a la portabilidad de los datos. El interesado tendrá derecho a recibir los datos personales que le conciernen y que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica.

Además, hay dos deberes esenciales que el responsable del tratamiento debe atender según el RGPD:

- obligación de proporcionar al interesado información sobre el procesamiento de sus datos, independientemente de que hayan sido recabos de él. Esto incluye información sobre la identidad y los datos de contacto del responsable del tratamiento y, en su caso, del representante del responsable del tratamiento, los datos de contacto del delegado de protección de datos, en su caso, los fines del

tratamiento a los que se destinan los datos personales, así como la base jurídica del tratamiento, etc. (véanse los artículos 13 y 14 del RGPD)

- obligación de notificación de la rectificación o supresión de los datos personales o de la limitación del tratamiento. El responsable del tratamiento comunicará toda rectificación o supresión de datos personales o la limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que ello resulte imposible o suponga un esfuerzo desproporcionado. El responsable del tratamiento informará al interesado sobre dichos destinatarios si éste lo solicita.

4.5 Los principales conceptos

Hay varios conceptos que son especialmente relevantes en el contexto del RGPD y los periodistas deben conocer su significado. Estos son:

- datos personales": toda información relativa a una persona física identificada o identificable ("interesado"); una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular mediante un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona física.

- tratamiento": cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

- seudonimización": el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

- fichero": todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

- "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;

- “Encargado del tratamiento": : la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

- "destinatario": la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

- tercero": persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

- El consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

5. Los Principios aplicados al periodismo

5.1 Introducción

Esta sección pretende ofrecer algunos consejos concretos para que los periodistas se enfrenten a sus actividades cotidianas. Utiliza un lenguaje sencillo y fácil de entender, que puede ser comprendido por un no experto. Está estructurado sobre la base de los principios establecidos por el RGPD. Esto se debe a un hecho sencillo: el tratamiento debe respetar siempre esos principios, que son el núcleo del RGPD. Esto significa que, aunque tenga una base legal para procesar datos personales, debe respetar estos principios fundamentales. De lo contrario, su tratamiento no será considerado legal.

En las siguientes páginas, mostramos estos principios y ofrecemos consejos sobre cómo tratarlos desde la perspectiva de un periodista. Estos consejos incorporan las recomendaciones formuladas por el Consejo de Europa en sus Directrices sobre la protección de la privacidad en los medios de comunicación aprobadas conjuntamente en junio de 2018 por el Comité Directivo de Medios de Comunicación y Sociedad de la Información (CDMSI) y el Comité del Convenio 108 (Convenio de Protección de Datos del Consejo de Europa). Estas Directrices comprenden un conjunto de normas del Consejo de Europa (el Consejo/CoE) y del Tribunal Europeo de Derechos Humanos (el Tribunal) relativas a la protección de la intimidad de los personajes públicos y privados en los medios de comunicación. **Por favor, tenga siempre presente que esta parte del Manual ofrece principalmente orientación sobre cómo tratar los principios adoptados por el RGPD desde una perspectiva ética. Para garantizar un cumplimiento legal adecuado, debe seguir la normativa elaborada por el Estado miembro correspondiente.**

5.2 Licitud, lealtad y transparencia

Según el artículo 5.1 (a) del RGPD, "los datos personales se tratarán de forma lícita, leal y transparente en relación con el interesado". Este principio incluye tres requisitos diferentes.

- Licitud. El tratamiento de datos sólo es lícito si una base de legitimidad lo permite (véase el apartado 3.1). La mayor parte de la información que recoge un periodista son datos personales. Por tanto, la obtención de información supone a menudo un tratamiento de datos y, por lo tanto, debe seguir los principios establecidos por el RGPD. Esto significa que debe tener una base legal para procesar los datos y debe justificar las razones por las que los recoge.

- Lealtad. El concepto de lealtad es difícil de definir. Se refiere al hecho de que el tratamiento debe ser conforme al espíritu del RGPD, no solo a su letra. De este modo, permite introducir en la aplicación del RGPD las disposiciones de otras normativas de especial importancia a la hora de definir lo que se considera "justo" dentro de la UE y sus Estados miembros, como la Carta de Derechos Fundamentales de la UE. En general, se podría afirmar que la equidad implica que se procese la información de forma que se satisfagan las expectativas racionales de los interesados. La ICO ha declarado que la lealtad significa que "siempre que sea posible, los medios de comunicación deben recoger y utilizar la información sobre las personas de forma justa y legal, y no causar ningún daño injustificado". A menudo los periodistas podrán recoger información sin el conocimiento o el consentimiento del sujeto, pero será injusto engañar activamente a las personas sobre la identidad o las intenciones del periodista" (ICO, 40).

- Transparencia. El principio de transparencia pretende garantizar que todas las partes interesadas sean conscientes de cada tratamiento de sus datos personales y que puedan acceder a la información esencial sobre su contenido específico. En general, también debes decir a la persona de la que recoges la información, y a la persona sobre la que la información se refiere (es decir, el interesado), quién

eres y qué haces con su información. Si le proporcionan la información para un fin concreto, no debe utilizarla para otro fin. A veces, notificar a los interesados el tratamiento de los datos podría perjudicar la actividad periodística. A veces, se utilizan métodos encubiertos e intrusivos para conseguir un reportaje, como la vigilancia. Todas estas circunstancias pueden ser aceptables, siempre y cuando no haya otra alternativa más respetuosa con los principios de protección de datos y la noticia sea de interés público. De hecho, este es el punto clave: puede evitar notificar al interesado sobre el tratamiento si, y sólo en la medida en que haría imposible el ejercicio del periodismo. En otras palabras, debe comunicar el tratamiento a los interesados a menos que considere que al hacerlo no podría construir el reportaje. Una vez que esto ya no es aplicable, debe proceder con las obligaciones establecidas por el GDPR. Tal y como declaró la OIC, "en el contexto del periodismo, aceptamos que, por lo general, no será factible que los periodistas se pongan en contacto con todas las personas sobre las que recojan información. A menudo será justo recoger información sobre asuntos de potencial interés periodístico sin el conocimiento del sujeto. Sin embargo, habrá casos en los que la imparcialidad puede requerir algún contacto directo con el sujeto de una investigación importante, para ofrecerle la oportunidad de exponer su versión de la historia" (ICO, 40).

5.3 Elección de una base jurídica para el tratamiento

Hay tres bases legales para el tratamiento que suelen aplicarse al periodismo. Son el consentimiento, el interés público y el interés legítimo.

Consentimiento. Los datos pueden ser tratados si las personas que son objeto de la información han dado su consentimiento para ello. Si la información se refiere a varias personas, el consentimiento debe ser dado por todas ellas. El consentimiento debe ser libre, específico e informado. Hay que destacar que el mero hecho de que alguien haya publicado datos personales en un sitio público, como su perfil de Facebook, no significa que estos datos puedan ser utilizados sin su consentimiento u otra base legal. El consentimiento debe cubrir los fines del tratamiento de datos. Por lo tanto, si se quieren utilizar los datos para una finalidad distinta de la buscada originalmente por el

interesado, se necesita una base jurídica. Puede haber excepciones a esta regla, especialmente si el interesado es una figura pública, pero en tales circunstancias, debe tratar los datos sobre la base del interés legítimo, en lugar del consentimiento. Según las Directrices para la Protección de la Intimidad en los Medios de Comunicación, "los periodistas deben, en principio, obtener el consentimiento de la persona afectada en el momento de tomar la fotografía y no simplemente si se publica y cuando se publica. De lo contrario, un atributo esencial de la personalidad (la imagen) depende de terceros y la persona afectada no tiene control sobre ella" (p. 20).

Interés público. Los datos pueden ser tratados si son necesarios para el cumplimiento de una tarea realizada en interés público. De hecho, esta es la base jurídica más recomendable si usted forma parte de una institución pública que actúa como tal (si no se aplica el consentimiento). Si usted es un actor privado o si es una institución pública que trabaja como actor privado, la base del interés legítimo es más recomendable. Esto se debe a que el interés público no puede legitimar el tratamiento si no se tienen en cuenta los intereses del interesado, ya que la información no es un derecho o un deber absoluto. Sin embargo, si este es el caso, el interés legítimo y la prueba de equilibrio son conceptos que funcionan muy bien con el tratamiento. Por lo tanto, es recomendable utilizar el interés legítimo como base jurídica del tratamiento.

Interés legítimo. El tratamiento es necesario por "intereses legítimos", siempre que no cause un daño injustificado a la persona afectada. "Los intereses legítimos incluirán los intereses comerciales y periodísticos de un medio de comunicación en la recopilación y publicación de material, así como el interés público en la libertad de expresión y el derecho a saber". Por tanto, se trata de una base jurídica amplia que comprende el interés público, pero no sólo el interés público. Para equilibrar todos los intereses implicados, debe seguirse un procedimiento capaz de garantizar que el interés legítimo sirva de base legal de tratamiento incluye tres fases principales (Detrekői):

- en primer lugar, debe identificar una prueba de interés legítimo (por qué la historia sirve al interés público)
- en segundo lugar, debe realizar una prueba de necesidad (cómo la publicación de nombres y datos personales es necesaria para que el artículo sea informativo)

- Por último, hay que realizar una ponderación entre derechos, destinada a demostrar que el interés del público por conocer el tema tratado en la noticia supera el interés de la persona por mantener sus datos personales ocultos a la vista del público. Cuanto mayor sea el valor de la información para el público, más tiene que ceder el interés de la persona en ser protegida contra la publicación, y viceversa (Guidelines on Safeguarding Privacy in the Media, p.11).

En el Anexo I de este documento se incluye una amplia descripción de cómo realizar esa ponderación. La jurisprudencia del TEDH ha tratado profusamente el conflicto entre entre el interés público y la intimidad (véase Derecho a la protección de la propia imagen, en: https://www.echr.coe.int/documents/fs_own_image_eng.pdf). En el asunto Kaboğlu y Orán contra Turquía se incluyó un excelente resumen de su posición: "En varias de sus sentencias, el Tribunal ha resumido los criterios pertinentes para equilibrar el derecho al respeto de la vida privada y el derecho a la libertad de expresión de la siguiente manera: la contribución a un debate de interés público, la notoriedad de la persona en cuestión, el tema del informe, el comportamiento previo de la persona en cuestión, el contenido, la forma y las consecuencias de la publicación, así como, si procede, las circunstancias del caso (véase *Von Hannover* (nº 2) [GC], antes citada, §§ 108-113, y *Axel Springer AG*, antes citada, §§ 89-95; véase también *Couderc y Hachette Filipacchi Associés*, antes citada, § 93). Si los dos derechos en cuestión han sido ponderados de manera coherente con los criterios establecidos por la jurisprudencia del Tribunal de Justicia, éste respetará la opinión por la de los tribunales nacionales,

que plasma un justo equilibrio entre los derechos en juego (véase *Palomo Sánchez y otros c. España* [GC], nºs 28955/06, 28957/06, 28959/06 y 28964/06, § 57, TEDH 2011)".

5.4 Limitación de la finalidad

Los datos personales se recogerán con fines determinados, explícitos y legítimos, y no se tratarán de forma incompatible con dichos fines. En virtud de esto, los datos sólo pueden ser tratados para determinados fines, que deben ser explícitamente indicados al justificar el tratamiento. Por lo tanto, debe tener siempre presente, por ejemplo, que no puede utilizar los datos que conserva en sus registros para fines distintos de los que

justificaron su tratamiento, a menos que tenga una base que sirva de fundamento para el nuevo tratamiento.

5.5 Minimización de datos

Los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Este principio implica que "hay que tener suficiente información para hacer el trabajo, pero no hay que tener nada que no se necesite". Tenga en cuenta que este principio tiene en cuenta sus intereses, “como la naturaleza del periodismo requiere la recopilación y el cruce de grandes volúmenes de información, aceptamos que la información sin relevancia inmediata para una historia actual puede ser justificadamente retenida para su uso futuro si se refiere a una persona o tema de interés periodístico más general" (ICO, 25).

5.6 Precisión

Según el artículo 5.1 (d), "los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".

La exactitud es tanto un principio esencial del RGPD como un valor clave del periodismo. Por lo tanto, los periodistas deben prestar especial atención a que la información publicada sea exacta. Se puede argumentar que solo la información precisa funciona bien con la idea de promover el interés público. Por lo tanto, las exenciones y excepciones del artículo 85 sólo se aplicarán si la información es exacta. Sin embargo, “la exención puede estar disponible si, por ejemplo, la noticia es de interés público urgente y el corto plazo hace muy difícil una comprobación completa de la exactitud. Al igual que con cualquier uso de la exención, tendrá que demostrar que alguien de un nivel adecuado ha estudiado adecuadamente sobre las comprobaciones posibles, si la publicación pudiera retrasarse para realizar más comprobaciones, la naturaleza del interés público en juego y que la decisión de publicar fue, por tanto, razonable" (ICO, 14).

Además, la exactitud implica que deben tomarse medidas razonables para garantizar que los datos personales que sean inexactos se borren o rectifiquen sin demora. Esto es esencial, ya que la información publicada puede comprometer gravemente la imagen pública o la vida privada del interesado. Según el grupo de trabajo del artículo 29, "el derecho de réplica y la posibilidad de hacer rectificar las informaciones falsas, las obligaciones profesionales de los periodistas y los procedimientos especiales de autorregulación que les son propios, así como la ley de protección del honor (disposiciones penales y civiles relativas a la difamación) deben tenerse en cuenta al evaluar la protección de la vida privada en relación con los medios de comunicación" (A29WP, p. 7).

Por lo tanto, los periodistas deben ser especialmente cuidadosos y corregir la información si se demuestra que no refleja fielmente la realidad. Esto, por supuesto, debe considerarse especialmente si las personas que solicitan la rectificación son los interesados, de acuerdo con su derecho a la rectificación. Por último, hay que declarar siempre si se está expresando una opinión o informando sobre un hecho. Esto es crucial para que la audiencia no malinterprete la información.

5.6 Limitación del almacenamiento

El principio de limitación del almacenamiento obliga a que los datos sean "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales" (art. 5. 1 (e) del RGPD). En el contexto del periodismo, esto significa que, una vez que se dispone de información que contiene datos personales, es necesario tomar decisiones sobre si se quiere almacenar y en su caso, durante cuánto tiempo. Los datos son activos muy valiosos para el periodista, ya que a menudo pueden servir como material de base para su trabajo. Los datos de contacto también son un recurso muy importante y el periodista suele querer conservarlos. En principio, se pueden conservar estos datos durante largos periodos o indefinidamente. El RGPD no impone un límite de tiempo para conservar los datos personales. El principio de "limitación del almacenamiento" sólo impone que haya una buena razón para conservar los datos. Suponiendo que se de este requisito, pueden conservarse indefinidamente.

Sin embargo, tal y como afirma la ICO (ICO, 12), "debe revisar la información conservada de vez en cuando para asegurarse de que los datos siguen estando actualizados, son pertinentes y no son excesivos para sus necesidades, y debe eliminar cualquier dato que ya no necesite (por ejemplo, si un contacto ha cambiado de número). Además, la forma de conservar la información o de revisarla debe establecerse en las políticas de la organización.

5.7 Integridad y confidencialidad

Los datos deben ser "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, 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" (art. 5. 1 (f) del RGPD). Este principio tiene como objetivo evitar el tratamiento no autorizado o ilegal y la pérdida, destrucción o daño accidental de los datos.

Los datos que almacena son material sensible. Por lo tanto, debes hacer todo lo posible para evitar que se pierdan, sean robados o se utilicen de forma indebida. Intente mantenerlos a salvo prestando atención a los procedimientos y protocolos de seguridad establecidos por su organización. De hecho, todos los empleados de una empresa de comunicación deben conocer y seguir las políticas y procedimientos de la organización. La información debe estar bloqueada, protegida con contraseña y encriptada siempre que sea posible. Hay que ser especialmente consciente de la seguridad de los datos cuando se desplaze fuera de su lugar habitual de trabjo, portando documentos, teléfonos u ordenadores portátiles que contengan ficheros de datos personales.

En la normativa de protección de datos no se fije un nivel concreto de seguridad al que deben estar sometidos los datos perosnales. En principio, las medidas de seguridad adoptados deben ser adecuadas para garantizar que no se produzca ningún acceso ilegal o para evitar pérdidas, destrucciones o daños accidentales. Los periodistas deben tener en cuenta el grado de sensibilidad o confidencialidad de la información que poseen, el daño que podría ocasionar su pérdida o uso indebido, la tecnología disponible y los costes que conlleva a la hora de determinar qué medidas van a adoptar para proteger los datos. No es necesario que dispongan de una seguridad de última generación, pero sí

debe ajustarse al nivel de riesgo que implica el tratamiento. Las organizaciones deben tener en cuenta las medidas de seguridad técnicas (electrónicas) y físicas, las políticas y procedimientos, y la formación y supervisión del personal. Estas medidas deben abarcar al personal que trabaja tanto dentro como fuera de sus instalaciones. En cualquier caso, las organizaciones deben ser capaces de justificar el nivel de seguridad adoptado (ICO, 43).

5.8 Responsabilidad proactiva.

Según el artículo 5.2 del RGPD, "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo". El apartado primero enumera los principios ya tratados. Recae sobre el responsable cumplir estos principios y documentar las medidas implementadas que garantizan su cumplimiento. Hay que tener en cuenta que en el ámbito periodístico concurren excepciones que pueden limitar el alcance de estos principios y los derechos del interesado frente al responsable (art 85 RGPD). En estos casos, las organizaciones o los periodistas deben poder explicar por qué el cumplimiento de las disposiciones pertinentes no es compatible con los fines del periodismo. Para ello, deben demostrar que han realizado una prueba de equilibrio, considerando los diferentes intereses en juego. Hay que recalcar que el responsable no puede ampararse en prácticas generales del sector, que no tienen en cuenta los derechos del interesado para eludir la aplicación de la normativa de protección de datos. Mantener una pista de auditoría en los casos controvertidos o especialmente susceptibles de resultar polémicos podría ser una herramienta adecuada para demostrar la responsabilidad.

Como declaró Biriukova, "en primer lugar, la empresa de medios de comunicación, un periodista o, esencialmente, cualquier persona que quiera acogerse a la exención tendría que establecer el interés público de la publicación prevista y, en segundo lugar, comprender qué obligaciones de protección de datos entrarían, en ese caso, en conflicto con los fines periodísticos". Tal vez, cuando se trata de una investigación periodística sobre la corrupción gubernamental, una negativa a revelar la fuente de información podría defenderse fácilmente, sin embargo, otros escenarios menos claros (por ejemplo, la notificación de una brecha en la seguridad de los datos), pueden crear problemas de

interpretación. Por otro lado, es difícil concebir que un ciudadano que ejerce el periodismo como hobbie esté lo suficientemente bien formado para realizar a un justo equilibrio de los intereses en juego. A menos que se proporcionen orientaciones más detalladas, códigos de prácticas o de conducta, "un enfoque tan matizado corre el riesgo de permanecer en gran medida teórico y no operativo" (Biriukova, 22).

También hay que tener siempre presente que, en general, el responsable del tratamiento no es un periodista aislado, sino la organización en la que trabaja. Por lo tanto, la organización es responsable de aplicar medidas y políticas organizativas sobre el tratamiento de datos y la responsabilidad. De hecho, la organización debe poder demostrar que el tratamiento de los datos fue el resultado final de un proceso de toma de decisiones que tuvo en cuenta todos los intereses en juego. Los procedimientos pueden variar considerablemente, dependiendo del tipo de organización y de la información, pero debería haber un tipo de procedimiento estructurado en cada organización. Además, sería bueno desarrollar códigos de conducta en el marco de la profesión de periodista en cada Estado miembro. De hecho, el Grupo de Trabajo del Artículo 29 afirmó que "al evaluar si las exenciones o excepciones son proporcionadas, debe prestarse atención a las obligaciones éticas y profesionales existentes de los periodistas, así como a las formas de supervisión autorreguladoras que ofrece la profesión" (A29WP, p.8).

Como afirma el ICO, "en muchas historias cotidianas puede ser apropiado que el periodista utilice su propio juicio, pero las historias más destacadas, intrusivas o perjudiciales probablemente requieran una mayor implicación editorial y una consideración más formal del interés público". Las políticas de la organización deben servir para explicar cuándo es necesaria una mayor implicación de la redacción en la toma de decisiones. Nuestra opinión es que lo importante es la apreciación del interés público de la noticia en el momento del tratamiento. El responsable del tratamiento debe ser capaz de demostrar que creía que concurría un interés público en la noticia en el momento de la recogida y tratamiento de los datos de las personas afectadas. También debe poder demostrar que el interés público de la noticia se tuvo en cuenta en el momento del tratamiento de los datos personales en cuestión y no sólo a posteriori. Si un periodista considera inicialmente que una historia será de interés público, pero al

final la organización decide no publicarla, la exención puede seguir cubriendo todas las actividades periodísticas realizadas hasta ese momento.

En segundo lugar, la exención sólo requiere una creencia razonable de que concurre ese interés público en la noticia. De esta forma, se da más margen al periodista, en comparación con la aplicación de otras exenciones, lo cual refleja la importancia de unos medios de comunicación libres e independientes (ICO, 35). El siguiente cuadro muestra algunas medidas incluidas en las Directrices sobre la protección de la intimidad en los medios de comunicación que podrían servir a las organizaciones que tratan de garantizar el cumplimiento de la protección de datos.

6. Cuestiones adicionales

6.1 Solicitudes de acceso de los interesados

El acceso a la información almacenada por los periodistas puede ser muy importante, tanto para los sujetos a los que se refiere la información como para el público en general. Los primeros, sin embargo, tienen un derecho de acceso que no tienen los demás. El artículo 85, sin embargo, permite a los Estados miembros limitar ese derecho. En esta sección introduciremos algunas consideraciones sobre cómo suele formularse esta limitación. Para ello, nos centraremos tanto en el derecho de acceso como en el derecho a no revelar las fuentes de información, que están ampliamente reconocidos en diferentes Estados Miembros de la UE.

Según el artículo 15 del RGPD, el interesado tendrá derecho a obtener del responsable del tratamiento la confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, el acceso a los datos personales y a la información relativa a los fines del tratamiento, las categorías de datos de que se trata, los destinatarios o categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales, en particular los destinatarios de terceros países u organizaciones internacionales, el período previsto de conservación de los datos personales, etc.

Sobre esta base, el periodista debe facilitar a los interesados la información que posee sobre ellos, a menos que considere que, de hacerlo, no podría construir el reportaje. En

tales circunstancias, las excepciones y derogaciones del artículo 85 prevalecerían sobre su derecho de acceso. Ni que decir tiene que esto sólo ocurriría bajo el supuesto de que la historia sea de interés público. Cuanto mayor sea el interés, más fuerte será el derecho a no revelar la información al interesado. A menudo, puede ocurrir que usted pueda facilitar el acceso a parte de la información sobre el tratamiento o los datos personales utilizados sin que ello perjudique los objetivos de su investigación. Si este es el caso, debe proceder sin demora.

La negativa a facilitar la información solicitada podría estar perfectamente justificada incluso después de la publicación de la noticia. Si tiene razones de peso para considerar que puede ir en contra del interés público, si puede explicar por qué responder perjudicaría futuras investigaciones o publicaciones, o las actividades periodísticas en general, podría rechazar la solicitud. Pero siempre tendrá que dar una buena razón para oponerse a dicha solicitud. Por último, no olvide que no debe incluir ninguna información sobre otras personas a menos que éstas hayan dado su consentimiento, o que sea razonable suministrarla sin que eso sea necesario.

6.2 Fuentes confidenciales

Las fuentes de información son sagradas para los periodistas. Varios instrumentos internacionales garantizan su adecuada protección, entre ellos la Resolución sobre las libertades periodísticas y los derechos humanos, adoptada en la 4$^{a^{th}}$ Conferencia Ministerial Europea sobre Política de Medios de Comunicación (Praga, 7-8 de diciembre de 1994) y la Resolución sobre el secreto de las fuentes de los periodistas del Parlamento Europeo (18 de enero de 1994, Diario Oficial de las Comunidades Europeas nº C 44/34). Además, el Comité de Ministros del Consejo de Europa adoptó el 8 de marzo de 2000 la Recomendación nº R(2000) 7 sobre el derecho de los periodistas a no revelar sus fuentes de información. Además, en general, la legislación y la práctica nacionales de los Estados miembros prevén una protección explícita y clara del derecho de los periodistas a no revelar información que identifique a una fuente, de conformidad con el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

Por lo tanto, existe un marco legal que permite a los periodistas no revelar sus fuentes. Este derecho sólo puede limitarse en las condiciones mencionadas por el principio 3(b) de la Recomendación nº R(2000) 7, a saber:

> "i. no existen medidas alternativas razonables a la divulgación o han sido agotadas por las personas o autoridades públicas que solicitan la divulgación, y
>
> ii. el interés legítimo en la divulgación supera claramente el interés público en la no divulgación, teniendo en cuenta que:
>
> -se demuestre la necesidad de divulgación,
>
> -las circunstancias son de naturaleza suficientemente vital y grave,
>
> -se identifique la necesidad de la divulgación como respuesta a una necesidad social acuciante, y
>
> -Los Estados miembros gozan de un cierto margen de apreciación a la hora de evaluar esta necesidad, pero este margen va de la mano de la supervisión del Tribunal Europeo de Derechos Humanos.
>
> c.Los requisitos anteriores deben aplicarse en todas las fases de cualquier procedimiento en el que pueda invocarse el derecho de no divulgación".

Por último, no debemos olvidar que revelar una fuente también implica un tratamiento de datos, y que la fuente es también un sujeto de datos que tiene los derechos conferidos por el GDPR. Por lo tanto, si la fuente es un individuo, probablemente podrá preservar su identidad sobre la base del GDPR. De hecho, si el sujeto de una historia hace una solicitud de acceso del sujeto y esto sólo podría satisfacerse revelando la identidad de sus fuentes, sólo puede proceder si la fuente consiente, o si es razonable hacerlo, considerando todas las circunstancias. Si la fuente es una organización, las circunstancias cambian, ya que las personas jurídicas no están protegidas por el derecho a la protección de datos. Por lo tanto, los periodistas tienen que acogerse a la exención periodística para no revelar la identidad de la fuente si ésta no está dispuesta a revelar su nombre o si no es apropiado revelarlo.

6.3 Menores y población vulnerable

Debe tener especial cuidado si desea tratar datos relativos a menores o poblaciones vulnerables. En primer lugar, la base legal que considere para el tratamiento puede no ser la adecuada. El consentimiento de un menor sólo será válido si dicho menor puede prestarlo de acuerdo con el marco jurídico del Estado miembro. El RGPD establece una edad mínima, pero los Estados miembros están facultados para aumentarla. Por lo tanto, debe informarse al respecto, y acudir a la legislación de su Estado. Si el menor o la persona vulnerable no puede dar su consentimiento, sus representantes legales deberán prestarlo en su lugar.

Si no puede obtener un consentimiento informado, el tratamiento debe basarse en el interés legítimo. Sin embargo, el interés legítimo perseguido por el responsable del tratamiento no se aplica "cuando sobre dichos intereses prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de los datos personales, en particular cuando el interesado sea un menor". Por lo tanto, es muy improbable que la prueba de equilibrio permita el tratamiento de datos personales correspondientes a menores. En nuestra opinión, una reflexión similar es aplicable a las poblaciones vulnerables.

Las Directrices sobre la protección de la intimidad en los medios de comunicación incluyen un resumen de dos casos relacionados con menores.

- "En el caso Kahn contra Alemania, se publicaron en una revista las fotos de dos hijos de Oliver Kahn, antiguo portero de la selección alemana de fútbol, y de su esposa. Los periodistas fueron multados por haber violado el derecho a la intimidad de la familia. Todas las fotos mostraban a los niños en compañía de sus padres o de vacaciones, aunque el tema de los reportajes no eran los propios niños, sino la relación de sus padres y la carrera de Oliver Kahn.
- En el caso Reklos y Davourlis contra Grecia, la toma de fotografías de un recién nacido sin el consentimiento de sus padres (en la unidad de cuidados intensivos a la que sólo debía tener acceso el personal del hospital) se consideró una violación del derecho a la intimidad, aunque las fotografías no se publicaran".

Obsérvese que esta última frase es especialmente relevante, ya que se centra en la necesidad de contar con una base jurídica para el tratamiento de datos en el momento en que se realizan las fotografías. La decisión de no publicarlas sólo evita un tratamiento ilícito posterior (la publicación), pero no repara la infracción previa del derecho a la intimidad.

6.4 Puntos a tener en cuenta

Hay algunos consejos generales que pueden servir de resumen de los puntos clave sobre los que debe informarse en materia de protección de datos. En general, debe tener siempre presente que:

- La publicación de datos personales supone un tratamiento de datos. Por lo tanto, debe estar seguro de que se le permite mostrar estos datos antes de proceder a compartirlos. En ese momento debe disponer de una base legal que permita el tratamiento. De lo contrario, este será considerado ilegal.
- Si los datos personales se tratan para servir al interés público ("fines periodísticos"), es probable que el tratamiento no tenga que cumplir con algunos o todas las obligaciones que impone el RGPD. A la inversa, esto significa que, si los datos personales se recogen, analizan o procesan de otro modo por otros motivos, el RGPD se aplicará en su totalidad.
- La publicación de información sensible puede causar un daño considerable a la vida privada del interesado. Debe estar seguro de que los beneficios para el interés público justifican ese daño. Para ello, debe equilibrar los intereses en juego, considerando los diferentes niveles de intrusión en la vida privada del interesado. Sólo cuando las consideraciones de interés público prevalezcan claramente sobre la vida privada del interesado podrá usted publicar esa información.
- La intervención de la alta dirección editorial o las aportaciones de expertos pueden ser de gran ayuda para garantizar que se cumpla este requisito. No hay que olvidar que, por lo general, los periodistas interesados en que se publique la noticia no son tan objetivos a la hora de equilibrar los diferentes intereses en juego.

- Recuerde siempre que sólo debe recopilar datos que sean relevantes para su investigación y que puedan ser de interés público. Si, por ejemplo, está investigando a un político por una posible práctica de corrupción y descubre información sensible sobre su orientación sexual, no debe tratarla, siempre que no sea relevante para el asunto en cuestión. Este es un requisito esencial del principio de minimización, un concepto clave del RGPD.
- En los casos especialmente conflictivos, en los que no está del todo claro si la "exención periodística" se aplica al tratamiento de datos o en qué medida, debe mantenerse una pista de auditoría para explicar las consideraciones relativas a la protección de datos y debe solicitarse la consulta de la autoridad de control principal (Biriukova, p.30)
- Deben adoptarse precauciones especiales cuando se traten datos personales que revelen el origen racial o étnico, las opiniones políticas, la religión o las convicciones filosóficas, la afiliación sindical, así como el tratamiento de datos genéticos, datos relativos a la salud o datos relativos a la vida sexual o a las condenas e infracciones penales o medidas de seguridad relacionadas.
- Los datos relativos a la población vulnerable, y especialmente a los menores, sólo deben tratarse si existen razones de peso que lo justifiquen. Debe estar absolutamente seguro de que se aplican al tratamiento concreto antes de proceder.

7. Preguntas y respuestas

¿Qué ocurre con el uso secundario de los datos?

La respuesta a esta pregunta depende de algunas cuestiones clave. En primer lugar, si los datos se recogieron sobre la base de un interés legítimo, un contrato o intereses vitales, pueden utilizarse para otra finalidad, siempre que la nueva finalidad sea compatible con la original. Según el artículo 6.4 del RGPD, hay que tener en cuenta, entre otras cosas:

a. cualquier relación entre los fines para los que se han recogido los datos personales y los fines del tratamiento posterior previsto;

b. el contexto en el que se han recogido los datos personales, en particular en lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c. la naturaleza de los datos personales, en particular si se tratan categorías especiales de datos personales, de conformidad con el artículo 9, o si se tratan datos personales relacionados con condenas e infracciones penales, de conformidad con el artículo 10;
d. las posibles consecuencias del tratamiento posterior previsto para los interesados;
e. la existencia de garantías adecuadas, que pueden incluir el cifrado o la seudonimización.

Si se desea utilizar los datos para fines estadísticos o de investigación científica, no es necesario realizar la prueba de compatibilidad. Estos nuevos usos son compatibles con la finalidad original, según el artículo 5.2 (b) del RGPD.

Si se tratan los datos sobre la base del consentimiento de los interesados o a raíz de un requisito legal, no es posible un tratamiento posterior más allá de lo que cubre el consentimiento original o las disposiciones legales. Un tratamiento posterior requeriría la obtención de un nuevo consentimiento o una nueva base jurídica.

Me gustaría conseguir un enfoque sobre los temas involucrados en la comercialización de datos personales, una evaluación económica de la cantidad de este sistema de tráfico global

En principio, la comercialización de datos sólo es posible si no se trata de datos personales. En el caso de que un conjunto de datos mezcle ambos tipos de datos, se aplica el RGPD. Por lo tanto, la comercialización de datos no sería aceptable. Los datos personales están protegidos por los derechos. No son mercancías y no pueden comprarse ni venderse. Consulte la parte de las Directrices de PANELFIT dedicada a los conjuntos de datos y nuestro Análisis Crítico para obtener más datos.

Conservación/almacenamiento de datos, derecho al olvido

En general, los datos no deben conservarse más tiempo del estrictamente necesario para los fines que fueron recogidos. Si el responsable del tratamiento considera que

pueden ser útiles en el futuro, deberá justificar por qué. En cualquier caso, deben almacenarse de forma que se ajusten a los principios de minimización y limitación del almacenamiento. Por lo tanto, deben ser anónimos o, al menos, seudónimos siempre que sea posible.

El derecho al olvido está regulado por el artículo 17 del GDPR. Si se cumplen las condiciones establecidas en el artículo 17.1 del RGPD, el responsable del tratamiento "tendrá la obligación de suprimir los datos personales sin dilación indebida". No obstante, no se trata de un derecho absoluto. Las excepciones del artículo 17.3 del RGPD identifican los casos en los que no se aplica esta obligación. Una de estas condiciones es que el derecho "no se aplicará en la medida en que el tratamiento sea necesario (...) para el ejercicio del derecho a la libertad de expresión e información" (artículo 17.3 (a)). ¿Cómo se pueden equilibrar ambos derechos e intereses -derecho al borrado y derecho a la libertad de expresión e información-? Según explicó el TJUE en su sentencia Google 2, el artículo 17.3.a del RGPD es "una expresión del hecho de que el derecho a la protección de los datos personales no es un derecho absoluto, sino que (...) debe considerarse en relación con su función en la sociedad y equilibrarse con otros derechos fundamentales, de conformidad con el principio de proporcionalidad".[14] El Tribunal "establece expresamente la exigencia de equilibrio entre los derechos fundamentales a la intimidad y a la protección de los datos personales garantizados por los artículos 7 y 8 de la Carta, por una parte, y el derecho fundamental a la libertad de información garantizado por el artículo 11 de la Carta, por otra".[15] Por otro lado, el TEDH indicó en la sentencia "M.L. y W.W. contra Alemania" de 28 de junio de 2018, el que la ponderación de los intereses difícilmente podría resolverse a favor de una solicitud de borrado presentada contra el editor original cuya actividad está en el centro de lo que la libertad de expresión pretende proteger.[16] Así, en general, el derecho al olvido no se aplica si impide el ejercicio del derecho a la información.

Recogida de datos en investigaciones, almacenamiento de datos, tratamiento de datos de fuentes confidenciales

14 TJUE, asunto C-136/17, sentencia de 24 de septiembre de 2019, apartado 57.

15 TJUE, asunto C-136/17, sentencia de 24 de septiembre de 2019, apartado 59.

16 Tribunal Europeo de Derechos Humanos (TEDH), "M.L. y W.W. contra Alemania", 28 de junio de 2018.

El secreto profesional es un valor fundamental que no debe romperse en aras de la protección de datos. Lo más probable es que su Estado miembro haya adoptado normas específicas para establecer las facultades de las autoridades de control establecidas en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados del tratamiento que estén sujetos, en virtud del Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes cuando ello sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto (véase el artículo 90 del RGPD). No obstante, estas normas sólo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado de una actividad cubierta por la obligación de secreto o que hayan obtenido en ella.

Investigación forense con aprendizaje automático y resultados falsos de tales enfoques que afectan a los ciudadanos

Los periodistas deben comprobar cuidadosamente la exactitud de sus informaciones. Los datos inferidos son datos personales, ya que proporcionan información sobre una persona identificable. Se les aplican todos los derechos y deberes establecidos por el RGPD.

Herramientas específicas que pueden hacer más manejable el tratamiento de los datos

El manual para periodistas y las directrices de PANELFIT pueden ser muy útiles para estos fines.

El ciclo de vida del tratamiento de datos. Si puedes conservar los datos o, por ejemplo, las grabaciones de las entrevistas, ¿cuándo debes eliminarlos? Las mejores prácticas para separar lo que puede conservarse indefinidamente y lo que debe eliminarse, y sobre cómo tomarse el tiempo para eliminar realmente el material relevante de las ubicaciones de copia de seguridad después de un número x de años.

No hay nada parecido a una norma objetiva de tiempo de almacenamiento adecuado en el GDPR. Depende totalmente de si el almacenamiento tiene sentido o no. Si puede demostrar que el almacenamiento de esos datos es necesario para la finalidad del tratamiento, puede conservarlos indefinidamente. En cualquier caso, deben

almacenarse de una manera que funcione bien con los principios de minimización y limitación del almacenamiento. Así, deben ser anónimos o, al menos, seudónimos siempre que sea posible.

Normativa sobre información sanitaria

"Los datos personales que, por su naturaleza, son especialmente sensibles en relación con los derechos y libertades fundamentales merecen una protección específica, ya que el contexto de su tratamiento podría crear riesgos significativos para los derechos y libertades fundamentales" (considerando 51 del RGPD). Los datos relativos a la salud se consideran categorías especiales de datos personales. Según el artículo 9.1, no pueden tratarse a menos que se produzca una excepción que permita dicho tratamiento. Las excepciones se enumeran en el artículo 9.2.

Protección de imágenes

Las imágenes son datos personales. Por lo tanto, se necesita una base jurídica para tratar dichos datos. Si las imágenes corresponden a varias personas, la base jurídica debe aplicarse a todos los interesados. Por ejemplo, si la base de datos es el consentimiento, se debe contar con el consentimiento de todas las personas que aparecen en la fotografía o el vídeo. Por supuesto, el interés público puede ser una excelente base jurídica para permitir el tratamiento, pero debe equilibrar cuidadosamente los derechos, las libertades y el interés en juego. Por ejemplo, si puede evitar la identificación de las personas que no son esenciales para la información, debería hacerlo, especialmente si se trata de menores.

¿Cómo manejar los datos que están disponibles públicamente en un formato no estructurado con el propósito de compilar un nuevo conjunto de datos que podría conducir a información valiosa, pero también perjudicar a las personas vulnerables (por ejemplo, el raspado de datos personales [públicos] de un medio de comunicación social)?

En general, siempre hay que encontrar una base jurídica adecuada para el tratamiento de datos. Como se ha mencionado anteriormente, el interés legítimo es, en ausencia de consentimiento, el más adecuado. Si hablamos de la población vulnerable, esto debería

incluirse de forma destacada en la prueba de equilibrio. El tratamiento sólo sería lícito si el interés público es tan fuerte que supera el interés del interesado.

El scraping como tal no introduce novedades en esta regla básica. Aunque algunos datos sean públicos, esto no significa que puedas utilizarlos como quieras. En el caso de los datos que se expresan en una red social, también debe tener en cuenta que usted también es un usuario de esa red. Por lo tanto, las condiciones de servicio son aplicables a usted. En principio, esto no debería significar demasiado, pero debería tenerlo en cuenta.

Encontrará información detallada al respecto aquí:

Moreno Mancosu, Federico Vegetti, What You Can Scrape and *What Is Right to Scrape: Una propuesta de herramienta para recoger datos públicos de Facebook, Social media + Society*, Volumen: 6 número: 3, Artículo publicado por primera vez en línea: 31 de julio de 2020; Número publicado: 1 de julio de 2020, en: https://journals.sagepub.com/doi/full/10.1177/2056305120940703

Cómo comportarse cuando se quiere enviar un comunicado de prensa a la dirección de correo electrónico profesional de otro periodista (suponiendo que no se haya tenido ningún contacto previo). ¿Hay que pedir permiso de antemano (y cómo, si no es por correo electrónico) o hay que suponer que tienen interés en ser informados, por lo que se les envía el comunicado de prensa y se les da la posibilidad de excluirse? ¿Y qué pasa con los correos electrónicos de seguimiento?

En general, puedes enviar correos electrónicos a las direcciones profesionales de las personas, siempre que:

- tiene una buena razón para pensar que el destinatario puede beneficiarse de la información proporcionada por el comunicado de prensa.
- debe informar al destinatario de qué datos personales está tratando, con qué finalidad, y cómo puede eliminar sus datos de su lista de correo, o cambiarlos, en caso de que esta lista exista.

- Además, no debe procesar los datos personales de los destinatarios (almacenamiento, por ejemplo) durante más tiempo del necesario.

El envío de mensajes de seguimiento no infringe el GDPR si cumple los tres requisitos descritos en la respuesta anterior. El tratamiento de datos en caso de un mensaje de seguimiento debe seguir las mismas normas que un mensaje preliminar.

8. Glosario (art. 4 del GDPR)

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructu- ración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine

los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las caracte- rísticas físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un estableci- miento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:
a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
b) los interesados que residen en el Estado miembro de esa autoridad de control se

ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([1]);

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo

Anexo I. La prueba de equilibrio

Introducción: La prueba de equilibrio en el contexto del interés legítimo como base jurídica del tratamiento

El interés legítimo es una de las seis bases jurídicas para el tratamiento de datos personales que se recogen en el artículo 6, apartado 1, del RGPD. Esta base jurídica exige que los intereses legítimos del responsable del tratamiento o de los terceros a los que se comunican los datos prevalezcan sobre los intereses, los derechos fundamentales y las libertades de los interesados (artículo 6, apartado 1, letra f). Para comprobar que esto es así, los responsables del tratamiento pueden hacer uso de una herramienta denominada prueba de equilibrio, recomendada por el Grupo de Trabajo del Artículo 29, por ejemplo[17]. Esta herramienta tiene por objeto garantizar que los intereses legítimos del responsable del tratamiento o de los terceros a los que se comunican los datos prevalecen sobre los intereses y los derechos y libertades fundamentales de los interesados.

¿Cuándo no prevalecen los derechos y libertades fundamentales de la persona afectada por la protección de datos?

Llevar a cabo una prueba de equilibrio implica considerar varios factores clave que son decisivos para determinar qué intereses, libertades o derechos prevalecen, a saber[18]:

- la **naturaleza y el origen del interés legítimo**: si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, si es de interés público o si goza de reconocimiento en la comunidad. Es obligatorio evaluar el posible perjuicio sufrido por el responsable del tratamiento, por terceros o por la comunidad en general si el tratamiento de datos no se lleva a cabo.

17 A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p.24. En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consultado el 05 de enero de 2020

18 A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p.24. En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consultado el 5 de enero de 2020.

- El **poder y el estatus de las dos partes** (responsable del tratamiento o tercero y sujeto de los datos). Por ejemplo, un empresario que pretende tratar los datos de un empleado está en una posición más fuerte que el empleado. Si el sujeto de los datos es un menor de edad, sus intereses, derechos o libertades deben tener mayor peso.
- La **naturaleza de los datos**. Los datos de categorías especiales, por ejemplo, deben tener mayor peso. Del mismo modo, deben ponderarse adecuadamente los datos que la gente pueda considerar especialmente "privados" (por ejemplo, los datos financieros), los datos de los niños o los datos relativos a otras personas vulnerables.

- El **impacto del tratamiento en los interesados**. Para ello, los responsables del tratamiento deben considerar si el tratamiento puede suponer un alto riesgo para los derechos y libertades de las personas. Si este es el caso, deben realizar una evaluación de impacto previa.
- Las **expectativas razonables de** los interesados sobre lo que ocurrirá con sus datos. Los responsables del tratamiento deben poder demostrar que una persona razonable esperaría que pudiera darse el tratamiento de sus datos a la luz de las circunstancias particulares aplicables. Si la finalidad y el método de tratamiento no son inmediatamente obvios y existe la posibilidad de que la gente no haya anticipado que sus datos vayan a ser tratados los responsables del tratamiento podrían llevar a cabo algún tipo de consulta, grupo de discusión o estudio de mercado con las personas para demostrar las expectativas y apoyar su posición. Si existen estudios previos sobre las expectativas razonables en un contexto concreto, los responsables del tratamiento pueden basarse en ellos para determinar lo que los individuos pueden o no esperar[19].

- La **forma en que se procesan los datos** (a gran escala, extracción de datos, elaboración de perfiles, divulgación a un gran número de personas o publicación);

19 ICO, ¿Cómo aplicamos los intereses legítimos en la práctica? En: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Consultado: 15 de enero de 2020

- Las **salvaguardias adicionales** que podrían limitar el impacto indebido sobre el interesado, como la minimización de los datos (por ejemplo medidas técnicas y organizativas para garantizar que los datos no puedan utilizarse para tomar decisiones u otras acciones con respecto a las personas ("separación funcional") - amplio uso de técnicas de anonimización, agregación de datos, tecnologías que mejoran la privacidad, privacidad por diseño, evaluaciones de impacto sobre la privacidad y la protección de datos; mayor transparencia, derecho general e incondicional a oponerse (opt-out), portabilidad de datos y medidas relacionadas para empoderar a los interesados, etc.

La cuestión de las salvaguardias adicionales

El Grupo de Trabajo del Artículo 29 considera que las medidas de mitigación y las salvaguardias, como las medidas organizativas o técnicas adoptadas por el responsable del tratamiento para la protección de los derechos del interesado, deben incluirse en la prueba de equilibrio. Sin embargo, existe un enfoque alternativo, que considera que el artículo 6.1.f) pide una prueba de equilibrio entre dos valores, los intereses legítimos del responsable del tratamiento (o de un tercero) y los intereses, derechos y libertades del interesado. Las medidas paliativas y las salvaguardias no se ajustan a ninguno de estos valores. Por lo tanto, no deben considerarse. De lo contrario, tendrían más peso que la parte de los responsables del tratamiento, ya que socavarían la importancia del posible daño que se causaría a los intereses, derechos y libertades del interesado. Kamara y De Hert han hecho algunas declaraciones convincentes sobre esta cuestión concreta, al afirmar que[20]

> *"la inclusión de medidas de mitigación en la evaluación llevaría a una representación del impacto real previsto del tratamiento para los derechos de los interesados, y seguiría permitiendo que prevalecieran los intereses legítimos. Este enfoque no "castiga" al responsable del tratamiento que adopta medidas de mitigación y salvaguardias, al no incluirlas en la prueba de sopesamiento. Por el contrario, anima al responsable del tratamiento a hacerlo. Por otra parte, hay que tener en cuenta que el peso de las futuras salvaguardias y medidas de mitigación es*

20 Kamara, Irene y De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. En: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Consultado: 17 de enero de 2020

siempre relevante para su realización y eficacia. Por lo tanto, dichas medidas deben tenerse en cuenta, pero no deben desempeñar un papel significativo a la hora de determinar hacia qué lado se inclina la balanza."

Algunos ejemplos de pruebas de equilibrio

Ejemplo 1[21]

Caso: El periódico Z se plantea la publicación de unas fotografías en las que aparece X, un actor, tras ser detenido por posesión de cocaína en un desfile público. X es un personaje público famoso en su país, ya que interpreta a un policía en una serie de televisión. Además, ha concedido varias entrevistas aportando datos sobre su vida privada públicamente.

Prueba de equilibrio: los datos se refieren a la vida privada del individuo más que a la vida profesional. Compartir los datos podría contribuir a causar un daño significativo a la persona. Sin embargo, existe un interés público en compartir esta información. La expectativa del actor de que su privacidad será efectivamente protegida se ha visto reducida por el hecho de que ha revelado datos de su vida privada en varias entrevistas. El resultado para la empresa tras considerar todos los factores relevantes debe ser que los intereses del famoso actor no superan sus intereses legítimos en la publicación de las fotografías, y el tratamiento es legal sobre la base de estos intereses legítimos.

Ver: Axel Springer AG contra Alemania

Ejemplo 2[22]

Caso: Un empresario controla el uso de Internet durante el horario laboral de sus empleados para comprobar que no hacen un uso personal excesivo de los ordenadores de la empresa. Los datos recogidos incluyen los archivos temporales y las cookies generadas en los ordenadores de los empleados, que muestran los sitios web visitados y las descargas realizadas durante las horas de trabajo. Los datos se tratan sin consultar previamente a los interesados y a los

21 Fuente: A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p.63. En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consultado el 05 de enero de 2020

22 Fuente: ICO. ¿Cómo se aplican los intereses legítimos en la práctica? En: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Consultado: 15 de enero de 2020

representantes sindicales/comité de empresa. Tampoco se proporciona suficiente información a los interesados sobre estas prácticas.

Prueba de equilibrio: La cantidad y la naturaleza de los datos recogidos constituyen una intrusión significativa en la vida privada de los empleados. Además de las cuestiones de proporcionalidad, la transparencia sobre las prácticas, estrechamente vinculada a las expectativas razonables de los interesados, es también un factor importante que debe considerarse. Incluso si el empresario tiene un interés legítimo en limitar el tiempo que los empleados pasan visitando sitios web que no son directamente relevantes para su trabajo, los métodos utilizados no cumplen la prueba de equilibrio del artículo 7(f). El empresario debe utilizar métodos menos intrusivos (por ejemplo, limitar la accesibilidad a determinados sitios), que, como mejor práctica, se discutan y acuerden con los representantes de los trabajadores, y se comuniquen a éstos de forma transparente.

Lo que hay que hacer y lo que no hay que hacer

DOs

- Comprobar la naturaleza de los datos tratados y prestar especial atención a la protección de los intereses, derechos y libertades de los niños si están en juego
- Considerar las expectativas razonables de los interesados
- Realizar una evaluación de impacto si las circunstancias lo recomiendan

Lo que no hay que hacer

- No trate los datos de los niños si no es absolutamente necesario para alcanzar el interés perseguido
- No procesar los datos si el resultado de la prueba de equilibrio no es claramente favorable
- No dude en introducir las garantías adecuadas para minimizar el perjuicio a los intereses, derechos y libertades de los interesados

Lista de comprobación

- Los responsables del tratamiento se han asegurado de que los intereses de la persona no prevalecen sobre los intereses legítimos del responsable del tratamiento o de terceros.
- Los responsables del tratamiento utilizan los datos de las personas de la forma que razonablemente se espera.
- Los responsables del tratamiento no utilizan los datos de las personas de forma muy intrusiva o que pueda causarles daño, a menos que tengan una razón especialmente buena.
- Los responsables del tratamiento no procesan datos de niños o, si lo hacen, han tomado precauciones adicionales para asegurarse de proteger sus intereses.
- Los controladores han estudiado las salvaguardias para reducir el impacto en la medida de lo posible.
- Los controladores han considerado si necesitan realizar una DPIA.

Otras lecturas

- El Grupo de Trabajo del Artículo 29 proporcionó ejemplos adicionales de pruebas de equilibrio, que pueden encontrarse en su Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE

- A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p. 24. En: https: //ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
- SEPD, Evaluación de la necesidad de medidas que limiten el derecho fundamental a la protección de datos personales: A Toolkit, 11 de abril de 2017, en: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Consultado el 5 de mayo de 2020
- ICO, ¿Cómo aplicamos los intereses legítimos en la práctica? En: https: //ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/
- ICO, ¿Qué es la base de los "intereses legítimos"? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Consultado el 5 de mayo de 2020.

- Kamara, Irene y De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. En: https: //brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Anexo II. Análisis comparativo del marco normativo en los Estados miembros de la UE

La fuente principal de la información recopilada es el análisis comparativo de Bird&Bird, salvo que se indique lo contrario.

Austria

Revisado por última vez: 05.06.2018

El artículo 9 de la ADPA establece disposiciones especiales relativas al tratamiento de datos personales en el contexto de la libertad de expresión e información. Según estas disposiciones, varias normas del RGPD (especialmente sus principios y derechos de los interesados) no se aplican al tratamiento de datos personales con fines periodísticos, así como con fines científicos, artísticos o literarios.

Bélgica

Revisado por última vez: 13.09.2018

El artículo 16 de la DPA permite el tratamiento de datos personales con medios adecuados para fines periodísticos o de expresión académica, artística o literaria. Los artículos 17 y siguientes estipulan las excepciones a las obligaciones de información (artículo 17), la protección de la fuente y el contenido de la información (artículo 18), las excepciones al derecho de restricción del tratamiento (artículo 19), la información sobre rectificación y supresión (artículo 20) y la limitación del derecho de oposición (artículo 21).

Finlandia

Revisado por última vez: 13.11.2018

Según el artículo 27 de la Ley de Protección de Datos, sólo se aplican disposiciones limitadas del RGPD al tratamiento de datos personales con fines periodísticos o de

expresión académica, artística o literaria. Este enfoque mantiene la situación tal y como estaba bajo la derogada Ley de Datos Personales.

Francia

Revisado por última vez: 11.02.2019

Según el marco normativo francés, cuando los datos personales se tratan con fines periodísticos, artísticos o de expresión literaria, no se aplican las disposiciones relativas a la notificación de información, la transferencia de datos, los derechos del interesado, la conservación y el tratamiento de categorías especiales de datos.

Alemania

Revisado por última vez: 23.05.2018

§ El artículo 35 de la nueva Ley Federal de Protección de Datos ("FDPA") exime al responsable del tratamiento de la obligación de suprimir los datos personales cuando, en caso de tratamiento no automático de datos, la supresión sea imposible o sólo posible con un esfuerzo desproporcionado y el interesado tenga un interés menor en la supresión. § El artículo 27(2) de la FDPA restringe los derechos de los interesados a condición de que se cumplan otros requisitos.

Irlanda

Revisado por última vez: 07.06.2018

En virtud del artículo 43.1 de la Ley, el tratamiento de datos personales con el fin de ejercer el derecho a la libertad de expresión e información, incluido el tratamiento con fines periodísticos o de expresión académica, artística o literaria, estará exento del cumplimiento de determinadas disposiciones del RGPD cuando, habida cuenta de la importancia del derecho a la libertad de expresión e información en una sociedad democrática, el cumplimiento de dichas disposiciones sea incompatible con tales fines. La Comisión de Protección de Datos podrá remitir cualquier cuestión de derecho que

implique el examen de si el tratamiento de datos personales está exento en virtud del artículo 43, apartado 1, al Tribunal Superior para que éste resuelva.

Italia.

Revisado por última vez: 25.10.2018

Título XII de la IDPA - secciones 136-137-138-139. El código de prácticas sobre el tratamiento de datos personales y actividades periodísticas (anexo A.1 de la IDPA) sigue en vigor. La compatibilidad de este código con el GDPR será reevaluada por la Autoridad Italiana de Protección de Datos (en adelante, la "Autoridad"). La Autoridad deberá revisarlo antes de que finalice el calendario. Además, Italia incorporó algunos principios relativos a la exención periodística mediante un código deontológico, a saber

a) la exigencia de evitar cualquier tipo de censura previa

b) la exención del derecho de información en la recogida de datos cuando el ejercicio profesional lo requiera

c) el deber del periodista de rectificar sin demora los errores e inexactitudes

d) la necesidad de ser especialmente cuidadoso cuando el tratamiento afecte a datos especialmente protegidos. En estas circunstancias, el tratamiento se limitará a los hechos de indiscutible interés público. Además, se limitará a los aspectos esenciales de la información y evitará las referencias a personas no relacionadas con ellos. Incluso en el caso de asuntos que el interesado haya hecho públicos, o que se aprecien en la conducta pública, se reserva el derecho a ser protegido

e) se sugiere que se busque la "esencialidad" de la información, la proporcionalidad de lo que se hace público, para que se limite a lo esencial en relación con el caso

f) cuando se refiera a una noticia relacionada con la salud, se respetará la dignidad, el decoro y la vida privada del afectado, especialmente cuando se trate de enfermedades graves o terminales, absteniéndose de publicar datos analíticos o de interés estrictamente clínico. No obstante, podrá hacerse una excepción a esta exigencia cuando, de acuerdo con el principio de proporcionalidad, la persona afectada se

encuentre en una posición de especial relevancia pública. Lo mismo se aplica a la información sobre la vida sexual.

Países Bajos

Revisado por última vez: 17.09.2018

El artículo 41 de la Ley de Ejecución del RGPD establece que la orden de ejecución del RGPD no se aplica cuando los datos personales se procesan exclusivamente con fines periodísticos o con fines de expresión académica, artística o literaria. Además, resume una lista de capítulos y artículos del RGPD que tampoco son aplicables para estos fines: (a) el artículo 7, apartado 3, y el artículo 11, apartado 2; b) el capítulo III; c) el capítulo IV (con excepción de los artículos 24, 25, 28, 29 y 32); d) el capítulo V; e) el capítulo VI; y f) el capítulo VII. "El artículo 41 de la Ley de protección de datos limita el alcance de determinadas obligaciones en relación con los intereses generales (imperativos) en consonancia con el artículo 23 del RGPD. Por lo tanto, prevé excepciones a los derechos del interesado y a las obligaciones del responsable del tratamiento. El RGPD parcialmente (art. 12-21 y 34 RGPD) no se aplica (en la medida en que sea apropiado y proporcionado) al tratamiento de datos en vista de -entre otras cosas- importantes objetivos de interés público, la seguridad pública, la protección del sujeto de los datos o de los derechos y libertades de otros; y/o el cobro de reclamaciones civiles.

España

Revisado por última vez: 05.03.2019

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales no incluye ningún precepto legal que concilie la libertad de expresión con la protección de datos. Sólo hay una referencia a la libertad de expresión en el artículo 85 sobre el derecho a la libertad de expresión en Internet que tiene toda persona.

Suecia

Revisado por última vez: 06.09.2018

Párrafo 1:7 de la Ley de Protección de Datos: el RGPD y la Ley de Protección de Datos no se aplicarán en la medida en que infrinjan las leyes sobre libertad de expresión. La Ley de Protección de Datos establece que los artículos 5-30 y 35-50 del RGPD no serán aplicables al tratamiento de datos personales con fines periodísticos o de expresión académica, artística o literaria.

Reino Unido

Revisado por última vez: 23.05.2018

La Ley de Protección de Datos del Reino Unido de 2018 [23]ofrece una toma más matizada sobre los límites de la exención, sugiriendo que algunas de las disposiciones del GDPR no se aplicarían al procesamiento de datos cuando se cumplan tres condiciones acumulativas (Cain, 2018):

- los datos en cuestión deben ser tratados con vistas a la publicación de material periodístico,
- el responsable del tratamiento debe creer razonablemente que, teniendo en cuenta en particular la especial importancia del interés público en la libertad de expresión, la publicación sería de interés público, y
- el responsable del tratamiento debe creer razonablemente que la aplicación de la disposición del RGPD enumerada sería incompatible con su finalidad periodística.

El ICO del Reino Unido aconseja considerar la segunda condición -el "interés público"- caso por caso, teniendo en cuenta los códigos de conducta existentes y sopesando el interés público del asunto con el nivel de intrusión en la vida privada de un individuo. No es sorprendente ver el "interés público" incluido como uno de los criterios, ya que ocupa un lugar destacado en la jurisprudencia del TEDH. Aunque el TEDH se abstuvo de dar una definición del "interés público", reconoció que esta noción abarca el debate público, político e histórico, las cuestiones relacionadas con los políticos, el comportamiento de los funcionarios públicos, las grandes empresas, los gobiernos y los

23 Vid. Ley de Protección de Datos del Reino Unido de 2018, Anexo 2, Parte 5, par. 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

asuntos relacionados con la delincuencia. Sin embargo, también puede considerarse que otros asuntos menos aparentes responden al interés público o general (Bitiukowa, 21).

Información relacionada con las exenciones y excepciones en pocas palabras

El siguiente cuadro (Bitiukowa, 25) incluye una comparación actualizada entre varios Estados miembros de la UE en cuanto a la regulación de las excepciones.

TABLE 3

The scope of the "Journalistic exemption" under the national law of the selected Member States

GDPR Article	Explanation of the Article	Sweden	United Kingdom	Lithuania	Romania
Article 5(1)(f)	Principle of integrity and confidentiality, which means that a data controller (e.g., a media undertaking) must put in place technical and organizational measures to ensure that the personal data it processes is protection from unauthorized disclosure, accidental loss, damage,etc.	Partially exempted[94] ***	Not exempted**	Not exempted	Exempted
Article 6	Lawfulness of processing, which means that each processing operation can only be considered lawful if a data controller can identify a lawful basis for it (consent, contract, public interest, etc.).	Exempted*	Exempted	Not exempted	Exempted
Articles 12-23	Rights of data subjects, meaning that the data controller should provide individuals with information about processing and respond to their requests.	Exempted	Partially exempted[95]	Exempted	Exempted
Article 28	Processor, which means that where a media undertaking outsources data processing to another entity (e.g., a data centre or a data analytics company), they must have a data processing agreement in place with it.	Exempted	Not exempted	Not exempted	Exempted

* **Not exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply with the rule** the content of which is explained in the second column.

** **Exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **does not have to comply with the rule** the content of which is explained in the second column.

*** **Partially exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply only with the certain aspects of the rule** the content of which is explained in the second column and in the relevant footnote.

Fuentes de información

Bibliografía

Grupo de Trabajo del Artículo 29, RECOMENDACIÓN 1/97 La ley de protección de datos y los medios de comunicación. Adoptada por el Grupo de Trabajo el 25 de febrero de 1997, en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf. Última visita: 17/10/2020.

BIRD & BIRD, Datos personales y libertad de expresión, En: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression. Última visita: 17/10/2020.

BENEZIC, Dollores, Rumanía podría estar utilizando el GDPR para intimidar a los periodistas, Liberties, 2018, En: https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384. Última visita: 17/10/2020.

BITIUKOVA, Natalija, Journalistic exemption under the european data protection law, Vilnius Institute for Policy Analysis, 2020, en: https://vilniusinstitute.lt/wp-content/uploads/2020/01/VIPA_Bitiukova_2020_v4_f.pdf. Última visita: 17/10/2020.

CAIN N. y COWPER-COLES, R., GDPR and the Data Protection Act 2018 - how do they impact publishers?, 25 de mayo de 2018, https://www.lexology.com/library/detail.aspx?g=b26433e1-0548-4a9d-8351-f720e737f811. Última visita: 17/10/2020.

CULLAGH K. et al, Adaptaciones nacionales del GDPR, Luxemburgo: Blogdroiteuropéen, 17 de febrero de 2019, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf. Última visita: 17/10/2020.

DETREKŐI, Zsuzsa, GDPR in Hungary: A Road to Hell?, En: https://medium.com/center-for-media-data-and-society/gdpr-in-hungary-a-road-to-hell-3b60718a0281. Última visita: 17/10/2020.

DRECHSLER L., El GDPR y el periodismo. ¿Protección de la privacidad o ruptura de la responsabilidad democrática?, 18 de septiembre de 2018, https:// brusselsprivacyhub.eu/publications/ws21.html. Última visita: 17/10/2020.

TEDH, Guía sobre el artículo 8 del Convenio Europeo de Derechos Humanos, agosto de 2020, en: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Última visita: 17/10/2020.

EDRI, Proceda con precaución, en: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf. Última visita: 17/10/2020.

NIELSEN, Nikolaj. La UE advierte a Rumanía de que no debe abusar del RGPD contra la prensa, EU Observer (12 de noviembre de 2018).

REVENTLOW, Nani Jansen, Simposio sobre el GDPR y el derecho internacional. ¿Pueden coexistir el GDPR y la libertad de expresión? En: https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist. Última visita: 17/10/2020.

Oficina del Comisario de Información del Reino Unido, Data protection and journalism: a guide for the Media, 2014, en: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf. Última visita: 17/10/2020.

WARNER, Bernhard, Online-Privacy Laws Come With a Downside, The Atlantic, 2019, en: https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/. Última visita: 17/10/2020.

Documentos del Consejo de Europa

Convenio para la protección de las personas físicas en lo que respecta al tratamiento de datos personales

Recomendación CM/Rec(2018)1 del Comité de Ministros a los Estados miembros sobre el pluralismo de los medios de comunicación y la transparencia de su propiedad

Recomendación CM/Rec(2016)4 del Comité de Ministros a los Estados miembros sobre la protección del periodismo y la seguridad de los periodistas y otros actores de los medios de comunicación

Recomendación CM/Rec(2011)7 del Comité de Ministros a los Estados miembros sobre una nueva noción de medios de comunicación

Declaración del Comité de Ministros sobre la protección y el fomento del periodismo de investigación (26 de septiembre de 2007)

Resolución 2066 (2015), Responsabilidad y ética de los medios de comunicación en un entorno mediático cambiante, Asamblea Parlamentaria

Resolución 1843 (2011), La protección de la privacidad y los datos personales en Internet y los medios de comunicación en línea, Asamblea Parlamentaria

Resolución 1165 (1998), Derecho a la intimidad, Asamblea Parlamentaria

Resolución 1003 (1993), Ética del Periodismo, Asamblea Parlamentaria

Jurisprudencia del Tribunal Europeo de Derechos Humanos

- A c. Noruega, nº 28070/06, 9 de abril de 2009
- Ageyev c. Rusia, nº 7075/10, 18 de abril de 2013
- Alkaya c. Turquía, nº 42811/06, 9 de octubre de 2012
- Armonienė contra Lituania, nº 36919/02, 25 de noviembre de 2008
- Axel Springer Ag v. Germany [GC], No. 39954/08, 7 de febrero de 2012
- Bédat c. Suiza [GC], núm. 56925/08, 29 de marzo de 2016
- Biriuk c. Lituania, nº 23373/03, 25 de noviembre de 2008 Björk Eiðsdóttir c. Islandia, nº 46443/09, 10 de julio de 2012
- Bladet Tromsø y Stensaas contra Noruega, nº 21980/93, 20 de mayo de 1999
- Bodrožić c. Serbia, nº 32550/05, 23 de junio de 2009 Bohlen c. Alemania nº 53495/09 y Ernst August von Hannover c. Alemania nº 53649/09, 19 de febrero de 2015
- Couderc y Hachette Filipacchi Associés c. Francia [GC], nº 40454/07, 10 de noviembre de 2015

- Dorothea Sihler-Jauch contra Alemania y Günther Jauch contra Alemania, números 68273/10 y 34194/11, 24 de mayo de 2016 (decisión)
- Egeland y Hanseid v. Noruega, No. 34438/04, 15 de abril de 2009
- Erla Hlynsdóttir (nº 2), nº 54125/10, 21 de octubre de 2014
- Feldek c. Eslovaquia, nº 29032/95, 12 de julio de 2001 Flinkkilä y otros c. Finlandia, nº 25576/04, 6 de abril de 2010
- Fürst-Pfeifer c. Austria, números 33677/10 y 52340/10, 17 de mayo de 2016
- Guseva c. Bulgaria, nº 6987/07, 17 de febrero de 2015
- Hachette Filipacchi Associés contra Francia, nº 71111/01, 14 de junio de 2007
- Hachette Filipacchi Associés c. Francia [GC], nº 40454/07, 10 de noviembre de 2015
- Hachette Filipacchi Associés ("Ici Paris") contra Francia, nº 12268/03, 23 de julio de 2009
- Haldimann y otros c. Suiza, nº 21830/09, 24 de febrero de 2015
- Janowski c. Polonia, nº 25716/94, 21 de enero de 1999
- Khan c. Alemania, núm. 38030/12, 21 de septiembre de 2016
- Khmel c. Rusia, nº 20383/04, 12 de diciembre de 2012
- Khuzhin y otros c. Rusia, nº 13470/02, 23 de octubre de 2008
- Krone Verlag GmbH & Co. KG v. Austria, No. 34315/96, 26 de febrero de 2002
- Krone Verlag GmbH & Co KG y Krone Multimedia GmbH & Co KG c. Austria, nº 33497/07, 17 de enero de 2012
- Leempoel & S.A. ED. Ciné Revue c. Bélgica, nº 64772/01, 9 de noviembre de 2006
- Lillo-Stenberg y Sæther c. Noruega, nº 13258/09, 16 de enero de 2014 Mitkus c. Letonia, nº 7259/03, 2 de octubre de 2012
- MGN Limited contra el Reino Unido, nº 39401/04, 18 de enero de 2011
- Mosley contra el Reino Unido, nº 48009/08, 10 de mayo de 2011
- Müller v. Germany (Dec.), No. 43829/07, 14 de septiembre de 2010
- Österreichischer Rundfunk v. Austria, No. 35841/02, 7 de diciembre de 2006 Directrices sobre la protección de la intimidad en los medios de comunicación 38
- Peck. V. Reino Unido, nº 44647/98, 28 de enero de 2003 Pentikäinen v. Finlandia [GC], nº 11882/10, 20 de octubre de 2015 Reklos y Davourlis v. Grecia, nº 1234/05, 15 de enero de 2009 Renaud v. Francia, nº 13290/07, 25 de febrero de 2010

- Salihu y otros c. Suecia, nº 33628/15, 10 de mayo de 2016 (decisión)
- Schweizerische Radio- und Fernsehgesellschaft SRG c. Suiza, nº 34124/06, 21 de junio de 2012
- Selistö c. Finlandia, nº 56767/00, 16 de noviembre de 2004
- Standard Verlags GmbH v. Austria (No.2), No. 21277/05, 4 de junio de 2009
- Standard Verlags GmbH c. Austria (nº 3), nº 34702/07, 10 de enero de 2012
- Toma c. Rumanía, nº 42716/02, 24 de febrero de 2009
- Verlagsgruppe News GmbH c. Austria, nº 10520/02, 14 de diciembre de 2006
- Von Hannover c. Alemania, nº 59320/00, 24 de junio de 2004
- Von Hannover v. Germany (No.2) [GC], Nos. 40660/08 y 60641/08, 7 de febrero de 2012
- White v. Sweden, No. 42435/02, 19 de septiembre de 2006
- Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH contra Austria (nº 2), nº 62746/00, 14 de noviembre de 2002 (decisión)
- Y c. Suiza, No. 22998/13, 06 de junio de 2017
- Zvagulis c. Lituania, nº 8619/09, 26 de enero de 2017 (decisión)