CONSENTIR SIN ENTENDER: EL FRACASO DEL LENGUAJE EN LA PROTECCIÓN DE DATOS Y SUS CONSECUENCIAS PARA EL EJERCICIO PROFESIONAL

Resumen / Abstract

El presente trabajo sostiene que el principal déficit del sistema de protección de datos vigente no es de naturaleza normativa sino comunicativa. El Reglamento General de Protección de Datos (RGPD, Reglamento UE 2016/679) articuló un modelo de consentimiento ambicioso, fundado en la autonomía informada del interesado, pero la práctica cotidiana ha derivado en una liturgia formal que escasamente cumple la función que le fue encomendada. Las políticas de privacidad son documentos técnicamente exhaustivos e intelectualmente inaccesibles; los banners de cookies han mutado en artefactos de ingeniería persuasiva; los sistemas de inteligencia artificial añaden una capa adicional de opacidad que el marco normativo actual afronta con dificultad. El artículo analiza estas patologías desde una perspectiva que integra el rigor jurídico con las aportaciones de la comunicación, la economía conductual y el diseño de decisiones, y propone un conjunto de reformas orientadas a restaurar la sustancia del consentimiento. Se aborda, asimismo, el impacto de esta crisis comunicativa sobre el ejercicio profesional de la abogacía especializada en privacidad, que se ve compelida a operar en un espacio donde la forma ha desplazado al fondo.

Palabras clave: consentimiento informado; RGPD; lenguaje jurídico; privacidad by design; dark patterns; inteligencia artificial; ejercicio profesional.

I. Introducción: el consentimiento como promesa incumplida

Pensemos por un momento en una experiencia que cualquier usuario de Internet repite varias veces al día, con una mezcla de resignación y automatismo que ya no genera ningún tipo de reflexión: el clic sobre el botón que acepta la política de privacidad. Lo hace sin leerla. Sin entenderla. Sin que en realidad quiera hacerlo, porque sabe, con una certeza construida a base de repetición, que ese documento no ha sido escrito para ser comprendido sino para ser aceptado.

Esta escena banal encierra, si se examina con detenimiento, una contradicción de fondo que afecta a los pilares del sistema europeo de protección de datos. El RGPD fue diseñado sobre la premisa de que el consentimiento, cuando se presta, expresa una decisión genuina, consciente y libre de una persona sobre el tratamiento de su información personal. La Directiva 95/46/CE ya había configurado el consentimiento como eje del sistema, pero el Reglamento de 2016 lo elevó a una categoría más exigente: debía ser inequívoco, específico, informado y libre. Cuatro adjetivos que, en la práctica cotidiana, han quedado reducidos a una ficción jurídica de notable sofisticación formal y escasa eficacia material.

La paradoja es llamativa. Nunca antes habíamos contado con una normativa tan detallada sobre la forma en que debe informarse al ciudadano sobre el uso de sus datos. Nunca antes, tampoco, esa información había sido tan poco comprendida por sus destinatarios. El derecho a la protección de datos, que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce como derecho fundamental autónomo, se encuentra en una situación singular: es formalmente garantizado por normas exhaustivas y materialmente erosionado por una práctica comunicativa que sistemáticamente convierte la información en ruido.

Este artículo no pretende ser un análisis exhaustivo del régimen del consentimiento en el RGPD, ni una catalogación de sanciones impuestas por las autoridades de control, que ciertamente hablan por sí solas. Su pretensión es más modesta en apariencia y más

ambiciosa en el fondo: identificar el lenguaje y el diseño como el verdadero campo de batalla de la privacidad contemporánea, analizar las consecuencias de esa crisis comunicativa sobre la eficacia real del sistema y reflexionar sobre las implicaciones que todo ello tiene para quienes ejercemos la abogacía especializada en esta materia. Porque los abogados de privacidad somos, en buena medida, traductores de un idioma que nadie entiende. Y esa posición nos obliga a pensar con seriedad sobre si el edificio que ayudamos a construir cumple su función.

II. El consentimiento en el RGPD: arquitectura normativa y tensiones internas

El RGPD dedica una atención extraordinaria al consentimiento como base de legitimación del tratamiento. El artículo 6.1.a) lo reconoce como una de las seis bases jurídicas posibles, pero es el artículo 7, en combinación con el considerando 32, el que define las condiciones de su validez. A ellos se añaden los artículos 12 a 14, que regulan la transparencia y los deberes de información, formando un conjunto normativo que aspira a garantizar que el interesado sepa, antes de consentir, qué se hace con sus datos, con qué finalidad, por cuánto tiempo, con quién se comparten y qué derechos puede ejercitar.

La lectura de estos preceptos produce, en quien los aborda por primera vez desde el lado del cumplimiento, una impresión de robustez y coherencia. El sistema parece bien articulado: el responsable debe informar, el interesado debe comprender, el consentimiento debe ser libre y específico, y puede revocarse en cualquier momento sin consecuencias desfavorables. Todo encaja en la teoría.

Sin embargo, una observación más atenta revela tensiones internas que el propio Reglamento no resuelve de forma satisfactoria. La primera y más relevante afecta a la relación entre la completitud informativa exigida y la comprensibilidad que el mismo Reglamento reclama. El artículo 12.1 dispone que la información se facilitará "de forma

concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo". Este mandato de claridad convive con una lista de contenidos obligatorios —en los artículos 13 y 14— que, si se cumple íntegramente, produce documentos de extensión considerable y densidad técnica difícilmente compatible con la sencillez exigida. La contradicción no es menor: cuanta más información se incluye para satisfacer el deber de transparencia, más difícil resulta que esa información sea genuinamente inteligible.

La segunda tensión concierne a la gratuidad del consentimiento. El artículo 7.4 establece que, al evaluar la libertad del consentimiento, debe tenerse muy en cuenta si la ejecución de un contrato se supedita al consentimiento para el tratamiento de datos que no son necesarios para su ejecución. El considerando 43 añade que el consentimiento no se presumirá libre cuando exista un desequilibrio claro entre el interesado y el responsable del tratamiento. Estos preceptos son bienintencionados, pero encuentran un límite práctico en la estructura de la economía digital: la inmensa mayoría de los servicios en línea se ofrecen de forma aparentemente gratuita a cambio, precisamente, del tratamiento de datos personales con fines publicitarios. En ese modelo, negar el consentimiento significa, en la práctica, no acceder al servicio. La libertad, en tal contexto, es más una categoría formal que una realidad sustantiva.

El Tribunal de Justicia de la Unión Europea ha tenido ocasión de pronunciarse sobre algunas de estas cuestiones. La sentencia de 4 de julio de 2023 en el asunto C-252/21 (Meta Platforms) estableció criterios relevantes sobre la licitud del tratamiento de datos con fines publicitarios por parte de redes sociales dominantes, señalando que la posición dominante de una plataforma puede afectar a la libertad del consentimiento y que el interés legítimo no puede invocarse sin una ponderación genuina. La sentencia de 11 de noviembre de 2020 en el asunto C-61/19 (Orange România) había precisado, por su parte, que el consentimiento no puede presumirse del mero comportamiento pasivo del usuario y que la carga de demostrar que se prestó recae sobre el responsable. Son pronunciamientos importantes, pero que actúan sobre los efectos del problema sin alcanzar su raíz comunicativa.

III. El lenguaje jurídico como problema estructural

La crítica al lenguaje jurídico tiene una historia larga. Desde los movimientos del Plain Language de los años setenta hasta las más recientes iniciativas de comunicación clara en el derecho administrativo y procesal, el debate sobre la accesibilidad del discurso legal no es nuevo. Lo que sí resulta novedoso, o al menos más urgente, es el contexto en que ese problema se manifiesta en el ámbito de la privacidad: millones de personas son destinatarias cada día de documentos jurídicamente obligatorios cuya comprensión es condición normativa para que una base de tratamiento sea válida. La escala es inédita y los fallos estructurales, también.

Una política de privacidad cumple, simultáneamente, dos funciones que no siempre son compatibles entre sí. Desde la perspectiva del responsable del tratamiento, es un escudo frente a responsabilidades regulatorias y litigios: debe ser completa, técnicamente precisa y capaz de resistir el escrutinio de una autoridad de control o un tribunal. Desde la perspectiva del interesado, debería ser una ventana comprensible hacia lo que ocurrirá con su información. La primera función tiende a producir textos extensos, técnicos y llenos de cautelas. La segunda exigiría documentos breves, directos y escritos en un registro accesible. Cuando ambas funciones se confían al mismo documento, la que predomina siempre es la primera, porque los incentivos de quien redacta apuntan en esa dirección: el abogado que aconseja al responsable tiene un interés profesional en que el texto sea completo y blindado, no en que sea leído con placer.

El resultado de esta tensión es un género textual reconocible y omnipresente: la política de privacidad estándar. Un documento que comienza con afirmaciones de compromiso con la privacidad del usuario, continúa con una descripción de categorías de datos en términos abstractos ("datos de uso", "datos de comportamiento", "datos inferidos"), avanza por definiciones de términos técnicos copiadas del propio RGPD y concluye con una letanía de

derechos ejercitables que el interesado puede solicitar a través de formularios de dudosa accesibilidad. Todo ello redactado en un registro formal que combina la sintaxis administrativa con la terminología técnica del sector digital.

Estudios empíricos repetidamente citados en la literatura académica, aunque sus cifras exactas varían según metodología y año, convergen en un diagnóstico común: el tiempo necesario para leer todas las políticas de privacidad con las que un usuario promedio interactúa en un año supera con creces el tiempo disponible para ello. Más relevante aún es el nivel de comprensión lectora exigido por estos documentos, que investigadores como Lorrie Faith Cranor y su equipo de Carnegie Mellon identificaron como consistentemente superior al correspondiente a un lector universitario medio. El estándar de inteligibilidad que el RGPD impone mediante el mandato de "lenguaje claro y sencillo" del artículo 12.1 es, en la práctica, ignorado de forma sistemática sin que ello genere consecuencias sancionadoras proporcionales a su extensión.

Hay algo más profundo que la mera complejidad léxica. El lenguaje de la privacidad corporativa ha desarrollado una forma particular de eufemismo que merece atención específica. Cuando una empresa declara que "comparte datos con socios de confianza para mejorar la experiencia del usuario", está describiendo, en un vocabulario neutro y amable, algo que en términos más precisos podría formularse así: sus datos de navegación, compras y comportamiento son cedidos a terceros con fines publicitarios que en ningún caso controla usted. La brecha entre ambas formulaciones no es solo estilística; es epistemológica. El primero oculta la información relevante bajo una capa de benevolencia retórica. El segundo la revela de forma que podría generar una reacción informada. Las políticas de privacidad están escritas, sistemáticamente, en el primero de esos registros.

Esta observación tiene consecuencias jurídicas directas. Si el consentimiento válido requiere que sea informado —y el RGPD no admite otra interpretación—, entonces un consentimiento prestado sobre la base de un documento que oculta mediante el lenguaje lo que pretende

revelar mediante la forma podría cuestionarse en su validez. No se trataría de un defecto formal sino de un vicio en la formación de la voluntad: el interesado no sabe realmente a qué está consintiendo. Esta línea argumentativa, de notable fertilidad jurídica, apenas ha sido explorada de forma sistemática en la litigación española, aunque algunas resoluciones de autoridades de control europeas apuntan en esa dirección al sancionar la falta de claridad como incumplimiento autónomo de las obligaciones de transparencia.

IV. El consentimiento como acto formal vacío: anatomía de un fracaso

La tesis del consentimiento formal vacío parte de una constatación empírica difícilmente rebatible: la inmensa mayoría de los usuarios que "aceptan" una política de privacidad no han leído el documento que aceptan, no comprenden sus implicaciones principales y, en muchos casos, no tienen conciencia clara de que están autorizando algo específico. Esto no es una patología de usuarios poco sofisticados; afecta, en proporciones similares, a profesionales del derecho, expertos en tecnología y académicos especializados en privacidad. La razón no es la ignorancia sino la racionalidad: ante un coste de lectura y comprensión que supera con claridad el beneficio esperado de leer, la decisión racional es no leer.

Este fenómeno ha sido analizado desde la economía conductual bajo el concepto de "fatiga del consentimiento", estrechamente relacionado con la noción de "sobrecarga de información" acuñada por investigadores como Barry Schwartz en el contexto más amplio de la paradoja de la elección. Cuando el número de decisiones de privacidad que un usuario debe tomar supera su capacidad cognitiva de procesamiento, el comportamiento resultante no es la elección informada que el RGPD presupone, sino la aceptación reflexiva mínima que permite continuar con la tarea que se tenía entre manos. El clic sobre "Aceptar" no expresa una preferencia; expresa un deseo de que la pantalla de la cookie desaparezca.

La Agencia Española de Protección de Datos (AEPD) y el Comité Europeo de Protección de Datos (CEPD, en sus directrices sobre cookies y consentimiento de 2020 y sus actualizaciones posteriores) han abordado parcialmente estas cuestiones en el contexto específico de las cookies, estableciendo requisitos sobre el diseño de los banners: rechazo tan sencillo como la aceptación, ausencia de opciones preseleccionadas, posibilidad de revocar en todo momento. Son prescripciones pertinentes que sin embargo no atacan el problema de raíz, porque actúan sobre la interfaz sin modificar la comprensión que el usuario tiene de lo que está decidiendo.

El problema de la vacuidad formal del consentimiento tiene una dimensión adicional que conviene explicitar: la asimetría radical de información entre el responsable del tratamiento y el interesado. El primero sabe exactamente qué datos recopila, cómo los procesa, a quién los cede y qué valor económico extrae de ellos. El segundo tiene acceso, en teoría, a toda esa información a través de la política de privacidad. Pero "tener acceso" y "comprender" son cosas radicalmente distintas, y el sistema jurídico ha tendido a confundirlas. La teoría clásica del contrato asume que quien firma un documento ha tenido la oportunidad de leerlo y comprenderlo; el derecho de consumo ha matizado esta presunción introduciendo mecanismos de control de cláusulas abusivas y deberes reforzados de información precisamente porque reconoce que la igualdad formal entre las partes no produce igualdad real cuando existe asimetría informativa o de poder. El derecho de protección de datos comparte este diagnóstico en su exposición de motivos pero no siempre extrae de él consecuencias suficientemente radicales en su articulado.

V. Impacto en el ejercicio profesional de la abogacía de privacidad

Los abogados especializados en protección de datos operamos en un ecosistema en el que las patologías descritas tienen consecuencias directas y, en ocasiones, contradictorias sobre nuestra práctica profesional. Somos, a un tiempo, parte del problema y agentes potenciales

de su solución, lo que exige un ejercicio honesto de autocrítica colectiva antes de formular propuestas.

Cuando asesoramos a empresas en materia de cumplimiento, participamos en la redacción de esas políticas de privacidad que luego nadie lee. El mandato de nuestros clientes es, habitualmente, cumplir con el RGPD de la forma más eficiente posible, minimizando el riesgo regulatorio. Ese mandato no incluye, salvo que lo introduzcamos nosotros activamente, un objetivo de comunicación efectiva con los interesados. La consecuencia es que los documentos que producimos son técnicamente correctos e intelectualmente inaccesibles, y esa es exactamente la combinación que perpetúa el fracaso comunicativo que analizamos. No estamos haciendo nada ilegal; podríamos estar haciendo algo insuficiente.

Desde el lado de la defensa de interesados, la crisis comunicativa abre un espacio de litigación que aún no ha sido plenamente explorado en España. Si el consentimiento es inválido porque la información previa era incomprensible o engañosa en su formulación, la base jurídica del tratamiento desaparece y con ella la legitimación para tratar datos. Esta argumentación requiere una acreditación cuidadosa de en qué consiste exactamente la incomprensibilidad del documento en cuestión, pero no es jurídicamente descabellada: el artículo 13 del RGPD impone obligaciones de contenido específico, y su incumplimiento puede invocarse como fundamento de una reclamación ante la AEPD o de una acción civil de cesación. El artículo 82 RGPD, que reconoce el derecho a indemnización por daños y perjuicios causados por el incumplimiento, podría ofrecer un cauce adicional cuando el tratamiento indebido ha producido consecuencias concretas para el interesado.

El ejercicio profesional en materia de privacidad exige también una reflexión sobre el papel del Delegado de Protección de Datos (DPD). La figura del artículo 37 RGPD ha sido frecuentemente configurada como un mecanismo de cumplimiento interno, con funciones de asesoramiento y supervisión que en la práctica se orientan prioritariamente a evitar sanciones antes que a garantizar que los interesados comprendan cómo son tratados sus datos. No hay

en ello ninguna infracción; el DPD cumple las funciones que el Reglamento le atribuye. Pero sería un error pensar que ese enfoque es suficiente cuando la eficacia del sistema depende, en última instancia, de que los ciudadanos puedan ejercitar sus derechos con conocimiento real de causa. Un DPD que incorpora a su función el análisis crítico de la calidad comunicativa de los documentos de privacidad —y no solo su corrección formal— está contribuyendo de forma más genuina al espíritu del RGPD que uno que se limita a verificar que los 13 puntos del artículo 13 están presentes en el texto.

Hay, finalmente, una dimensión deontológica que merece mención. El artículo 4 del Estatuto General de la Abogacía Española de 2021 define como fin esencial de la profesión la defensa de los derechos fundamentales y libertades públicas. La protección de datos personales es, desde la sentencia del Tribunal Constitucional 292/2000, un derecho fundamental autónomo en el ordenamiento español —habeas data—, conectado con la dignidad de la persona y el libre desarrollo de la personalidad. Cuando los instrumentos técnicos del cumplimiento normativo se configuran de tal modo que vacían de sustancia ese derecho fundamental, la abogacía especializada tiene una responsabilidad que va más allá del interés de sus clientes corporativos inmediatos. Reconocer esta tensión es el primer paso para gestionarla con integridad.

VI. Diseño, persuasión y privacidad: los dark patterns como problema jurídico

El diseño de las interfaces digitales no es neutral. Esta afirmación, que hoy resulta casi un lugar común en los estudios de interacción persona-ordenador, tiene consecuencias jurídicas que el derecho de protección de datos solo ha comenzado a explorar de forma sistemática en los últimos años. La noción de "dark pattern" —patrón oscuro o, en la terminología más precisa del CEPD, "patrón de diseño engañoso"— designa aquellas opciones de diseño que explotan sesgos cognitivos para llevar al usuario a tomar decisiones que no tomaría si la interfaz fuera neutral.

En el contexto de la privacidad, los dark patterns más documentados incluyen el enmascaramiento de opciones (presentar la aceptación como el camino de menor resistencia mientras el rechazo requiere múltiples pasos), la interrupción repetida (mostrar el banner de cookies de nuevo tras su rechazo, en la esperanza de que el usuario acabe cediendo), la ingeniería emocional (usar colores, tamaños y formulaciones que asocian la aceptación a aspectos positivos y el rechazo a pérdidas o renuncias) y la sobrecarga deliberada (proporcionar tantas opciones granulares de configuración que el usuario renuncia a gestionarlas y acepta el perfil por defecto). El CEPD publicó en 2022 sus directrices 3/2022 sobre dark patterns en plataformas de redes sociales, ofreciendo un catálogo detallado de estas prácticas y estableciendo que su uso puede comprometer la validez del consentimiento al vulnerar el requisito de libertad del artículo 4.11 RGPD.

La frontera entre el diseño persuasivo legítimo y el dark pattern jurídicamente reprochable no es siempre nítida, y esa imprecisión plantea dificultades tanto para los responsables del tratamiento que deben cumplir la norma como para las autoridades de control que deben aplicarla. Hay casos claros en ambos extremos: un botón de "aceptar todo" en verde vivo junto a un enlace de texto gris que conduce a ocho páginas de opciones granulares constituye un dark pattern; presentar dos opciones visualmente equilibradas con texto igualmente claro en ambas no lo es. Pero entre esos extremos existe un espacio de incertidumbre considerable en el que la evaluación exige un análisis contextual y probabilístico sobre el comportamiento esperado del usuario medio ante ese diseño concreto.

Esta incertidumbre tiene implicaciones relevantes para la práctica profesional. Cuando asesoramos en el diseño de un sistema de gestión de consentimiento (Consent Management Platform o CMP), no basta con verificar que el banner cumple los requisitos formales de la AEPD. Es preciso evaluar si el diseño, en su conjunto, favorece o dificulta una elección genuinamente libre. Esta evaluación requiere conocimientos que van más allá del derecho positivo y se adentran en la psicología del usuario y en el análisis de la arquitectura de elección, en el sentido que Richard Thaler y Cass Sunstein dieron a este concepto en su

trabajo sobre el nudge. El abogado de privacidad que ignora estas dimensiones está entregando un dictamen incompleto.

El Reglamento 2024/1183 del Parlamento Europeo y del Consejo sobre mercados digitales (Digital Markets Act) y la Ley de Servicios Digitales (Digital Services Act, Reglamento 2022/2065) han incorporado prohibiciones específicas sobre determinadas prácticas de diseño de interfaces, aunque sus ámbitos de aplicación y sus definiciones de las conductas prohibidas no siempre se superponen perfectamente con el régimen del RGPD. La intersección entre estas normativas es un campo emergente de notable complejidad técnica que demanda una práctica profesional interdisciplinar.

VII. Inteligencia artificial y opacidad: nuevas formas del problema antiguo

La incorporación de sistemas de inteligencia artificial al tratamiento de datos personales no crea un problema nuevo en términos de principios, pero sí lo agrava en términos de escala e introduce dimensiones de opacidad que el marco del RGPD afronta con dificultad. El derecho a la información del artículo 13 y el derecho de acceso del artículo 15 presuponen que el responsable puede describir de forma comprensible qué hace con los datos. Cuando el "qué" incluye el entrenamiento de modelos de aprendizaje automático, la inferencia de atributos no proporcionados directamente por el interesado o la toma automatizada de decisiones que afectan a la persona, esa descripción se convierte en un ejercicio extraordinariamente difícil.

La opacidad algorítmica tiene dos dimensiones relevantes a estos efectos. La primera es técnica: los modelos de aprendizaje profundo producen resultados que ni sus propios creadores pueden explicar de forma completamente determinista. La segunda es estratégica: las empresas tienen incentivos económicos para no revelar los detalles de sus modelos, que constituyen su principal activo competitivo. El resultado es que las políticas de privacidad que describen el uso de IA tienden a ser o bien tan vagas que no dicen nada útil, o bien tan

técnicas que no son comprensibles para el usuario. En cualquiera de los dos casos, el requisito de información "clara y sencilla" del artículo 12.1 RGPD queda insatisfecho en su dimensión sustantiva.

El artículo 22 RGPD regula las decisiones automatizadas, incluida la elaboración de perfiles, estableciendo el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado que produzcan efectos jurídicos significativos o igualmente significativos sobre el interesado. Este precepto reconoce implícitamente que hay algo cualitativamente diferente en el tratamiento automatizado que exige garantías específicas. Sin embargo, su alcance está limitado por la expresión "basadas únicamente", lo que excluye los supuestos —mayoritarios en la práctica— en que hay una intervención humana nominal o formal que no altera sustancialmente el resultado del proceso automatizado.

El Reglamento 2024/1689, de Inteligencia Artificial (AI Act), que establece un marco horizontal para los sistemas de IA en la Unión Europea, introduce categorías de riesgo y obligaciones de transparencia que se superponen parcialmente con el régimen del RGPD. Los sistemas de IA de alto riesgo —entre los que se incluyen, significativamente, los utilizados en educación, empleo, servicios esenciales y aplicación de la ley— están sujetos a requisitos de información, documentación técnica y supervisión humana que van más allá de lo previsto en el Reglamento de protección de datos. La articulación entre ambos marcos normativos es una tarea que incumbe en primer lugar al legislador europeo, pero que en la práctica deberán resolver los profesionales del derecho en el asesoramiento cotidiano.

Desde la perspectiva del consentimiento, la IA introduce un problema adicional que conviene nombrar con precisión: la inferencia. Los sistemas modernos de tratamiento de datos no solo procesan la información que el interesado proporciona conscientemente, sino que infieren, a partir de ella, atributos que el interesado no ha revelado y en muchos casos no conocería como atribuibles a sí mismo: orientación política inferida a partir de patrones de consumo, estado de salud inferido a partir de búsquedas, situación económica inferida a partir de

comportamiento de navegación. El consentimiento para el tratamiento de los datos primarios no equivale al consentimiento para la generación y uso de estos datos inferidos, pero la cadena causal es tan difusa que resulta prácticamente imposible establecer dónde termina uno y empieza la otra. Las políticas de privacidad rara vez abordan esta cuestión con la claridad que la gravedad del fenómeno exigiría.

VIII. Propuestas de mejora: hacia un consentimiento que merezca ese nombre

8.1. La redacción como obligación de resultado

La primera propuesta es la más directa y, paradójicamente, la menos practicada: tomarse en serio el mandato de claridad del artículo 12.1 RGPD como una obligación de resultado y no de mero procedimiento. En el estado actual de las cosas, el responsable que redacta una política de privacidad extensa y técnica y la denomina "clara y sencilla" no incumple formalmente el Reglamento porque no existe un estándar objetivable de legibilidad. Una reforma deseable pasaría por introducir ese estándar: índices de legibilidad verificables, límites de extensión orientativos, obligaciones de versión simplificada en lenguaje no técnico para los tratamientos principales.

Esta reforma no requeriría modificación del RGPD. Podría articularse a través de directrices vinculantes del CEPD, como las que ya existen sobre otras materias, o a través de normativa de desarrollo nacional. La AEPD, que cuenta con una destacada labor de guías y herramientas prácticas, podría ejercer un liderazgo relevante en esta dirección. Lo que sí exigiría es un cambio de cultura en la práctica profesional: los abogados que redactamos estas políticas debemos asumir que nuestra responsabilidad no termina cuando el documento cumple con la lista de contenidos del artículo 13, sino cuando el documento es genuinamente comprensible para su destinatario.

8.2. Información por capas y documentación dinámica

El enfoque de información por capas —un resumen inicial accesible con enlaces a información más detallada para quienes deseen profundizar— ha sido respaldado por el Grupo de Trabajo del Artículo 29 (hoy CEPD) desde sus primeras directrices y representa un modelo probadamente superior al de la política de privacidad monolítica. Sin embargo, su adopción sigue siendo desigual y su implementación frecuentemente deficiente: el resumen inicial suele ser tan vago que no informa de nada relevante, mientras que la información detallada mantiene toda la complejidad del modelo anterior.

Un paso más ambicioso consistiría en adoptar modelos de documentación dinámica que se adapten al contexto específico del tratamiento: en el momento en que el usuario va a facilitar datos especialmente sensibles, recibe una información específica sobre ese tratamiento concreto. Esta aproximación contextual —que algunos denominan "consentimiento granular en el momento oportuno"— está más alineada con lo que la investigación sobre comunicación efectiva revela acerca del aprendizaje y la comprensión en contextos digitales. Exige, ciertamente, mayor inversión técnica y jurídica en el diseño de los sistemas, pero esa inversión debería verse como parte del coste del cumplimiento normativo real, no como un elemento supererogatorio.

8.3. Repensar el rol del consentimiento en el sistema del RGPD

Una propuesta de mayor calado, que trasciende la práctica profesional individual y apela a la política legislativa, consiste en reequilibrar el peso del consentimiento en el conjunto del sistema del RGPD. Parte de la crisis actual deriva de que el consentimiento ha sido sobreextendido: se le pide que soporte tratamientos para los que es una base jurídica inadecuada, bien porque la asimetría de poder hace que su libertad sea cuestionable, bien porque la complejidad del tratamiento hace que la información previa relevante sea inmanejable.

El RGPD ofrece otras bases jurídicas que en determinados contextos podrían ser más honestas: el interés legítimo del artículo 6.1.f), correctamente ponderado y documentado; la ejecución de un contrato del artículo 6.1.b) cuando el tratamiento es realmente necesario; el cumplimiento de obligaciones legales. Hay en la práctica una tendencia, no siempre justificada, a recurrir al consentimiento porque parece la base más "limpia" y menos discutible, cuando en realidad puede ser la que peor describe lo que realmente ocurre. Un sistema que utiliza el consentimiento selectivamente, reservándolo para los tratamientos en que es genuinamente posible una decisión libre e informada, sería más honesto intelectualmente y probablemente más eficaz en la práctica.

8.4. Regulación de los patrones de diseño

La regulación de los dark patterns en el contexto de la privacidad debería ir más allá de las directrices del CEPD y traducirse en prohibiciones específicas de conductas concretas, con definiciones operativas que permitan una aplicación consistente. La experiencia de los últimos años muestra que las directrices, aun siendo técnicamente correctas, no producen por sí solas cambios de comportamiento en los responsables del tratamiento cuando los incentivos económicos apuntan en sentido contrario. Se necesita un marco sancionador que haga que el coste esperado del dark pattern sea superior al beneficio esperado de su uso, lo que requiere no solo que las sanciones sean posibles en abstracto sino que sean aplicadas con regularidad y en proporciones que guarden relación con el tamaño y los beneficios del infractor.

8.5. Formación e interdisciplinariedad en la profesión

La crisis comunicativa de la privacidad es también, en parte, una crisis de formación profesional. Los abogados especializados en protección de datos recibimos una formación centrada en el análisis normativo y la aplicación del derecho positivo, pero escasamente orientada a las ciencias del comportamiento, el diseño de comunicaciones o la psicología del usuario. El ejercicio profesional excelente en este campo requiere hoy una comprensión al

menos funcional de cómo los seres humanos toman decisiones en contextos de información asimétrica, cómo el diseño de las interfaces afecta a esas decisiones y cómo pueden articularse documentos que sean simultáneamente correctos en derecho y comprensibles para sus destinatarios. Los programas de formación especializada —los másters, los cursos de certificación, los programas de formación continua de los colegios— deberían incorporar estas dimensiones con la misma seriedad con que incorporan el análisis de las resoluciones de la AEPD.

VIII bis. La lectura fácil como paradigma: lo que el derecho de la privacidad puede aprender de la discapacidad

Existe un campo del conocimiento que lleva décadas resolviendo exactamente el problema que tenemos. No en el derecho de la privacidad, sino en un territorio aparentemente alejado: la comunicación con personas con dificultades de comprensión. Y la solución que ese campo ha desarrollado es tan pertinente para nuestro debate que resulta llamativo que nadie la haya trasladado formalmente a él.

Se llama lectura fácil. Plena Inclusión, organización de referencia en España en materia de discapacidad intelectual, la define como un "método que recoge un conjunto de pautas y recomendaciones relativas a la redacción de textos, al diseño y maquetación de documentos y a la validación de la comprensibilidad de los mismos, destinado a hacer accesible la información a las personas con dificultades de comprensión lectora". Tiene norma técnica propia en España —la UNE 153101:2018 EX— y respaldo en las pautas europeas de Inclusion Europe. No es una intuición pedagógica ni una simplificación informal: es un método con criterios técnicos codificados, aplicable a cualquier tipo de documento, y con un rasgo que lo distingue radicalmente de todos los intentos institucionales de "escribir claro": la validación la hacen siempre las propias personas a quienes va dirigido el texto, no el experto que lo redactó.

Ese detalle —quién valida— es todo. En el modelo actual de cumplimiento del RGPD, quien decide si una política de privacidad cumple el mandato de "lenguaje claro y sencillo" del artículo 12.1 es el abogado que la redacta, el DPD que la supervisa o, en el mejor de los casos, la autoridad de control que la inspecciona. Ninguno de ellos es el ciudadano que va a leerla. La lectura fácil invierte esa jerarquía: el criterio definitivo de comprensibilidad lo tiene el destinatario, no el emisor. Es un giro copernicano que el derecho de la privacidad no ha dado todavía.

Los documentos a los que se ha aplicado la lectura fácil desmontan el argumento más habitual contra la simplificación. Plena Inclusión tiene publicada la Constitución Española en lectura fácil. Y la Convención de la ONU sobre los Derechos de las Personas con Discapacidad. Y normativa administrativa de notable complejidad técnica. Si esos textos han resistido la adaptación sin perder su función esencial, la afirmación de que una política de privacidad es demasiado compleja para hacerse comprensible no es un argumento: es una decisión. Una decisión de no intentarlo.

Ahora bien, la tensión real existe y en esta reflexión no la vamos a eludir. La lectura fácil estándar —frases de no más de quince o veinte palabras, una idea por párrafo, vocabulario cotidiano, apoyo visual— sacrifica deliberadamente el matiz en favor de la comprensión. En protección de datos hay matices que tienen consecuencias jurídicas reales: la diferencia entre responsable y encargado del tratamiento, entre cesión y comunicación, entre base de legitimación contractual e interés legítimo, no es cosmética. Una versión en lectura fácil que los difumine podría producir un texto más legible y menos informativo que el original.

La solución a esa tensión no es descartar la propuesta. Es precisamente el modelo por capas que la propia Plena Inclusión aplica a sus documentos más complejos y que el CEPD lleva años recomendando en abstracto sin extraer sus consecuencias lógicas: una primera capa obligatoria en lectura fácil —o al menos en lenguaje claro con criterios objetivables— que comunique lo esencial con precisión suficiente; y una segunda capa, completa y técnicamente

exhaustiva, disponible para quien quiera o necesite profundizar. No como alternativa al texto completo. Como puerta de entrada obligatoria a él.

Lo revolucionario de esta propuesta no es técnico. Es político, en el sentido más preciso del término: implica que la primera versión que el ciudadano ve no sea la que protege al responsable del tratamiento ante una inspección, sino la que informa al interesado antes de que consienta. Ese cambio de prioridad es exactamente lo que el artículo 12.1 del RGPD exige y exactamente lo que la práctica actual invierte de forma sistemática.

Hay además una dimensión que va más allá de la técnica y que conecta con algo más profundo. La lectura fácil nació de una pregunta de justicia: ¿por qué las personas con discapacidad intelectual deben quedar excluidas de la comprensión de documentos que les afectan directamente? Trasladada al campo de la privacidad, esa misma pregunta suena así: ¿por qué el ciudadano sin formación jurídica —es decir, la inmensa mayoría de los ciudadanos— debe quedar excluido de comprender realmente lo que autoriza cuando acepta una política de privacidad? La respuesta, en ambos casos, es que no debe. Y que, si el sistema produce sistemáticamente ese resultado, el problema está en el sistema, no en el ciudadano.

Plena Inclusión lleva décadas demostrando que ese problema tiene solución técnica. Lo que falta en el campo de la privacidad no es saber cómo hacerlo. Es decidir que vale la pena hacerlo. Y, llegado el caso, que la norma lo exija.

IX. Conclusión: la forma sin el fondo no es suficiente

El RGPD fue, en su momento, la norma de protección de datos más ambiciosa del mundo. Sigue siéndolo en muchos aspectos. Pero la ambición de un sistema jurídico no se mide solo por la sofisticación de sus enunciados normativos, sino también por la eficacia con que esos enunciados se traducen en realidades vividas por los ciudadanos a quienes están destinados.

Y en ese segundo plano, el de la eficacia material, el sistema del consentimiento muestra grietas que no pueden seguir ignorándose.

El diagnóstico de este artículo no es catastrofista. No sostiene que el RGPD haya fracasado ni que el consentimiento sea una categoría jurídica irrecuperable. Sostiene, más precisamente, que el sistema ha priorizado la forma sobre el fondo de manera que compromete la genuinidad del acto de consentir, y que esa priorización no es un accidente sino el resultado predecible de incentivos mal alineados: los responsables del tratamiento tienen interés en que los documentos sean completos pero no necesariamente comprensibles; los abogados que les asesoramos tendemos a optimizar para el cumplimiento formal; las autoridades de control, desbordadas por el volumen de trabajo, han concentrado sus recursos sancionadores en las infracciones más graves y más visibles. En ese ecosistema, la calidad comunicativa de las políticas de privacidad ha quedado sistemáticamente desatendida.

La respuesta a este diagnóstico exige intervenciones en varios planos simultáneos. En el plano normativo, la introducción de estándares objetivables de legibilidad y la prohibición específica de determinados patrones de diseño. En el plano de la práctica profesional, una cultura que entienda el asesoramiento en privacidad como un ejercicio de comunicación efectiva además de cumplimiento técnico. En el plano de la formación, la incorporación de perspectivas interdisciplinares que dotan al profesional de herramientas para navegar la dimensión conductual y comunicativa de la privacidad. Y en el plano del litigio, la exploración más decidida de las vías de reclamación que ofrece el propio RGPD cuando el incumplimiento de los deberes de transparencia e información afecta a la validez del consentimiento y, con ella, a la legitimidad del tratamiento.

En el fondo, la cuestión es más sencilla de formular de lo que es de resolver: el consentimiento es una promesa que el derecho hace al ciudadano. La promesa de que nadie tratará sus datos sin que él lo decida, sabiendo lo que decide. Cuando esa promesa se mantiene en el

papel mientras se vacía en la práctica, algo importante se pierde: no solo la eficacia de una norma, sino la confianza en que las normas sirven para lo que dicen servir. Y esa confianza, en una sociedad que deposita en las instituciones jurídicas la gestión de sus bienes más valiosos, no es un bien superfluo. Es, en muchos sentidos, la condición de posibilidad del derecho mismo.

Referencias normativas y jurisprudenciales

- 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 (Reglamento General de Protección de Datos).
- Carta de los Derechos Fundamentales de la Unión Europea, artículo 8 (Protección de datos de carácter personal). DO C 326, 26.10.2012.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial).
- Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales (Ley de Servicios Digitales).
- Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Real Decreto 135/2021, de 2 de marzo, por el que se aprueba el Estatuto General de la Abogacía Española.
- TJUE, sentencia de 4 de julio de 2023, asunto C-252/21 (Meta Platforms, Inc. y otros v. Bundeskartellamt).
- TJUE, sentencia de 11 de noviembre de 2020, asunto C-61/19 (Orange România SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal).
- Tribunal Constitucional español, sentencia 292/2000, de 30 de noviembre, sobre el derecho fundamental a la protección de datos (habeas data).
- Comité Europeo de Protección de Datos, Directrices 05/2020 sobre el consentimiento en el sentido del Reglamento 2016/679 (versión 1.1, adoptada el 4 de mayo de 2020).
- Comité Europeo de Protección de Datos, Directrices 03/2022 sobre dark patterns en las plataformas de redes sociales (adoptadas el 14 de marzo de 2022).
- Inclusion Europe y FEAPS (Confederación Española de Organizaciones en favor de las Personas con Discapacidad Intelectual). *Información para todos. Las reglas europeas para hacer información fácil de leer y comprender*. Bruselas: Inclusion Europe, 2009. ISBN 2-87460-127-6. Disponible en: https://www.plenainclusion.org/wp-content/uploads/2021/03/informacion_todos.pdf