REDES

Revista Eletrônica Direito e Sociedade

Canoas, v. 8, n. 3, 2020

Artigo

Recebido: 05.05.2018

Aprovado: 29.07.2020

Publicado: 30.07.2020

DOI http://dx.doi.org/10.18316/REDES.v8i3.6907

Privacidad y consentimiento en el entorno digital: aproximación desde la perspectiva de la Unión Europea[1]

Maria Natalia Mato Pacín

Universidad Carlos III, Madrid, Espanha

https://orcid.org/0000-0003-4194-8802

Resumen: En el marco de la protección de datos personales en el entorno digital de la Unión Europea, el objetivo de este trabajo es exponer las bases legales para el tratamiento de los datos personales, en especial, el consentimiento. Respecto de éste, se apuntarán algunas controversias que han surgido en torno a su aplicación en Internet (¿cómo cumplir con los requisitos en la práctica? ¿datos personales como "contraprestación" en contratos digitales?) y se pondrá de relieve la tendencia a la protección de datos personales desde el diseño y por defecto, como mecanismo para una mayor garantía de seguridad.

Palabras-clave: Protección de Datos Personales; E-privacidad; Unión Europea; Consentimiento; Licitud del Tratamiento; Privacidad Desde el Diseño y por Defecto.

Privacy and consent in the digital environment: approach from a European Union perspective

Abstract: Within the framework of the European Union personal data protection in the digital environment, the objective of this paper is to expose the legal bases of the personal data processing, focusing on consent. Regarding the latter, on the one hand, some controversies that have arisen linked to its application on the Internet will be pointed out (how to comply with the requirements in practice? Personal data as "counter-parter" in digital contracts?). On the other hand, the paper provides a quick overview about the trend towards personal data protection by design and by default, as a mechanism for a greater guarantee of security.

Key-words: Personal Data Protection; E-privacy; European Union; Consent; Lawfulness of Processing; Privacy by Design and by Default.

Introducción: Desarrollo tecnológico y datos personales

Uno de los muchos ámbitos en los que ha tenido un evidente impacto el desarrollo tecnológico – concretamente, Internet – es

[1] Trabajo realizado en el marco del Proyecto de Investigación DER 2017-82638-P. La prestación de servicios de carácter digital: Retos y lagunas. Investigadora Principal: Prof. Dra. María José Santos Morón.

en el de los datos personales. La penetración y omnipresencia de este instrumento en múltiples aspectos de la vida cotidiana ha llevado a una preocupación creciente por la protección de los datos personales de los usuarios. Seamos o no conscientes de ello, cuando navegamos en Internet o interactuamos adquiriendo productos o servicios, estamos proporcionando datos de muy diversas maneras[2]. En algunos casos, los datos son facilitados directamente por el propio sujeto, al formalizar la relación contractual o en el marco de la misma. Pensemos, por ejemplo, en el *home banking* (servicios bancarios *online)*. Para formalizar el contrato, el usuario puede tener que proporcionar datos personales tales como el nombre y apellidos, el correo electrónico o la fotografía y número del documento de identidad. Pero también, en la propia ejecución de esa relación contractual, se genera mucha información, como son los movimientos de las cuentas, las compras que se realizan, los créditos o las posibles situaciones de insolvencia del cliente. Parte de este flujo de información de naturaleza financiera puede revelar, incluso, datos de naturaleza sensible, como serían los relacionados con la ideología, religión o salud (pago de cuotas de afiliación a un partido político, a una asociación, compras de medicamentos o de servicios médicos)[3].

Además, los sujetos también proporcionan multitud de datos de forma que podríamos denominar indirecta, con la mera navegación a través de las distintas páginas. Esto último se posibilita, entre otros, gracias a las conocidas como *cookies* – propias o de terceros –, pequeños archivos que permiten a las páginas web recoger información del usuario que visita la página (tipo de navegador, sistema operativo, dirección IP, etc.) para, por ejemplo, reconocerle y recordar su usuario y contraseña o analizar su comportamiento y preferencias[4].

Todos estos datos son utilizados por las empresas para la propia prestación del bien o servicio contratado, pero también es muy habitual en la actualidad que la recolección de datos sea un negocio en sí mismo. Como es sabido, el análisis de la información de sus clientes puede ayudar a las empresas a ser más eficientes o a desarrollar nuevos productos y servicios basándose en su comportamiento, sus necesidades existentes o previendo otras nuevas. Pero también pueden monetizar los datos vendiéndolos a terceros. De hecho, han surgido múltiples modelos de negocio que se nutren del *tracking* y *profiling* de los datos, esto es, operadores cuyo negocio consiste, precisamente, en rastrear, recopilar y tratar datos para construir perfiles o patrones que tienen un gran interés de cara a, por ejemplo, una mayor eficacia de la publicidad de las

[2] **NE**. Nos seja permitido informar que o belíssimo texto ora publicado dialoga com dois outros artigos cinzelados nas páginas da REDES: CONSALTER, Zilda Mara; ROCHA, Isadora de Souza Rocha. A privacidade e o panóptico digital: as práticas consumeristas e a superexposição como vetores da relativização desse direito individual. **Revista Eletrônica Direito e Sociedade**, Canoas, v. 7, n. 3, p. 167–195, out. 2019. EHRHARDT JUNIOR, Marcos; MODESTO, Jéssica Andrade. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica Direito e Sociedade**, Canoas, v. 8, n. 2, *Ahead of print*, ago. 2020.

[3] GIOBBI, M. Home banking y tutela de los datos personales. En: PÉREZ GALLARDO, L. (Coord.). **Contratación electrónica y protección de los consumidores – una visión panorámica**. Madrid: Reus, 2017. p. 313.

[4] ORTIZ LÓPEZ, P. Cookies, fingerprinting y la privacidad digital. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018. p. 269. Otras técnicas, además de las *cookies*, son balizas-web o las etiquetas de píxeles invisibles. V. CÁMARA LAPUENTE, S. Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad. En CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. (Dir.). **El mercado digital en la Unión Europea**. Madrid: Reus, 2019. p. 193-194.

empresas. Pensemos en proveedores de redes sociales, de apps para la salud o de suministro de servicios y contenidos digitales como podrían ser *Facebook*, *LinkedIn*, *Dropbox*, *Google Fit* o *Youtube*. Son todos "gratuitos" o bien forman parte de lo que se ha venido a denominar el modelo de negocio "freemium"[5]. Sea como fuere, ofrecen al usuario la posibilidad de recibir sus prestaciones de forma gratuita en el sentido de no retribuida con dinero. Los usuarios "pagan" con contribuciones no monetarias, con la información y los contenidos que generan, con su actividad e interacción en la página o en otras, esto es, con información derivada de sus datos, que se explotan comercialmente[6].

Viendo el aumento del peso de la economía de datos y de los negocios basados en la explotación de esta información, es obligado volver la mirada al marco jurídico existente para la recolección y tratamiento de datos. Si nos centramos en el ámbito europeo, la norma principal vigente en la actualidad es el Reglamento (UE) 2016/679, 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 (en adelante, RGPD)[7]. Esta norma, de carácter imperativo y de aplicación directa en todos los Estados miembros[8], ha supuesto, por un lado, la armonización de criterio en la aplicación y garantía de los derechos de los ciudadanos europeos en materia de privacidad y protección de datos. Esta regulación más uniforme está en consonancia con una sociedad cada vez más globalizada en la que ha aumentado el flujo transfronterizo de datos personales. Por otro lado, y como tendremos ocasión de señalar, el RGPD ha conllevado, asimismo, un cambio en el enfoque desde el que se aborda la protección de datos, siendo los requisitos del consentimiento y el principio de responsabilidad o rendición de cuentas -el conocido como *accountability*- algunas de las novedades más relevantes de la norma[9].

Junto con el RGPD, en el entorno digital también hay que atender a la Directiva 2002/58/CE, de 12 de julio de 2002, sobre la privacidad y las comunicaciones electrónicas que, entre otras cuestiones, vino a regular el uso de las *cookies* (de hecho, se conoce informalmente como la "ley de *cookies*"). Esta norma fue modificada en 2009 (por la Directiva 2009/136/CE) para reforzar las garantías de los usuarios de Internet, endureciendo el régimen de consentimiento para la instalación y ulterior uso de las *cookies*.

---

[5] Se entiende por el modelo de negocio "*freemium*" aquel que ofrece a sus usuarios la posibilidad de recibir acceso gratuito a ciertos servicios restringidos (*free*) con la opción de eliminar esas restricciones mediante una suscripción de pago (*premium*). Sobre el concepto: SEUFERT, E. B., **Freemium Economics: leveraging analytics and user segmentation to drive revenue**. Massachusetts: Morgan Kaufmann, 2014. p. 1.

[6] Sobre la monetización de los datos y el modelo de negocio de las redes sociales: GARCÍA MEXÍA, P.; PERETE RAMÍREZ, C. Internet, el RGPD y la LOPDGDD. En: **La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD**. Madrid: Bosch Wolters Kluwer, 2019. p. 852-857.

[7] Esta norma ha venido a derogar la Directiva 95/46/CE, vigente hasta la entrada en vigor del Reglamento.

[8] Debe apuntarse que el Reglamento, aun siendo imperativo, incluye una habilitación a los Estados miembros para que puedan especificar sus normas (Considerando 10º RGPD). Por ejemplo, en el caso español, la adaptación del RGPD al Ordenamiento Jurídico nacional se ha producido a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[9] Una primera aproximación a los aspectos característicos del modelo europeo de protección de datos se encuentra en CERVERA-NAVAS, L. El nuevo modelo europeo de protección de datos de carácter personal. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018. p. 71-72.

No obstante, en la actualidad se está debatiendo una Propuesta de Reglamento del Parlamento Europeo y del Consejo (2017/0003) sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (el denominado Reglamento de e-Privacidad). Aunque no hay un texto definitivo, esta norma nace desde planteamientos más restrictivos y con la idea de garantizar un alto nivel de protección de la privacidad en todas las comunicaciones electrónicas cuyos usuarios finales se encuentren en la Unión Europea. Cuando se apruebe[10], en su caso, derogará a la Directiva de 2002 y será, junto con el RGPD, la otra norma fundamental a tener en cuenta en esta materia y ámbito geográfico. Volveremos sobre ella más adelante, como parte de "lo que está por venir".

El consentimiento como base legal para el tratamiento de datos personales

Requisitos para un consentimiento válido

Es un hecho constatado que el tratamiento de datos personales es una actividad fundamental en la economía digital. Para su licitud, el RGPD exige que concurra al menos una de las seis bases legales que se establecen en su art. 6.1. El primer fundamento que habilita el tratamiento de los datos personales es el consentimiento del propio interesado (art. 6.1.a RGPD)[11]. Nos detendremos en este trabajo a realizar algunas consideraciones acerca de esta causa justificativa del tratamiento pues, como tendremos ocasión de ver en este epígrafe, precisamente su régimen jurídico es una de las novedades relevantes que ha supuesto la entrada en vigor del RGPD y uno de los mecanismos a través del que se ha pretendido reforzar la protección del titular. Idéntica orientación tendrá el epígrafe III, respecto de, en este caso, la Propuesta de Reglamento de e-Privacidad.

Pues bien, si en la Directiva 95/46/CE se definía el consentimiento del interesado como "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen" (art. 2.h), en el RGPD se añade a los tres requisitos "libre, específica e informada" un cuarto, pues la declaración de voluntad por la que el interesado acepta debe ser, además, "inequívoca", "ya sea mediante una declaración o una clara acción afirmativa" (art. 4.11). Además, el Reglamento se detiene explícitamente a desarrollar las condiciones para dicho consentimiento (art. 7).

Que el consentimiento sea *libre* se vincula con el hecho de que la prestación o ejecución del contrato no esté supeditada a acceder al tratamiento de datos personales que no sean necesarios para la misma. Esto es, que sea una elección real y que, de no tomarla, el sujeto no sufra ninguna consecuencia negativa que disminuya su nivel de prestación, aunque sí pueda, por ejemplo, perder ciertos servicios o ventajas extras (por ejemplo, descuentos personalizados o poder resolver consultas y solicitudes fácilmente a través de los

[10] Aunque la Propuesta de Reglamento fue publicada el 10 de enero de 2017, aún no se ha logrado consenso sobre un texto definitivo (última reunión, 22 de noviembre de 2019).

[11] Aunque no se establece ningún orden de prioridad en las causas de legitimación, siendo todas ellas igual de lícitas, tal y como subraya PUENTE ESCOBAR, A. Principios y licitud del tratamiento. En: RALLO LOMBARTE, A. (Dir.). **Tratado de protección de datos**. Valencia: Tirant lo Blanch, 2019. p. 124.

canales de atención o comunicación habilitados por la entidad)[12]. Por otro lado, y enlazando con el requisito de que sea una manifestación de voluntad *específica*, es necesario que el interesado pueda elegir libremente qué fines del tratamiento acepta y cuáles no, teniendo en cuenta que el tratamiento de los datos que se recaban puede tener muy distintas finalidades (por ejemplo, personalizar el servicio, conservar datos de tarjetas de pago para futuras compras, gestionar un servicio de alertas de disponibilidad de productos, emitir documentos acreditativos de venta como el ticket digital, gestionar espacios de publicidad o medición de audiencias, etc.)[13]. Esto implica, asimismo, que los fines concretos deben identificarse claramente y no con referencias vagas y genéricas[14], de tal forma que también sea evidente qué finalidades abarca el consentimiento y cuáles quedan fuera y, por tanto, necesitarían de una nueva y diferente manifestación de voluntad[15].

Denominador común a estos requisitos para un consentimiento lícito es la necesidad de información. Difícilmente una manifestación de voluntad puede haberse formado de una manera libre y específica si no ha sido *informada*, esto es, si el usuario no ha recibido toda la información necesaria, de una forma comprensible y adecuada. Así, se hace presente de un modo especial en el consentimiento el principio de transparencia, para empezar, desde el punto de vista del contenido, es decir, de los datos mínimos que deben proporcionarse al interesado, como la identidad del responsable del tratamiento, su finalidad, el tipo de datos, el plazo durante el que se conservarán o los derechos que le asisten, entre otros (art. 13 RGPD).

> En el ámbito de las *cookies*, es de observar que la sentencia del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) de 1 de octubre de 2019 (asunto C 673/17) recientemente ha precisado que forma parte de la información clara y completa que se exige legalmente la información acerca del tiempo durante el cual las *cookies* estarán activas, así como la posibilidad de que terceros tengan acceso a ellas (Considerando 75).

Por otro lado, el principio de transparencia también se manifiesta desde la perspectiva del modo en el que se debe proporcionar esa información. A este respecto, el RGPD deja claro que debe ser dispuesta de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo (arts. 7.2 y 12.1).

---

[12] GRUPO DE TRABAJO DEL ARTICULO 29 (en adelante, GT29). **Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679**, WP259. p. 12. Un ejemplo de cómo plasmar esta directriz en el clausulado sería señalar: "La retirada del consentimiento de estos tratamientos por parte del interesado no condicionará la ejecución del contrato de compraventa celebrado entre éste y la entidad". Es usual que, respecto de los datos recabados por las *cookies*, las entidades introduzcan la recomendación de dar su consentimiento a todo tratamiento propuesto a efectos de no perder calidad en el servicio, con menciones tales como: "El usuario tiene la posibilidad de configurar su navegador en cualquier momento, deshabilitando la instalación de las *cookies* y eliminando las *cookies* previamente instaladas en su equipo. Al eliminar y/o deshabilitar las *cookies*, el usuario se expone a no poder acceder a determinadas funcionalidades de la Web/App o a que su experiencia de navegación resulte menos satisfactoria. Por eso, le recomendamos que las mantenga activadas".

[13] Que exista la opción consentir (o no) de forma específica y separada para una de las finalidades es lo que se entiende por consentimiento granular.

[14] Así, motivos como "mejorar la experiencia del usuario", "fines de mercadotecnia", "fines de seguridad informática" o "investigaciones futuras", sin más detalles, normalmente no cumplen el criterio de ser específico, como pone de relieve el GT29 en sus **Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679**, WP259. p. 13 – nota a pie 28.

[15] Por ejemplo, el consentimiento dado para el tratamiento de los datos personales derivados de los comandos o conversaciones del usuario con un asistente virtual de la entidad con la que ha contratado, con el fin de disfrutar de ese servicio de atención personalizada, no abarcaría el tratamiento de esos datos para su envío a terceros colaboradores que pudieran estar interesados en los problemas o preferencias del usuario a efectos de desarrollar productos o enviarle publicidad.

Dado que, como es sabido, el exceso de información, muy detallada y con cierta terminología tecnológica y/o jurídica, puede generar en el usuario medio el efecto contrario al que se pretende conseguir, en muchos casos se tiende a proporcionarla "por capas" o "niveles", esto es, ofreciendo una visión general en un primer nivel de información y señalando después cómo acceder a más detalles[16].

A su vez, que se trate de una declaración de voluntad informada conlleva también que el interesado pueda claramente identificar la solicitud de consentimiento para el tratamiento de datos respecto de otras posibles declaraciones. Así las cosas, el art. 7.2 RGPD exige que, si el consentimiento se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud se presente de tal forma que se distinga nítidamente de los demás contenidos: en documentos separados, si es en papel; separado de otros términos y condiciones, si es a través de medios electrónicos. Volveremos sobre ello, pero el hecho de que deba ser evidente para el interesado que está prestando su consentimiento para el tratamiento de datos personales convierte en contrario a la norma que un responsable del tratamiento solicite conjuntamente y mediante una misma acción (por ejemplo, seleccionar una única casilla) que el usuario acepte los términos y condiciones generales de un contrato y, a la vez, la política de privacidad[17]. Esta condición para un consentimiento válido a efectos del RGPD está relacionada con el último de los requisitos exigidos por la norma, esto es, un consentimiento *inequívoco*, "ya sea mediante una declaración o una clara acción afirmativa". Se trata, éste, de un importante nuevo requisito respecto de la Directiva 95/46/CE, que no exigía que el consentimiento fuera prestado de forma expresa. Junto a una solicitud diferenciada, exigir la existencia de un acto afirmativo claro excluye como consentimiento válido el silencio, la inacción o el recurso a casillas premarcadas o a casillas de exclusión voluntaria en un sitio web[18]. Ha de quedar claro – y tiene la carga de probarlo el responsable[19] – que el sujeto ha consentido intencionadamente el tratamiento de sus datos personales.

> La anteriormente citada sentencia del TJUE de 1 de octubre de 2019 ha venido también a subrayar este criterio en el marco del almacenamiento y uso de información obtenida mediante la instalación de *cookies*. En el caso concreto, el litigio se plantea al hilo de una página de internet de juego con fines promocionales en la que se mostraban dos avisos a fin de que los usuarios prestasen su consentimiento para, por un lado, el tratamiento de

[16] VILASAU SOLANA, M. El consentimiento general y de menores. En: RALLO LOMBARTE, A. (Dir.). **Tratado de protección de datos**. Valencia: Tirant lo Blanch, 2019. p. 211-212. APARICIO SALOM, J. Derechos del interesado (arts. 12-19 RGPD. Arts. 11-16 LOPDGDD). En: LÓPEZ CALVO, J. (Coord.). **La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD**. Madrid: Wolters Kluwer, 2019. p. 326-327. GT29. **Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679**, WP259. p. 16-17. En la práctica se suele articular con enlaces en expresiones como: "Obtén más información sobre estos fundamentos legales y cómo se aplican a nuestro tratamiento de datos". También con pequeños textos resumen al lado de las cláusulas, recogiendo de un modo sencillo y directo la idea fundamental de cada cláusula/epígrafe de las condiciones de privacidad.

[17] GT29. **Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679**, WP259. p. 14 y 16.

[18] Considerando 32 RGPD y GT29. **Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679**, WP259. p. 18. Como señala este último documento (p. 19), si bien continuar con la navegación en un sitio web o desplazar hacia abajo no es un movimiento concluyente de aceptación, sí lo podrían ser otros como arrastrar una barra en una pantalla, saludar con la mano ante una cámara inteligente o hacer girar un teléfono inteligente de una determinada manera.

[19] Así lo establece claramente el art. 7.1 RGPD.

> datos encaminado a recibir comunicaciones de terceros patrocinadores y colaboradores y, por otro, la instalación de *cookies* para fines publicitarios propios y de terceros. Esta última casilla estaba marcada por defecto, lo que, en palabras del Tribunal, hace prácticamente imposible determinar de manera objetiva si el usuario ha dado efectivamente su consentimiento para el tratamiento de sus datos personales, al no quitar la marca, y si dicho consentimiento ha sido dado, en todo caso, de manera informada. Este razonamiento permite reafirmar, como se apunta en la sentencia, que el consentimiento dado mediante una casilla marcada por defecto no implica un comportamiento activo por parte del usuario de un sitio de internet y, por tanto, no es un consentimiento válido (Considerandos 52 y 55).

El consentimiento al tratamiento de datos personales en los contratos "gratuitos"

Vistos de forma genérica los requisitos actuales del RGPD para que el consentimiento funcione como una base legal lícita para el tratamiento, no podemos dejar de hacer referencia a una controversia al respecto que surge en relación con los contratos digitales "gratuitos", entendiendo por tales aquellos en los que el beneficio del proveedor de un servicio se nutre de los datos personales de sus usuarios. Estos modelos de negocio que han florecido considerablemente de la mano de la economía digital y la publicidad *online*, son percibidos por los usuarios como gratuitos pues, como decíamos, no conllevan el pago de una contraprestación de naturaleza pecuniaria, es decir, lo que tradicionalmente entendemos por "precio". Sin embargo, como ha afirmado el *Tribunal de Grande Instance de Paris*, en su sentencia de 9 de abril de 2019, conociendo de una demanda por cláusulas abusivas e ilícitas contra *Facebook*, "el suministro de datos recopilados de forma gratuita y luego analizados y valorados por la empresa *Facebook* debe considerarse como una "ventaja" en el sentido del art. 1107 del Código civil"[20]. Ventaja que "constituye la contrapartida del servicio de red social que la empresa proporciona al usuario, de modo que el contrato concluido con Facebook es un contrato oneroso".

Se produce lo que se ha denominado como una "contractualización de los datos personales"[21]. Entran en juego, por tanto, además de las reglas propias de la protección de datos personales – por el objeto de la contrapartida –, las reglas de Derecho de contratos que son de aplicación a las contraprestaciones en un negocio jurídico. Si nos referimos al ámbito de los contratos de consumo, por representar, posiblemente, la mayoría de los supuestos en la práctica, tratar la "autorización para el uso de datos"[22] como la "contrapartida" de un contrato plantea el interrogante de tener que cumplir, respecto de ella, con ciertas obligaciones de información derivadas de las normas de protección al consumidor.

---

[20] Art. 1107 del Código civil francés: "El contrato es oneroso cuando cada una de las partes recibe de la otra una ventaja a cambio de la que ella proporciona".

[21] En palabras de DE FRANCESCHI, A. **La circolazione dei dati personali tra privacy e contratto**. Napoli: Edizioni Scientifiche Italiane, 2017. p. 9.

[22] Considera CÁMARA LAPUENTE, S. Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad. En: CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. (Dir.). **El mercado digital en la Unión Europea**. Madrid: Reus, 2019. p. 178, que, esta expresión es más adecuada que hablar de "cesión de datos" o cesión del uso – no exclusivo ni excluyente y siempre revocable) de los datos.

Por una parte, y por ser típicamente contratos no negociados, todas las cláusulas tendrán que superar el denominado control de incorporación formal que busca garantizar que el adherente ha tenido la oportunidad de saber que el contrato está regido por un clausulado predispuesto y de acceder y comprender el mismo (de ahí la necesidad de una información clara y comprensible, según el art. 5 de la Directiva 93/13/CEE, de 5 de abril, sobre las cláusulas abusivas en los contratos celebrados con consumidores).

Por otra parte, también estas cláusulas se podrían ver afectadas por las obligaciones de información precontractual a cargo del empresario en los contratos de consumidores, recogidas, en el ámbito europeo, en el art. 6.1 de la Directiva 2011/83/UE, de 25 de octubre, sobre los derechos de los consumidores, respecto de los contratos celebrados a distancia. En él se exige que el empresario facilite de forma clara y comprensible al consumidor, antes de que éste quede vinculado, información sobre una serie de elementos entre los que, obviamente, resalta el precio (art. 6.1.e), así como sobre la existencia de una obligación de pago (art. 8.2). Matizábamos al inicio del párrafo que estos deberes *podrían* afectar a la autorización para el uso de los datos que nos ocupa porque existe un debate en la actualidad acerca de la naturaleza de los datos como "contraprestación" en un contrato y, por tanto, su posible asimilación por extensión al concepto de "precio" y su correspondiente régimen jurídico[23]. Lo cierto es que las citadas Directivas no hacen referencia a deberes específicos de información respecto de los datos recabados por el proveedor de servicios como tampoco lo hace la reciente Directiva 2019/770, de 20 de mayo, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.

Se ha considerado como uno de los grandes logros en esta última norma el hecho de reconocer expresamente la existencia y los derechos de los consumidores que faciliten o se comprometan a facilitar datos personales al empresario a cambio de que éste suministre o se comprometa a suministrar servicios digitales al consumidor (art. 3.1)[24]. Pero, aunque la Directiva de 2019 reconoce positivamente la categoría, ni incluye deberes especiales de información a los usuarios sobre la contraprestación en datos, ni facilita su asimilación al concepto de "precio", pues evita calificar el pago en datos como "contraprestación"[25]. En todo

[23] El debate sobre si los datos personales deberían ser considerados o no como contraprestación tiene su punto de partida en la naturaleza sensible de los mismos pues participan de los derechos de la personalidad, pero con una importante dimensión patrimonial o monetaria. Al respecto, en la medida en que excede de este estudio, nos remitimos a CÁMARA LAPUENTE, S. Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad. En: CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. (Dir.). **El mercado digital en la Unión Europea**. Madrid: Reus, 2019. p. 178-181; METZGER, A. Data as Counter-Performance. What rights and duties do parties have?. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, Berlin, v. 8, n. 1, p. 1-8, 2017. p. 3 y 8. DE FRANCESCHI, A. **La circolazione dei dati personali tra privacy e contratto**. Napoli: Edizioni Scientifiche Italiane, 2017. p. 76-77 y 111. EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content**, 14 March 2017. p. 7, 9-10.

[24] SCHULZE, R.; STAUDENMAYER, D. Digital Revolution – Challenges for contract law. En: SCHULZE, R.; STAUDENMAYER, D. (Eds.). **Digital revolution: challenges for contract law in practice**. Baden-Baden: Nomos, 2016. p. 32. Estos autores resaltan que los datos son ya una moneda en la actualidad y lo serán más en el futuro, además de la savia de la economía *data-driven*.

[25] De hecho, la expresión inicial de "contraprestación no dineraria en forma de datos personales" se eliminó del texto durante su tramitación.

caso, con independencia de la terminología, entendemos que lo lógico es que el consumidor deba recibir información suficiente acerca de qué es lo que supone el contrato para él, sea dinero o no[26].

En apoyo de esta afirmación cabría añadir la existencia de un control en la contratación no negociada de consumo – desarrollado jurisprudencial y doctrinalmente en los últimos años en el Derecho europeo – relacionado con una especial transparencia exigible al empresario respecto de las cláusulas que se refieren al objeto principal del contrato (en el caso que nos ocupa, la cesión del uso de datos personales). Se trata del conocido como control de transparencia material, en aplicación del cual, el consumidor debe haber recibido la información suficiente sobre las cláusulas que definen el objeto principal del contrato como para poder comprender realmente a qué se está vinculando pues éste – el bien o servicio y lo que va a dar a cambio – es lo que determina la decisión del consumidor de contratar o no contratar[27].

Pues bien, si yuxtaponemos las obligaciones de información de las normas contractuales con los requisitos del RGPD de un consentimiento lícito para el tratamiento de los datos personales, y todo ello, a su vez, con la práctica habitual en la formación de muchos contratos *online* "gratuitos", surgen ciertos interrogantes. Es frecuente, por ejemplo, que solo haya que marcar una única casilla para aceptar las condiciones generales del contrato, las condiciones de privacidad y la política de *cookies*, advertida la simple existencia de estas dos últimas de forma muy secundaria (ni que decir tiene su contenido e implicaciones, que solo serían visibles tras hacer clic en un enlace). Es cuestionable que ese consentimiento al tratamiento de datos personales sea un consentimiento realmente informado y transparente y, por otro lado, no parece cumplir con el requisito de ser inequívoco, en el sentido de distinguirse visiblemente respecto de cualquier otro asunto o consentimiento que se preste[28].

---

[26] DE FRANCESCHI, A. **La circolazione dei dati personali tra privacy e contratto**. Napoli: Edizioni Scientifiche Italiane, 2017. p. 91-94, 127. Sostiene que también en las hipótesis de suministro de contenido o servicios digitales que tengan como "contrapartida" el consentimiento al tratamiento de datos el proveedor oferente deberá respetar las obligaciones derivadas de los requisitos formales de los contratos a distancia.

En general, de manera más amplia sobre las garantías de información aplicables al supuesto de hecho desde el punto de vista del Derecho de los contratos, ver MATO PACÍN, M. N. Los contratos de redes sociales como contratos mediante condiciones generales. En: ALONSO PÉREZ, M.T.; HERNÁNDEZ SÁINZ, E. (Dir.). **Servicios, condiciones generales y transparencia**. Pamplona: Aranzadi, 2020.

[27] El referido control de transparencia material se ha desarrollado en los últimos años al hilo de determinadas cláusulas en un supuesto totalmente diferente del objeto de estas líneas, como es el de los contratos de préstamo hipotecario de consumo. Un resumen acerca del funcionamiento y justificación del control -perfectamente extrapolable a cualquier tipo de contrato no negociado de consumo-, se encuentra en MATO PACIN, M. N. Deber de transparencia material en la contratación de préstamos hipotecarios con consumidores en el ordenamiento jurídico español. **Revista Boliviana de Derecho**, Bogotá, n. 27, p. 188-219, 2019. p. 190-196.

[28] Nos referimos, evidentemente, al tratamiento de datos que tiene como base legal el consentimiento del interesado y no aquel que se asienta sobre otro fundamento habilitador distinto como podría, ser, por ejemplo, la propia ejecución del contrato (ver siguiente epígrafe). En los últimos tiempos, de forma paralela a ciertos acuerdos con órganos de la Comisión Europea, algunos de estos proveedores de servicios (por ejemplo, *Facebook*) han trabajado en clarificar al usuario en sus clausulados generales cuál es su modelo de negocio en relación con el tratamiento de datos. Sin embargo, sigue sin estar resaltado de una manera clara, transparente e inequívoca en la fase previa a "registrarse" o contratar. Sobre estas cuestiones, nos remitimos a MATO PACÍN, M. N. Los contratos de redes sociales como contratos mediante condiciones generales. En: ALONSO PÉREZ, M.T.; HERNÁNDEZ SÁINZ, E. (Dir.). **Servicios, condiciones generales y transparencia**. Pamplona: Aranzadi, 2020.

Las otras bases legales para el tratamiento de datos personales

Si bien el consentimiento del titular de los datos personales es uno de los fundamentos que habilita para su tratamiento, no es el único. Es más, se ha apuntado que, desde el punto de vista del responsable del tratamiento, el consentimiento – dada su fragilidad – sería la base legal a la que recurrir cuando dicho tratamiento no puede subsumirse en ninguna otra[29]. ¿Cuáles son esos otros fundamentos jurídicos que permiten, aunque no haya consentimiento, el tratamiento lícito de datos personales? De forma sucinta, y en virtud del art. 6.1, letras (b) a (f) RGPD, son los que a continuación se enumeran.

En primer lugar, hay ciertos datos cuyo tratamiento es *necesario para la propia ejecución del contrato* en el que el interesado es parte y en cuyo marco se han aportado o recabado o bien *para la aplicación de medidas precontractuales a petición del interesado*. Pensemos, por ejemplo, en la dirección para la tramitación del envío de los bienes adquiridos objeto del contrato, en los datos del medio de pago del cliente para ejecutar la venta, en el teléfono o el email para la resolución de problemas del servicio contratado o, respecto de las medidas precontractuales, en los datos derivados de una solicitud de proposición de seguro[30]. Evidentemente, los datos que caen dentro de esta categoría deben ser interpretados de forma restrictiva[31]. El tratamiento deber ser objetivamente necesario para la ejecución de ese contrato concreto y ser la forma menos intrusiva de conseguirlo, sin que, por otra parte, sea suficiente que en el clausulado del contrato se recoja esta base si realmente no existe la necesidad del tratamiento (no sería una base legítima, aunque conste como tal en el contrato)[32].

En otro orden de ideas, no ofrece problema entender el fundamento de las bases legales que están vinculadas con valores que transcienden los intereses particulares. Así, será lícito el tratamiento de datos *necesarios para el cumplimiento de una obligación legal* (por ejemplo, datos de pagos y compras necesarios para la gestión y emisión de la factura de venta al cliente o para detectar pagos fraudulentos; datos relevantes en investigaciones penales) o el tratamiento *necesario para proteger los intereses vitales del interesado u otra persona física* o *por cumplimiento de una misión realizada en interés público* (pensemos en datos de movilidad de los clientes de operadores de telecomunicaciones para hacer un seguimiento de la población de un país y controlar una pandemia, como está sucediendo en Europa con el Covid-19).

---

[29] SEINEN, W.; WALTER, A.; VAN GRONDELLE, S. Compatibility as a mechanism for responsible further processing of personal data. En: MEDINA, M. et al (Ed.). **Privacy technologies and policy**. Switzerland: Springer, 2018. p. 155. Los autores señalan que el consentimiento es un concepto frágil en el sentido de que puede ser revocado, su validez puede ser modificada y, al recaer sobre el responsable del tratamiento la carga de la prueba, éste debe crear un rastro de los datos que confirme que el consentimiento se ha obtenido a través de un proceso válido.

[30] LLÁCER MATACÁS, M. R. **La autorización al tratamiento de información personal en la contratación de bienes y servicios**. Madrid: Dykinson, 2012. p. 74-75. Señala como ejemplos de tratamiento legítimo de información precontractual el de los datos necesarios para que la aseguradora valore correctamente el riesgo o el de los que requieren las entidades financieras para evaluar la solvencia de un futuro cliente con el fin de concederle un crédito responsable.

[31] DE FRANCESCHI, A. **La circolazione dei dati personali tra privacy e contratto**. Napoli: Edizioni Scientifiche Italiane, 2017. p. 84.

[32] Acerca de la interpretación del art. 6.1.b RGPD, ver EUROPEAN DATA PROTECTION BOARD. **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects**, 9 April 2019. p. 7-9.

Por último, el art. 6.1 letra (f) contempla los *intereses legítimos* del responsable del tratamiento o de un tercero – siempre que, hecha una ponderación, no existan intereses o derechos y libertades del interesado que prevalezcan – como justificación para el tratamiento de los datos (por ejemplo, tratamiento de datos para la prevención del fraude o para mercadotecnia directa[33]). Es obvio que el tipo de fines que podría un responsable encajar dentro de su "interés legítimo" puede ser de lo más variado y, por otra parte, no siempre claro, dada la indeterminación con la que se prevé en la norma y dada, además, la necesidad de realizar una ponderación. Se trata, en la práctica y atendiendo a los clausulados de las entidades, de un fundamento al que se recurre frecuentemente.

> Respecto de esta base legal, el TJUE, en su sentencia de 19 de octubre de 2014 (caso C-582/14), falló a favor de entender que la dirección IP dinámica mediante la que un usuario accede a la página web de un proveedor de servicios de telecomunicaciones es un dato personal, cuyo tratamiento para garantizar el servicio y protegerlo contra ciberataques puede considerarse como un interés legítimo.

Junto con las seis bases legales recogidas en el art. 6.1 RGPD, es de obligada mención una especie de puerta que abre la propia norma para el tratamiento de datos con fines distintos de aquellos para los que fueron recogidos inicialmente (*further processing*). Siempre, eso sí, que sean compatibles con éstos y que la base jurídica legal del tratamiento inicial no hubiera sido ni el consentimiento del interesado ni el Derecho comunitario o nacional (art. 6.4 RGPD). El *further processing* es muy relevante en la práctica para buena parte de los responsables del tratamiento en la medida en que permite reutilizar datos para otras finalidades[34]. No obstante, el concepto de la "compatibilidad" no es un concepto bajo el que, lógicamente, pueda ampararse todo tipo de tratamiento pues no hay que olvidar que uno de los principios que rigen la protección de datos es el de limitación de la finalidad[35]. Se trata de un concepto indeterminado, a valorar caso por caso, teniendo en cuenta una serie de criterios como la relación entre ambos fines y entre el responsable del tratamiento y el interesado, el contexto en el que se recogieron o la naturaleza de los datos personales (art. 6.4 RGPD).

---

[33] Considerandos 47 y 48 RGPD. En todo caso, se realiza un análisis en profundidad acerca de esta base legal por parte del GT29. **Dictamen 6/2014, sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE**, 9 abril 2014. p. 29 y ss. Asimismo, ejemplos extraídos de las condiciones de privacidad de una compañía de venta de ropa y que se amparan en esta base legal serían la elaboración de programas de fidelización para clientes registrados o el envío de encuestas de satisfacción sobre los productos adquiridos o servicios usados por los clientes para poder mejorarlos. Todo ello dentro del interés legítimo de la entidad de garantizar que la página y la app permanecen seguras y de mejorar los servicios, productos y marcas comprendiendo mejor a los clientes. También se ha incluido en esta categoría -en este caso, en las condiciones generales de privacidad de un proveedor de servicios digitales (*Spotify*)- el tratamiento para cumplir con obligaciones contractuales con terceros (ej. contratos de licencia), para tomar las medidas oportunas respecto a informes de vulneración de propiedad intelectual y contenidos inadecuados, para iniciar actuaciones legales u oponerse a ellas o para fines de planificación, información y estimaciones del negocio.

[34] Sobre la compatibilidad, véase SEINEN, W.; WALTER, A.; VAN GRONDELLE, S. Compatibility as a mechanism for responsible further processing of personal data. En: MEDINA, M. et al (Ed.). **Privacy technologies and policy**. Switzerland: Springer, 2018. p. 153 y ss.

[35] Art. 5.1.(b) RGPD: "Los datos personales serán: (b) recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines […]".

> Por ejemplo, tras quejas de consumidores ante la modificación de la política de privacidad de un banco, la Autoridad de Protección de Datos holandesa advirtió en julio de 2019 que utilizar los datos obtenidos inicialmente de las cuentas de sus clientes para una finalidad ulterior diferente -la de marketing, ofreciéndoles productos adicionales-, es contrario al RGPD. Si bien el tratamiento de los datos derivados de las operaciones de pago encaja válidamente en el supuesto de necesidad para la ejecución del contrato, el segundo tratamiento no superaría el test de la compatibilidad que le podría dar amparo normativo: tener una cuenta bancaria -algo casi imposible de evitar hoy en día, entiende la Autoridad holandesa- no presume el interés en otros productos financieros y este nuevo uso de los datos -mostrar anuncios basados en sus hábitos de gastos- excedería las expectativas razonables de los usuarios respecto de la confidencialidad en el marco de esa relación[36].

¿Del modelo "advice & consent" al del "privacy by design"?

Cuando hablamos de privacidad y entorno digital, y como señalábamos al delimitar el marco jurídico aplicable, el RGPD debe completarse con la Directiva 2002/58/CEE (en su versión de 2009), norma que será sustituida por el Reglamento de e-Privacidad, en discusión en la actualidad. Este nuevo Reglamento será, en el que caso de que finalmente se apruebe, norma especial frente a la general (RGPD), que seguirá siendo de aplicación para aquellas cuestiones relacionadas con el tratamiento de datos personales no reguladas específicamente en la primera. Muchas de las medidas que recoge la Propuesta son más estrictas que las vigentes en la actualidad, lo que ha generado cierto debate entre los distintos grupos de interés.

Entre las novedades del texto original de la Propuesta y en relación con el objeto de este trabajo, podemos resaltar el refuerzo del papel del consentimiento como base legal del tratamiento de datos personales (arts. 6 y 9), restringiendo, respecto del RGDP, las posibilidades para tratar datos del usuario con otros fundamentos distintos. Por ejemplo, aunque sigue autorizándose el tratamiento de datos que sea necesario para proporcionar el servicio, no existe ya mención específica al "interés legítimo" del responsable como causa justificativa general del tratamiento de los datos personales[37].

Pero si hay un artículo de la Propuesta de Reglamento de e-Privacidad que conlleva un vuelco en la perspectiva desde la que abordar el consentimiento del interesado para el tratamiento de datos personales es el art. 10 ("Información y opciones de configuración de privacidad que han de proporcionarse").

---

[36] BIRD&BIRD, Dutch Data Protection Authority warns banks to refrain from using transactional data for direct marketing purposes, July 2019. En la carta se resaltaba cómo ciertas transacciones de pago pueden ser sensibles y dar una imagen muy exacta de la vida de una persona (en qué se gasta el dinero el cliente -hospitales, farmacias, asociaciones a las que pertenece-, con quién se relaciona, etc.), por lo que el cliente tiene una expectativa de privacidad (https://www.dutchnews.nl/news/2019/07/privacy-watchdog-warns-banks-not-to-use-client-payment-details-for-marketing/)

[37] Sí que se contemplan casos como el tratamiento necesario para mantener la seguridad de las redes y servicios o la detección de fallos, que en el RGPD podrían caer dentro de ese "interés legítimo" del responsable, pero no existe la categoría general como tal. Respecto del consentimiento del usuario final como eje sobre el que descansa el sistema en la propuesta de Reglamento, ver FLAQUER RIUTORT, J. Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy). **Revista Aranzadi de Derecho y Nuevas Tecnologías**, Pamplona, v. 47, [s.p.], 2018. ORTIZ LÓPEZ, P. Cookies, fingerprinting y la privacidad digital. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018. p. 272.

Según el tenor literal de los dos primeros apartados: "1. Los programas informáticos comercializados que permiten comunicaciones electrónicas, incluyendo la recuperación y presentación de información de Internet, ofrecerán la posibilidad de impedir a terceros almacenar información sobre el equipo terminal de un usuario final o el tratamiento de información ya almacenada en ese equipo. 2. Al iniciarse la instalación, los programas deberán informar a los usuarios finales acerca de las opciones de configuración de confidencialidad y, para que pueda proseguir la instalación, solicitar el consentimiento del usuario final respecto de una configuración determinada".

Este precepto abre la posibilidad a que *ya en el diseño del software* que permite el acceso a Internet puedan configurarse los ajustes de privacidad necesarios para que, de forma general, terceros no puedan almacenar información sobre ese equipo o no puedan tratar la ya almacenada. En ese primer momento, el usuario recibe información sobre esta posibilidad para que decida el ajuste de privacidad que mejor encaja con sus intereses. Esta previsión no supone, pese a lo dicho, una novedad estrictamente hablando. Se enmarca dentro de lo que se conoce como la privacidad desde el diseño ("*privacy by design*") y por defecto ("*by default*"), dos conceptos ya presentes en el RGPD (art. 25 RGPD) y que no son sino manifestación del nuevo enfoque de esta norma europea en lo que a la actitud de los responsables del tratamiento de datos personales se refiere: una actitud (y, por tanto, responsabilidad) proactiva, concepto cercano al principio anglosajón "*accountability*"[38]. Si la privacidad desde el diseño implica que la privacidad esté integrada en el propio sistema desde su concepción y no añadida como una capa de seguridad *a posteriori*, la privacidad por defecto conlleva que, de las diferentes opciones de tratamiento de datos, se opte por la más respetuosa para la privacidad del usuario, mientras que éste no autorice activamente lo contrario[39].

Este modo de configurar desde el diseño, en lo que aquí interesa, cómo se recaba el consentimiento, difiere del sistema - podríamos decir, más tradicional – de protección del titular de los datos personales basado en el conocido como "*advice-and-consent*". Este último modelo, que descansa sobre la existencia de un aviso y posterior consentimiento previo a la recogida de datos, presenta, sin embargo, algunas conocidas

---

[38] Este principio, una de las novedades más significativas que aporta el RGPD, está recogido principalmente en el art. 5.2: "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")". Según este nuevo paradigma de responsabilidad, ya no se trata de que el responsable se limite a aplicar normas predeterminadas por la Administración, sino que, para cumplir con su obligación, le corresponde tener iniciativa, ser diligente, y hacer una valoración de los riesgos relacionados con el tratamiento de datos de cara a decidir qué medidas debe adoptar para garantizar el nivel adecuado de protección de datos personales (y demostrarlo), según apunta TRONCOSO REIGADA, A. Del principio de seguridad de los datos al derecho a la seguridad digital. **Economía Industrial**, Madrid, n. 410, p. 127-151, 2018. p. 130-133. Acerca de la responsabilidad proactiva en el RGPD entre otros, ver también MARTÍNEZ MARTÍNEZ, R. El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto. En: GARCÍA MAHAMUT, R.; TOMÁS MALLÉN, B. (Ed.). **El Reglamento General de Protección de Datos.** Un enfoque nacional y comparado. Valencia: Tirant lo Blanch, 2019. p. 312 y ss. BAJO, J. C. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el compliance. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018. p. 279-285.

[39] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Guía de Privacidad desde el Diseño**, Oct. 2019. p. 8. MIRALLES LÓPEZ, R. Protección de datos desde el diseño y por defecto (Art. 25). En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018. p. 427-428.

debilidades en el entorno digital. Se han citado como tales, por ejemplo, la opacidad y complejidad de muchas de las prácticas de recolección automática de datos, que, para un usuario medio, obstaculizan poder entender, en muchas ocasiones, el lenguaje e implicaciones de las advertencias o los clausulados de privacidad que deben aceptar. Por otra parte, la existencia de continuos avisos y peticiones de consentimiento -en muchos casos, además, de forma granulada- durante la navegación o cuando se entabla una relación contractual en Internet, se ha demostrado como inadecuada en la medida en que genera una alta percepción de protección que da lugar, contradictoriamente, a un mayor nivel de exposición en la práctica (*privacy fatigue*)[40]. En definitiva, una gran cantidad de información y de peticiones de autorización puede conllevar que el consentimiento se preste sin reflexionar y originar, así, al efecto contrario al perseguido.

Así las cosas, permitir al consumidor prestar un consentimiento general (modificable con posterioridad) a través de los ajustes de un *software* se ha visto en la Propuesta de Reglamento de e-Privacidad como una forma de recabar el consentimiento que permitiría superar las debilidades mencionadas y garantizar una mayor protección. En este sentido, el Comité Europeo de Protección de Datos ha considerado que el art. 10 permitiría a los usuarios tener el control sobre sus datos abogando incluso, junto con el Supervisor Europeo de Protección de Datos, por endurecer el artículo imponiendo la obligación al proveedor de *software* o *hardware* de implementar como configuración predeterminada la opción máxima de privacidad para el usuario, sin necesidad para ello de ninguna acción positiva por su parte Hay que tener en cuenta que el art. 10 parece que solo exige a los proveedores que ofrezcan la posibilidad a los usuarios pero no obliga a que por defecto se establezca la máxima protección[41].

[40] KEITH, M.; LOWRY, P. B.; EVANS, C.; BABB, J. Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure. **International Conference on Information Systems**, Auckland, 2014. p. 2. Los professores definen "privacy fatigue" como la tendencia de los consumidores a revelar más información conforme pasa el tiempo cuando usan controles de privacidad más complejos y poco prácticos. Apuntan estas debilidades del enfoque de "aviso y consentimiento". ENGELMANN, S.; GROSSKLAGS, J.; PAPAKYRIAKOPOULOS, O. A democracy called Facebook? Participation as a Privacy Strategy on Social Media. En: MEDINA, M. et al (Ed.). **Privacy technologies and policy**. Switzerland: Springer, 2018. p. 92. En similar sentido, apunta SUSSER, D. Notice after notice-and-consent: Why privacy disclosures are valuable even if frameworks aren´t. **Journal of Information Policy**, Pensilvânia, v. 9, p. 37-62, 2019. p. 46: que el método "notice-and-consent" muchas veces no ofrece una elección real al usuario pues es una decisión para cuyo análisis el usuario no tiene las herramientas necesarias (cláusulas difíciles de comprender, dificultad para ser consciente de todos los datos que realmente se están proporcionando debido a las sinergias que se crean con la agregación de datos provenientes de distintas fuentes, etc.).

[41] Respaldan el artículo 10 de la Propuesta (aunque con el mayor nivel de protección por defecto) EUROPEAN DATA PROTECTION BOARD. **Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications**, 25 May 2018. p. 3. EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)**, 24 April 2017. p. 19. Por su parte, considera esta agravación planteada como excesiva FLAQUER RIUTORT, J. Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy). **Revista Aranzadi de Derecho y Nuevas Tecnologías**, Pamplona, v. 47, [s.p.], 2018. El autor entiende correcta la dicción del art. 10 tal y como está por representar una solución ecléctica (configuración *ab initio* por el usuario con información junto con la posibilidad de cambiar después si la opción elegida le genera problemas en la navegación).

Evidentemente, también este enfoque tiene sus aspectos negativos como, por ejemplo, no ser el más adecuado para aquellos modelos de negocio en Internet que se basan en las interacciones de los usuarios y los flujos de datos que generan[42]. Este es, de hecho, uno de los argumentos de los detractores de la privacidad por defecto y desde el diseño del art. 10 de la Propuesta, que vaticinan un gran efecto negativo para la industria de la publicidad *online* y para todo ese creciente mercado digital que se financia con ella. Esta medida afecta a las *cookies* de terceros para fines publicitarios – que necesariamente requieren del fundamento legal del consentimiento para su instalación y funcionamiento – y los anunciantes serán reacios a pagar por la publicidad si no tienen un conocimiento real del grado de penetración de sus mensajes[43]. A ello añaden los críticos que no necesariamente se reducirían las solicitudes de consentimiento (las webs que se financian con publicidad tendrían que seguir preguntando en cada página si el usuario acepta las *cookies*) y, especialmente, que un único consentimiento de carácter general para todo el tratamiento de datos en Internet, como el planteado por la Propuesta, puede entrar en colisión con los ya expuestos requisitos del RGPD de un consentimiento inequívoco, informado y específico[44].

Recapitulando, en el presente trabajo se ha pretendido exponer de forma resumida una visión panorámica, dentro del ámbito de la Unión Europea, de las tendencias legislativas en materia de consentimiento para el tratamiento de datos personales, así como de algunas de las controversias generadas a su alrededor. Pronto se identifica la cuestión de fondo que subyace a esta problemática – común a otras en el entorno digital – y que no es sino la tensión entre el Derecho a la privacidad y el desarrollo del mercado digital. Privacidad, en este caso, abordada desde la óptica de la protección de los datos personales, una de las principales preocupaciones del legislador europeo en los últimos años, como acredita la evolución normativa y su tendencia a futuro. Y mercado digital, claramente basado en los datos, de indudable relevancia económica y de cuyo desarrollo en la actualidad ya no se puede realmente prescindir.

Buena muestra de las – lógicas – tensiones que existen en este ámbito es la dificultad para aprobar la Propuesta de Reglamento de e-Privacidad que está teniendo la Unión Europea. Por otra parte, también es significativa la orientación de las modificaciones que se han producido en la fase de discusión en un texto que partía de un muy alto nivel de protección para los sujetos. En la última versión publicada del texto de la Propuesta (noviembre de 2019) algunas de las medidas se han relajado respecto de la versión original

[42] ENGELMANN, S.; GROSSKLAGS, J.; PAPAKYRIAKOPOULOS, O. A democracy called Facebook? Participation as a Privacy Strategy on Social Media. En: MEDINA, M. et al (Ed.). **Privacy technologies and policy**. Switzerland: Springer, 2018. p. 92.

[43] FLAQUER RIUTORT, J. Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy). **Revista Aranzadi de Derecho y Nuevas Tecnologías**, Pamplona, v. 47, [s.p.], 2018.

[44] Desde una postura crítica con el art. 10, recoge los distintos argumentos en su contra ORTIZ LÓPEZ, P. Cookies, fingerprinting y la privacidad digital. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018. p. 271-277. Respecto de la contravención con los principios del RGPD en cuanto al consentimiento, en palabras de la autora, el art. 10 desplaza "la elección individual caso por caso, informada y específica por una elección previa, no específica y general a través de los navegadores". Esto, "al obligar a contar con un único permiso de carácter general dentro de la interfaz, dificulta en la práctica la transparencia y el empoderamiento del usuario". p. 274.

de enero de 2017. Por ejemplo, se han incluido vías de tratamiento de datos que no estaban contempladas en la Propuesta original (así, la posibilidad de tratamiento con nuevas finalidades si son compatibles con las iniciales) y, precisamente respecto del art. 10, que tanto debate ha generado, se habría propuesto su eliminación, al menos, en esta última versión. Esto es relevante porque hay que tener en cuenta que, si bien el RGPD ya supuso un avance reconociendo la privacidad desde el diseño y por defecto, el paso que se daba en la Propuesta de Reglamento de e-Privacidad con este artículo era establecer una obligación específica para el proveedor de tener que ofrecer esta opción e informar sobre ello

De todo lo hasta aquí dicho y con la duda acerca de la viabilidad o contenido de la Propuesta de Reglamento europeo de e-Privacidad, se comprende que uno de los retos actuales y a futuro es encontrar una regulación equilibrada que otorgue una necesaria protección real de los datos personales de los sujetos pero que, a la vez, reconozca y permita el desarrollo de una economía que, por la influencia de las nuevas tecnologías, está basada cada vez más en el flujo de información y datos (*data-driven economy*).

Referencias

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Guía de Privacidad desde el Diseño**, Oct. 2019.

APARICIO SALOM, J. Derechos del interesado (arts. 12-19 RGPD. Arts. 11-16 LOPDGDD). En: LÓPEZ CALVO, J. (Coord.). **La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD**. Madrid: Wolters Kluwer, 2019.

BAJO, J. C. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el compliance. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018.

CÁMARA LAPUENTE, S. Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad. En: CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. (Dir.). **El mercado digital en la Unión Europea**. Madrid: Reus, 2019.

CERVERA-NAVAS, L. El nuevo modelo europeo de protección de datos de carácter personal. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018.

CONSALTER, Zilda Mara; ROCHA, Isadora de Souza Rocha. A privacidade e o panóptico digital: as práticas consumeristas e a superexposição como vetores da relativização desse direito individual. **Revista Eletrônica Direito e Sociedade**, Canoas, v. 7, n. 3, p. 167–195, out. 2019 **(NE)**.

DE FRANCESCHI, A. **La circolazione dei dati personali tra privacy e contratto**. Napoli: Edizioni Scientifiche Italiane, 2017.

EHRHARDT JUNIOR, Marcos; MODESTO, Jéssica Andrade. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica Direito e Sociedade**, Canoas, v. 8, n. 2, *Ahead of print*, ago. 2020 **(NE)**.

ENGELMANN, S.; GROSSKLAGS, J.; PAPAKYRIAKOPOULOS, O. A democracy called Facebook? Participation as a Privacy Strategy on Social Media. En: MEDINA, M. et al (Ed.). **Privacy technologies and policy**. Switzerland: Springer, 2018.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects**, 9 April 2019.

EUROPEAN DATA PROTECTION BOARD. **Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications**, 25 May 2018.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content**, 14 March 2017.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)**, 24 April 2017.

FLAQUER RIUTORT, J. Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy). **Revista Aranzadi de Derecho y Nuevas Tecnologías**, Pamplona, v. 47, [s.p.], 2018.

GARCÍA MEXÍA, P.; PERETE RAMÍREZ, C. Internet, el RGPD y la LOPDGDD. En: **La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD**. Madrid: Bosch Wolters Kluwer, 2019.

GIOBBI, M. Home banking y tutela de los datos personales. En: PÉREZ GALLARDO, L. (Coord.). **Contratación electrónica y protección de los consumidores – una visión panorámica**. Madrid: Reus, 2017.

GT29. **Dictamen 6/2014, sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE**, 9 abril 2014.

GT29. **Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679**, WP259.

KEITH, M.; LOWRY, P. B.; EVANS, C.; BABB, J. Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure. **International Conference on Information Systems**, Auckland, 2014.

LLÁCER MATACÁS, M. R. **La autorización al tratamiento de información personal en la contratación de bienes y servicios**. Madrid: Dykinson, 2012.

MARTÍNEZ MARTÍNEZ, R. El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto. En: GARCÍA MAHAMUT, R.; TOMÁS MALLÉN, B. (Ed.). **El Reglamento General de Protección de Datos.** Un enfoque nacional y comparado. Valencia: Tirant lo Blanch, 2019.

MATO PACIN, M. N. Deber de transparencia material en la contratación de préstamos hipotecarios con consumidores en el ordenamiento jurídico español. **Revista Boliviana de Derecho**, Bogotá, n. 27, p. 188-219, 2019.

MATO PACÍN, M. N. Los contratos de redes sociales como contratos mediante condiciones generales. En: ALONSO PÉREZ, M.T.; HERNÁNDEZ SÁINZ, E. (Dir.). **Servicios, condiciones generales y transparencia**. Pamplona: Aranzadi, 2020.

METZGER, A. Data as Counter-Performance. What rights and duties do parties have?. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, Berlin, v. 8, n. 1, p. 1-8, 2017.

MIRALLES LÓPEZ, R. Protección de datos desde el diseño y por defecto (Art. 25). En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018.

ORTIZ LÓPEZ, P. Cookies, fingerprinting y la privacidad digital. En: LÓPEZ CALVO, J. (Coord.). **El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos**. Madrid: Wolters Kluwer, 2018.

PUENTE ESCOBAR, A. Principios y licitud del tratamiento. En: RALLO LOMBARTE, A. (Dir.). **Tratado de protección de datos**. Valencia: Tirant lo Blanch, 2019.

SCHULZE, R.; STAUDENMAYER, D. Digital Revolution – Challenges for contract law. En: SCHULZE, R.; STAUDENMAYER, D. (Eds.). **Digital revolution: challenges for contract law in practice**. Baden-Baden: Nomos, 2016.

SEINEN, W.; WALTER, A.; VAN GRONDELLE, S. Compatibility as a mechanism for responsible further processing of personal data. En: MEDINA, M. et al (Ed.). **Privacy technologies and policy**. Switzerland: Springer, 2018.

SEUFERT, E. B., **Freemium Economics: leveraging analytics and user segmentation to drive revenue**. Massachusetts: Morgan Kaufmann, 2014.

SUSSER, D. Notice after notice-and-consent: Why privacy disclosures are valuable even if frameworks aren´t. **Journal of Information Policy**, Pensilvânia, v. 9, p. 37-62, 2019.

TRONCOSO REIGADA, A. Del principio de seguridad de los datos al derecho a la seguridad digital. **Economía Industrial**, Madrid, n. 410, p. 127-151, 2018.

VILASAU SOLANA, M. El consentimiento general y de menores. En: RALLO LOMBARTE, A. (Dir.). **Tratado de protección de datos**. Valencia: Tirant lo Blanch, 2019.