Informe PSWG3 de la GPA, sesión 43

Preparado para el WG3 de la GPA sobre privacidad y derechos humanos

Índice

Privacidad y protección de datos como derechos fundamentales: una narrativa

Acerca de este documento

Este documento es un producto del Grupo de Trabajo de Estrategia Política Tres («PSWG3») de la Asamblea Mundial de la Privacidad («GPA»).

El PSWG3 tiene por cometido de desarrollar una narrativa que destaque la relación entre la privacidad y la protección de datos y otros derechos y libertades, basándose en la *Resolución internacional sobre la privacidad como derecho humano fundamental y condición previa para el ejercicio de otros derechos fundamentales*, adoptada en la Conferencia de la GPA de 2019.[1]

Para lograr este objetivo, el PSWG3 elaboró un plan basado en cuatro fases:

1. Investigación y recopilación de información (*fact-finding*).
2. Elaboración de un borrador de narrativa.
3. Recepción de comentarios externos sobre el borrador de la narrativa, y
4. Finalización de la narrativa para su consideración y adopción en 2021.

Queremos agradecer a nuestros colegas de protección de datos de todas las regiones del mundo la aportación de datos vitales, investigaciones esclarecedoras y reflexiones meditadas sobre los resultados que presentamos a continuación. Este esfuerzo no habría sido posible sin su participación, sus aportaciones, sus comentarios y su implicación activa. Entre ellas:

- Dirección Nacional de Protección de Datos Personales, Argentina
- Autoridad Nacional de Protección de Datos, Bélgica
- Oficina del Comisionado de Privacidad de Canadá
- Autoridad Catalana de Protección de Datos, Cataluña
- Consejo de Europa
- Consejo para la Transparencia chileno
- Centro Financiero Internacional de Dubái
- Supervisor Europeo de Protección de Datos
- Agencia de los Derechos Fundamentales de la Unión Europea
- Servicio de Inspección Estatal de Georgia
- Comisionado Federal para la Protección de Datos y la Libertad de Información, Alemania
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México
- Centro Nacional de Privacidad y Protección de Datos, Moldavia
- Oficina del Comisionado de Información y Privacidad, Terranova
- Oficina de Protección de Datos Personales, Polonia
- Autoridad de Protección de Datos de la República de San Marino
- Comisión de Datos Personales, Senegal
- Regulador de la Información, Sudáfrica
- Comisionado Federal de Protección de Datos e Información, Suiza
- *Instance nationale de protection des données personnelles (INPDP),* Túnez
- Oficina del Comisionado de Información, Reino Unido

- Comisión Federal de Comercio, EE. UU.
- Oficina de Información de Victoria, Victoria

También queremos agradecer la contribución vital de los revisores externos y de otros reguladores que comentaron el documento. Fueron, entre otros, los siguientes:

- Comisión Canadiense de Derechos Humanos
- Consejo para la Transparencia chileno
- Consejo de Europa
- Supervisor Europeo de Protección de Datos
- Agencia de los Derechos Fundamentales de la Unión Europea
- Oficina de Inspección Estatal de Georgia
- Oficina del Comisionado de Información y Privacidad, Terranova
- Autoridad de Protección de Datos de la República de San Marino
- Oficina de Información de Victoria, Victoria
- Miembros de la Mesa de Referencia de la Asamblea Mundial de la Privacidad (Amber Sinha, Colin Bennett, Clarisse Girot, Estelle Masse y Valeria Milanes)**.**

Por último, queremos agradecer y reconocer el inestimable esfuerzo de investigación, análisis y redacción de las profesoras Orla Lynskey y Judith Rauhofer, cuyo pensamiento y síntesis han vertebrado este informe. Orla Lynskey es profesora adjunta de Derecho en la LSE y profesora visitante en el *College of Europe* de Brujas. Investiga e imparte docencia en las áreas de protección de datos, derechos digitales y regulación tecnológica. Su investigación actual se centra en los retos jurídicos y políticos que la integración de tecnologías del sector privado en las infraestructuras y la toma de decisiones del sector público plantea. Es editora de International Data Privacy Law y Modern Law Review. Judith Rauhofer es profesora titular y directora adjunta del *Centre for Studies of Intellectual Property and Technology Law* (SCRIPT) de la Universidad de Edimburgo.

1. Resumen ejecutivo

A. Finalidad de la narrativa

En la última década, se han modernizado varios de los principales instrumentos internacionales de protección de datos como, por ejemplo, las Directrices de privacidad de la Organización para la Cooperación y el Desarrollo Económico (OCDE), el Convenio 108 del Consejo de Europa y el marco de protección de datos de la Unión Europea (UE). Al mismo tiempo, las leyes de protección de datos han ido proliferando a escala nacional.[2]

Esta narrativa hace balance de estos acontecimientos y refuerza los argumentos a favor de la adopción de un enfoque de derechos fundamentales en materia de protección de datos y privacidad a escala mundial. Aborda la pregunta «¿Qué protegemos cuando protegemos la privacidad y garantizamos la protección de datos?», y articula la conexión entre estos derechos y otros derechos e intereses, como la dignidad humana, la libertad en general y la libertad de expresión. Por último, identifica los posibles impedimentos para el desarrollo de estos derechos y sugiere cómo pueden superarse, allanando el camino para su refuerzo en las formas jurídicas nacionales e internacionales.

B. Enlaces a la iniciativa del Grupo de Trabajo de la GPA

Centramos nuestro trabajo en la idea de que la privacidad y la protección de datos son derechos humanos universales y fundamentales para nuestra democracia, y lo son también para el ejercicio de otros derechos que valoramos colectivamente en nuestras sociedades. En muchos contextos, son nuestros derechos a la privacidad y a la protección de datos los que permiten el ejercicio significativo de otros derechos fundamentales; por ejemplo, la libertad de creencias políticas, de circulación y de asociación, el ejercicio de los derechos democráticos, la disidencia pacífica o la libertad de conciencia y de expresión.

Así, en los últimos cinco años se ha hecho cada vez más evidente la vulnerabilidad de los procedimientos electorales a la intrusión y la manipulación, lo que demuestra cómo los problemas de la injerencia extranjera, las salvaguardias en línea y los derechos a la privacidad y la protección de datos están profundamente entrelazados. Gobiernos, legisladores, reguladores, empresas y sociedad civil deben colaborar entre sí para hacer frente a estos complejos desafíos.[4]

Cualquiera que sea la motivación, ya no es posible minimizar ni ignorar los complejos riesgos para la privacidad. Hay quienes sostienen que las instituciones deberían hacer más en nombre de las obligaciones legales fundamentales y otros que deberían hacer más para garantizar la protección de los derechos individuales.[5] También hay comentaristas que destacan las obligaciones organizativas para mejorar la rendición de cuentas y la gobernanza, o para innovar con los datos de forma más transparente.[6] Cada uno de estos puntos de vista tiene detractores y defensores. Sin embargo, pese a que los fines y motivaciones de las distintas partes interesadas siguen siendo fluidos, este informe demuestra que la adopción de medidas concretas para salvaguardar la privacidad y la protección de datos es ahora una obligación innegociable en muchas jurisdicciones.

Con nuestro esfuerzo internacional perseguimos hacer balance de estas lecciones y experiencias de todo el mundo, y así comprender mejor cómo la protección significativa de la privacidad es parte integral de otros derechos fundamentales que en sociedades abiertas y libres debemos respetar y fomentar.[7].

C. El porqué de su importancia

En la última década, los avances tecnológicos, las economías digitales emergentes, las redes de datos globalizadas, la gobernanza basada en los datos, los nuevos modelos empresariales y las iniciativas de gobierno digital de gran alcance han hecho de la protección de las libertades civiles un reto complejo y global.

En el centro de estos cambios residen la recopilación e intercambio masivo de datos, la toma de decisiones automatizada y la elaboración de perfiles, por parte tanto de organizaciones públicas como de entidades comerciales privadas. Estas tecnologías y procesos digitales y basados en datos, además de suscitar preocupación por la privacidad como derecho humano, tienen implicaciones para la dignidad humana, la igualdad, la no discriminación y el derecho a la reputación, entre otros.[8] No resulta exagerado afirmar que la llegada de nuevas plataformas, prácticas y tecnologías digitales ha tenido y seguirá teniendo profundos efectos históricos en los individuos y la sociedad.[9] Serán efectos similares a los presenciados en la revolución industrial, o en el período moderno temprano con la proliferación de la imprenta, que condujo a la Reforma, el Renacimiento, el surgimiento del Estado-nación y las nuevas ideas políticas, junto con las guerras y conflictos asociados a esta historia.

El potencial de las herramientas digitales es igualmente transformador.[10] Si bien nos encontramos al principio de esta transformación como sociedad, ya presentamos el nacimiento de una nueva generación de personas en un mundo en que la vida digital es una realidad cotidiana. La gran pregunta sigue siendo cómo la digitalización afectará al individuo y a la sociedad y cómo podemos garantizar que nuestras leyes protejan nuestros valores y derechos a medida que la transformación digital se acelera.[11]

2. Introducción: el porqué de su importancia presente

Dada la multiplicidad de leyes de protección de datos en todo el mundo, y el compromiso existente con la privacidad y la protección de datos como derechos fundamentales en muchos países, podríamos —con razón— preguntarnos por qué esto es importante ahora. Esta narrativa expone los argumentos a favor del reconocimiento del derecho a la privacidad y el derecho a la protección de datos personales en los Estados que aún no reconocen tales derechos. Y, con respecto a los países donde el reconocimiento ya existe, reclama un compromiso renovado y manifiestamente explícito con estos derechos y sus principios subyacentes. El reconocimiento y la reafirmación son urgentemente necesarios para abordar importantes cambios tecnológicos y sociales.

La digitalización cada vez está más presente en nuestras interacciones cotidianas. La tecnología continúa aplicándose de formas que avanzan y promueven nuestros derechos fundamentales en algunos casos, pero que los ponen en riesgo en otros.[12] Tenemos, de ello, un buen ejemplo en la informática afectiva, o tecnología de detección de emociones. Mediante métodos de aprendizaje automático, la «inteligencia artificial emocional» infiere los estados mentales de los sujetos y se aplica a una amplia gama de fines, desde la vigilancia de la seguridad vial de los conductores hasta la publicidad dirigida.[13] La empresa EyeQ, por ejemplo, ofrece una tecnología de reconocimiento de emociones que afirma proporcionar a los minoristas datos en tiempo real sobre las emociones de los clientes y datos demográficos (como el sexo y la edad) «que se pueden utilizar para mejorar el servicio y aumentar la tasa de retención».[14].

Se trata de tecnologías que pueden exacerbar las asimetrías de poder e información entre quienes recopilan y utilizan estos datos y las personas cuyas emociones se miden de esta manera. En particular, existe un potencial obvio para que esta tecnología se utilice para explotar nuestras fragilidades emocionales y debilidades cognitivas. Si bien puede ser difícil reunir pruebas de esta explotación, hay indicios de que ya está teniendo lugar. En 2017, un medio de comunicación australiano informó de que Facebook presentó a los anunciantes la capacidad que poseía para identificar cuándo los adolescentes se sentían «faltos de un impulso de confianza», «inseguros» o «inútiles».[15]

Al considerar cómo regular dicha tecnología, el punto de partida de la legislación basada en el mercado, como es el caso de las leyes de protección al consumidor, que se limita a acuerdos entre «consumidor» y «empresa» y da por hecho que los individuos actúan como agentes racionales al tomar decisiones, será por fuerza deficiente.16 He ahí el punto en que la protección de datos y el derecho a la privacidad deben intervenir.17 La tecnología, en sí misma, por consiguiente, ha cambiado en el sentido de que busca captar y representar nuestras acciones e influir en nuestras conductas. No obstante, también asistimos ahora a un aumento de la presión para «capitalizar» estos avances tecnológicos, con independencia de las repercusiones sociales de mayor alcance que hacerlo pueda tener.

En el sector privado, el espíritu de «moverse rápido y romper cosas» personificado por las empresas emergentes de Silicon Valley ha cultivado la percepción de que cualquier forma de regulación, en particular la de los derechos fundamentales, representa un obstáculo para la innovación y frustra la eficiencia.[18] Al hacer de la regulación de la protección de datos y la privacidad un hombre de paja, se facilita la

propagación del mito de que, violando derechos fundamentales como el derecho a la privacidad o la protección de datos y aceptando una nueva realidad en la que se libera el potencial sin explotar de los datos personales, ganaremos todos. Sin embargo, tal y como se argumenta en esta narrativa, solo si se adoptan los principios básicos de la protección de datos y la privacidad, las tecnologías constituirán un progreso social real y serán merecedores de personas y consumidores y se seguirán respetando nuestros valores sociales, democráticos y éticos vigentes.

Por supuesto, ciertas escuelas de pensamiento discrepan de esta formulación. Por razones de aceleración de la innovación o de limitación de la responsabilidad legal, por ejemplo, muchos comentaristas insisten en la responsabilidad social corporativa y en los modelos de gobernanza (anteponiéndolos a las obligaciones fundamentales en materia de derechos humanos) al abordar los problemas de privacidad.[19] La industria tecnológica ha sostenido argumentos similares durante décadas, junto con el rechazo de una regulación restrictiva. En otro extremo del debate, investigadores respetados se centran en el poder, los privilegios y la vigilancia como control social, en lugar de centrarse en los derechos de privacidad individualizados. Ambos grupos presentan argumentos legítimos.[20] Sin embargo, aunque el beneficio y el poder son claramente factores legítimos, los reguladores consideran que muchos de los términos (por ejemplo, responsabilidad demostrable) y conceptos (por ejemplo, supervisión independiente) de estas voces son complementarios, compatibles.

Contrapunto: privacidad, tecnología y protección de derechos

No todos los ejemplos de digitalización y progreso de las tecnologías han socavado la privacidad, y cabe señalar que algunos avances recientes en tecnologías que mejoran la privacidad han contribuido significativamente a la protección de los derechos humanos. La verificación multifactorial de la identidad (como protección contra el registro de dispositivos), las herramientas de anonimización (como contramedida al bloqueo de contenidos en Internet) y el cifrado de extremo a extremo (como medida contra la vigilancia gubernamental), entre otras tecnologías, nos presentan ejemplos concretos en los que las tecnologías digitales ofrecen ahora protecciones muy reales y tangibles contra los riesgos para la privacidad. Un ejemplo de estas tecnologías de cifrado de extremo a extremo nos lo ofrecen las redes privadas virtuales. Con el término redes privadas virtuales, o «VPN», se hace referencia a las tecnologías que permiten a los usuarios acceder a internet de forma segura y privada. Pueden cifrar el dispositivo de comunicaciones de un usuario y redirigir sus datos de red (normalmente una dirección IP), a través de un canal seguro, a los servidores extranjeros del proveedor de servicios VPN, enmascarando así la dirección IP del usuario. De esta forma, las VPN pueden permitir a los usuarios eludir la censura en internet y las interrupciones en las redes sociales provocadas por los gobiernos nacionales. Gracias a esta tecnología de preservación de la privacidad, los usuarios pueden acceder a sitios web bloqueados y, además, coordinar con seguridad movimientos sociales y protestas políticas. Por ejemplo, en 2019, cuando el gobierno egipcio bloqueó el acceso a sitios de redes sociales como Facebook y BBC News en un intento de desalentar las protestas políticas, los ciudadanos egipcios pudieron sortear las interrupciones de los medios sociales mediante el uso de VPN y seguir coordinando las protestas. Las VPN también son de uso común en otras partes del mundo, sobre todo en países donde los gobiernos han impuesto restricciones a internet. Su uso y popularidad destaca la relación entre privacidad, protección de datos y derechos humanos, ya que animan y permiten a la gente ejercer su derecho a protestar.

Fuentes: *La vigilancia y los derechos humanos: Informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (mayo de 2019);*
L. Gill, T. Israel, C. Parsons, Shining a Light on the Encryption Debate (2018); «Ensuring Human Rights for Digital Citizens» (29-37) del informe Global Commission on Internet Governance (June 2016); Katherine Barnett, «The impact of social media on modern protest movements and democracy», The Sociable, 20 de septiembre de 2019. https://sociable.co/social-media/impact-social-media-modern-protest-movements-democracy/

La confianza y la transparencia continúan siendo un tema recurrente en todas estas subliteraturas, al igual que la cuestión de cómo priorizamos y regulamos las cuestiones tecnológicas.
Gobiernos y organismos públicos han manifestado una voluntad clara y persistente de abordar los problemas sociales con soluciones tecnológicas basadas en datos.21 La ventaja de acudir a la tecnología para crear soluciones para las dificultades sociales es la eficiencia que se le percibe (en cuanto a coste y rendimiento), así posibilidad de que la soluciones automatizadas se auditen y sean coherentes.22 A ello podemos añadir la reticencia de los estados ante la posibilidad de quedar por detrás en su capacidad de tratamiento de datos, ya que ello sería un impedimento para su ventaja competitiva en la competición geopolítica para la IA en el futuro.23

Estas soluciones tecnológicas fueron el primer recurso de muchos organismos del sector público durante la pandemia de COVID-19. La utilización de un algoritmo para calcular los resultados de los exámenes finales de los estudiantes británicos fue un ejemplo paradigmático. Tal fue el clamor contra su implantación que el primer ministro británico lo tachó de «algoritmo mutante» y se abandonó.24 Aunque se introdujo para contrarrestar las predicciones optimistas de los profesores sobre el rendimiento de sus alumnos en los exámenes, en la práctica, el modelo penalizaba a los centros que ayudaban a los alumnos a mejorar significativamente entre exámenes estatales comparándolos con el rendimiento medio de los centros, y su precisión fue cuestionada.25

Sin embargo, como constató el presidente del *Open Data Institute*, dicha historia únicamente ponía de relieve los problemas en torno a la toma de decisiones automatizada cuando se despliega por el sector público, si bien en otros contextos confidenciales en los que se utiliza surte un impacto igual que los algoritmos basados en el sector privado, pero no atrae la misma atención crítica.26 La falta de transparencia (antes del proceso de despliegue y durante este) se amplifica por la difuminación entre el uso público y el uso privado. En muchos casos, sin ningún escrutinio en el proceso de contratación, el sector público confiará en herramientas desarrolladas, vendidas y ofrecidas a prueba por empresas. Así, se lanzan herramientas antes de debatir públicamente los objetivos y los impactos correspondientes.

El ejemplo expuesto reveló las desigualdades subyacentes en el sistema educativo, por ejemplo, al favorecer sistemáticamente a los alumnos de cohortes más pequeñas frente a los de cohortes más grandes, cuando los primeros eran los más habituales en los colegios de pago. Esto confirma un peligro obvio de este solucionismo tecnológico que trasciende la protección de datos y la privacidad: que las sociedades busquen en la tecnología la forma predeterminada de abordar casi todos los problemas, desde la desigualdad hasta el cambio climático, y desvíen la atención de las causas profundas de estas crisis.27 Si bien estas causas profundas no pueden omitirse, tampoco se debe restar importancia a la capacidad del respeto a la protección de datos y la privacidad para aumentar la confianza en estos sistemas. En cualquier caso, al integrar las desigualdades existentes en las soluciones tecnológicas, nos arriesgamos a perpetuar estos retos en lugar de atajar sus causas.

Durante la pandemia, la prestación de servicios digitales se aceleró tanto en el sector público como en el privado, y las preocupaciones basadas en los derechos con frecuencia se dejaron de lado a raíz de la crisis mundial.28 Si no se controla, los

efectos del crecimiento de esta forma de capitalismo de vigilancia serán profundos y duraderos en muchos sectores. De hecho, podría reducir o incluso anular las anteriores expectativas razonables de privacidad en ámbitos como el trabajo, la educación y la medicina.[29] Ante tales avances tecnológicos y sociales, ahora, más que nunca, es importante que los estados afirmen —o reafirmen y declaren explícitamente en estatutos escritos— su compromiso con la protección de datos y la privacidad.

La afirmación explícita de los derechos en documentos constitucionales o estatutos legales, deja claro a todos los ciudadanos y organizaciones que un derecho está protegido y reconocido en dichas jurisdicciones. Aunque los Estados cuentan con jurisprudencia que afirma o aclara los derechos, esta sigue siendo dominio de abogados y académicos y, por tanto, la afirmación más opaca de un derecho. En la mayoría de las sociedades, el público en general no suele estar al corriente de las decisiones jurídicas y, por lo tanto, no está en posición de plantear inquietudes sobre una violación de sus derechos.
Aunque es jurídicamente sólida, la afirmación judicial no siempre mejora el acceso a la justicia en la práctica ni la protección del derecho a la privacidad.

En conclusión, esta protección no puede dejarse únicamente en manos de organismos públicos no responsables o de las fuerzas del mercado. Es necesaria como control esencial del creciente poder que los datos y las infraestructuras tecnológicas permiten a los agentes públicos y privados ejercer sobre nosotros como individuos, como grupos y como sociedad en conjunto. En último término, queremos garantizar que las personas y la sociedad puedan seguir beneficiándose de los servicios digitales —para socializar, aprender, comprar, interactuar con servicios críticos— dentro del respeto a la protección de datos y la privacidad y otros derechos fundamentales dependientes. Al fin y al cabo, las personas tienen derecho a vivir libres de la vigilancia injustificada del Estado y las empresas.

3. Orígenes del derecho a la privacidad y a la protección de datos

Para ampliar el apoyo internacional al desarrollo de un instrumento jurídico internacional basado en derechos sobre privacidad y protección de datos, es útil explorar primero el alcance y la historia tanto del derecho general a la privacidad como del derecho a la privacidad informativa/protección de datos.

A. El origen del derecho a la privacidad

En las naciones occidentales desarrolladas y en el norte global, la trayectoria del derecho a la privacidad como derecho humano universal ha sido particular. En su acepción cultural original, a menudo, las personas relacionan la idea de privacidad con una dimensión física o un sentido de ubicación, como el hogar, y el nivel de protección depende de cuán accesible sea o deba ser ese lugar para los demás. En un contexto menos tangible, la privacidad también suele considerarse una forma de secreto (lo que significa que deja de existir cuando se comparte el secreto) o de confidencialidad (según la cual una intrusión se define por una violación de la confianza mutua). Esto se demostró hace unos dos mil años, cuando Cicerón escribió su *Tratado de los oficios del Estado* como consejo a su hijo, quien consideraba la posibilidad de hacer carrera en el servicio del Estado romano.[30] Cicerón pidió al miembro más joven de la familia que pensara en lo que los ciudadanos esperamos del gobierno. Pero, en última instancia, ¿para qué se creó el gobierno? ¿Qué esperamos de él?

Formulando tales preguntas a su gobierno, Cicerón ascendió desde el papel de fiscal hasta el de cónsul de Roma. ¿Por qué el derecho romano insistía en distinguir de una forma tan marcada entre las cosas privadas y el espacio personal, frente a las cosas del Estado y la propiedad pública? Concluyó que un gobierno correcto debe proteger la inviolabilidad de las esferas pública y privada. Todavía hoy el razonamiento es vigente: ¿para qué nos hemos dotado de gobierno y ley si no es para tener clara la línea divisoria entre la vida personal de los ciudadanos y los objetivos del Estado?

En consecuencia, el antiguo derecho romano extiende la noción de que, si se quiere proteger de forma significativa la privacidad, el poder del gobierno para invadir la propiedad privada, registrar el espacio privado y confiscar documentos o propiedades privadas debe estar severamente limitado por la ley.[31] Las limitaciones y restricciones a la intrusión y coerción del Estado en la esfera privada sitúan a la privacidad directamente dentro del aparato intelectual que sustenta tanto el debido proceso como el Estado de derecho.

También coinciden el derecho a la privacidad (en particular en las comunicaciones) y el Estado de derecho (en particular sus requisitos de debido proceso) en el hecho de que ambos son reacciones populares específicas ante el problema del poder estatal intrusivo.[32] Si elegimos una vertiente aún más específica del debate jurídico sobre la privacidad, como la privacidad de los documentos y las comunicaciones personales, detectamos aún otros casos de la antigüedad. En particular, en 1215, cuando el rey Juan firmó la Carta Magna, se consagró el derecho personal contra la confiscación o el acceso ilegal del gobierno a las pertenencias personales. Específicamente, la Carta Magna y su cláusula 39, dice:

> *Ningún hombre libre podrá ser detenido o encarcelado o privado de sus derechos o de sus bienes, ni puesto fuera de la ley ni desterrado o privado de su rango de cualquier otra forma, ni usaremos de la fuerza contra él ni enviaremos a otros que lo hagan, sino en virtud de sentencia judicial de sus pares y con arreglo a la ley del reino.*

La *Carta Magna* fue una respuesta del Estado de derecho a las órdenes intrusivas de la Corona, como también lo fue la Cuarta Enmienda de la *Constitución de Estados Unidos.*[33] En su raíz, el Estado de derecho establece diversas condiciones para que el gobierno pueda ejecutar una acción intrusiva o coercitiva. Significa que el gobierno solo puede detener, registrar o confiscar a una persona sus posesiones, propiedades y papeles con un proceso legal, ya sea a través de un juez (el juicio legal) o una promulgación parlamentaria (la ley del país).[34] Teniendo presente el mandato de 800 años de antigüedad de la Carta Magna, nace el debate en torno a las órdenes judiciales, las garantías procesales básicas y las facultades de registro e incautación del gobierno.[35] El hilo conductor se extiende desde el pensamiento de James Madison y Alexander Hamilton en sus *Federalist Papers*, hasta la jurisprudencia de Warren y Brandeis.[36].

Aunque el derecho individual a la privacidad tardó en evolucionar (antes del siglo XVII), el término latino *privatus* distinguía entre los asuntos pertenecientes a la colectividad (y, por tanto, sujetos a la autoridad pública) y los asuntos pertenecientes a una comunidad cerrada (gobernada por un hogar).[37] Según Dianete Shaw, «la afirmación errónea de que la noción de privacidad física estaba ausente en la sociedad medieval quizá derive de la suposición moderna de que la privacidad es individual y absoluta, en lugar de comunitaria y relativa.»[38] Como señala sucintamente David Vincent, la narrativa de la privacidad no es una progresión de la ausencia a la invención, o necesariamente un avance, sino más bien un derecho fundamental que siempre ha apuntalado la comprensión que tenemos de la vida individual y colectiva, cuando «no hay comienzos en esta historia, solo finales amenazados.»[39].

Estos fundamentos históricos occidentales de la privacidad y su interpretación como forma de secreto (lo que significa que la privacidad desaparece cuando se comparte el secreto) o confidencialidad (según la cual una intrusión es una violación de la confianza mutua) permanecieron en gran medida incontestados hasta finales del siglo XIX, cuando Samuel Warren y Louis Brandeis escribieron su ensayo de 1890, *The Right to Privacy*. Para ellos, la privacidad era el «derecho a ser dejado en paz», lo que desafiaba la conceptualización tradicional.[40]

En concreto, el ensayo trataba de identificar una base jurídica para un derecho más activo de los individuos a controlar e impedir la divulgación de sus «pensamientos, sentimientos y emociones», del mismo modo que ya podían excluir a otros de cualquier espacio físico bajo su control (utilizando las normas de allanamiento).[41] Así pues, más allá de nociones como «lugar», «secreto» o «confidencialidad», la novedad de este enfoque radicaba en la ampliación de la esfera protectora de la privacidad. En lugar de limitar el derecho a una dimensión puramente espacial, incluye, entre otras cosas, el derecho del individuo a controlar la información que le concierne.

Esta noción de privacidad como derecho del individuo a controlar la información continuó en el siglo XX, cuando el auge de los regímenes autoritarios y totalitarios en todo el mundo catalizó los esfuerzos por establecer un derecho a la privacidad. En

concreto, se trataba de la capacidad de dichos regímenes para ejercer poder sobre sus ciudadanos como resultado directo de su acceso a información detallada sobre la identidad, los pensamientos, las creencias y las acciones de estos ciudadanos y para influir y controlar su comportamiento en consecuencia.

Tras la Segunda Guerra Mundial, esta experiencia llevó a un reconocimiento ampliamente compartido entre los gobiernos democráticos de que, para mantener la democracia, la privacidad como derecho humano debía establecerse y reconocerse. Así se protegería a las personas de injerencias en su vida privada y familiar, en particular, pero no exclusivamente, por parte de agentes estatales. Para ser claros, reconocemos plenamente que se trata de puntos particularizados del pensamiento liberal tradicional. En algunos casos, ese conjunto específico de experiencias históricas ha moldeado el discurso global sobre la privacidad. Pero esto no debería disipar la preocupación. La privacidad y la protección de datos deben promoverse como derechos universales, a través de instrumentos internacionales, precisamente porque estos riesgos, antaño particularizados, ahora se han «universalizado»: por la libre circulación de datos, las nuevas tecnologías, los modelos empresariales internacionales y la congruencia de las prácticas gubernamentales.

i. El derecho a la privacidad en el ámbito internacional

A escala internacional, la *Declaración Americana de los Derechos y Deberes del Hombre* (DADDH), fue el primer documento en enumerar una lista de derechos, y las naciones de América la adoptaron en mayo de 1948. Ese mismo año, la Organización de las Naciones Unidas (ONU) proclamó la *Declaración Universal de los Derechos Humanos* (DUDH), que establecía amplias protecciones para la privacidad. Según el artículo 12 de la DUDH:

> *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

Al poner en primer plano un concepto general amplio de privacidad, la DADDH y la DUDH allanaron el camino para concepciones más amplias de la privacidad, que van más allá de la privacidad en determinados lugares, como el hogar, o contextos, como la vida familiar. Los instrumentos internacionales posteriores siguieron la tendencia para ampliar la protección de la privacidad. Por ejemplo, en el ámbito regional, la Organización de Estados Americanos (OEA) reconoció el derecho de toda persona «al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o a su reputación», en la *Convención Interamericana de Derechos Humanos (Pacto de San José de Costa Rica)*.

El *Convenio Europeo de Derechos Humanos* (CEDH), adoptado por el Consejo de Europa en 1950 y que entró en vigor en 1953, fue el primer instrumento internacional jurídicamente vinculante que reconocía un derecho general a la privacidad. El apartado 1 del artículo 8 establece el derecho («Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia») antes de identificar las condiciones para limitar este derecho en

el apartado 2 del artículo 8 del CEDH.

Posteriormente, la ONU adoptó el *Pacto Internacional de Derechos Civiles y Políticos* (ICCPR) y un protocolo facultativo que lo acompañaba en 1966.[42] Estos documentos adicionales estaban abiertos a la adhesión y ratificación de los Estados de la ONU y eran vinculantes para los que los ratificaban. El derecho a la privacidad se encuentra en el artículo 17 del ICCPR, en cuya virtud:

> 1. *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
> 2. *Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

Para supervisar el cumplimiento, el Consejo de Derechos Humanos de la ONU (CDH) examina los informes periódicos (que los Estados parte del ICCPR presentan) sobre el cumplimiento de los derechos del ICCPR.[43] Hasta el presente, el CDH ha emitido más de 100 dictámenes relativos al cumplimiento del artículo 17 del ICCPR por los Estados parte.[44] Sin embargo, el carácter jurídico de sus conclusiones o «dictámenes» sigue siendo controvertido.[45] A partir de 2015, también se creó un relator especial de la ONU sobre el derecho a la privacidad, una figura que investiga y publica informes sobre una amplia gama de cuestiones de protección de datos y derechos digitales.[46]

Otro organismo, la Comisión de Derecho Internacional, tiene por misión la que la Carta de la ONU le asigna, la de iniciar estudios y hacer recomendaciones para fomentar «el desarrollo progresivo del derecho internacional y su codificación».[47] La «protección de datos personales en el flujo transfronterizo de información» se incluyó en el programa de trabajo a largo plazo de la Comisión de Derecho Internacional en 1997. Este trabajo resulta de la labor política y los informes de varios relatores especiales relevantes, como los de libertad de opinión y expresión, derecho a la privacidad y derechos del niño. Además, la defensa internacional de los titulares de derechos individuales y de las instituciones nacionales de derechos humanos sigue informando e influyendo en el desarrollo y la interpretación de los instrumentos modernos de derechos y en las revisiones de la ONU. Estos esfuerzos han dado lugar a claros avances (por ejemplo, la DNUDPI) y probablemente desempeñarán un papel clave en el desarrollo futuro de nuevos instrumentos sobre privacidad.

ii. El derecho a la privacidad en el ámbito nacional

En el ámbito nacional, el derecho a la privacidad o a la protección de datos habitualmente se establecía de una de estas cuatro formas:

Disposiciones constitucionales: En primer lugar, los países pueden incluir expresamente el derecho a la privacidad como derecho fundamental en sus constituciones nacionales o cartas de derechos.[48] Si bien no era algo habitual hasta los años 60/70, se trata de un enfoque que ahora, entre otros países, se sigue en México, Suiza, Bélgica, Corea, Filipinas, Hong Kong, Portugal, Colombia, Chile, Trinidad y Tobago y Gabón, varios de los cuales incluyeron posteriormente tales derechos en sus constituciones vigentes.[49] No todos estos países reconocen un derecho general a la privacidad. En cambio, en las constituciones respectivas, pueden incluir derechos que protejan un aspecto específico de la privacidad. Por

ejemplo, la Constitución de las Bermudas protege un derecho muy específico a la protección de la privacidad del hogar y otros bienes personales.[50] En los países con una estructura federal, los derechos a la privacidad o a la protección de datos también pueden incluirse en las constituciones estatales pertinentes, en lugar de en las federales. En Alemania, por ejemplo, las constituciones estatales de todos los «*Nue Bundesländer*» (estados que pasaron a formar parte de la República Federal tras la reunificación entre Alemania Occidental y la RDA en 1990) y de varios de los demás estados incluyen un derecho expreso a la privacidad, la autodeterminación informativa, la privacidad de la información o la protección de datos.[51] En términos similares, el estado australiano de Victoria ha consagrado el derecho a la privacidad en el artículo 13 de la Carta de Derechos Humanos y Responsabilidades de Victoria de 2006.

Legislación específica: abordada de forma detallada en el apartado siguiente («el origen del derecho a la protección de datos»), muchas jurisdicciones crearon, en los años 60 y 70, legislación sectorial específica sobre privacidad o protección de datos. Algunos Estados pueden incluso reconocer explícitamente el derecho en estatutos cuasiconstitucionales; por ejemplo, en códigos de derechos humanos o leyes de privacidad de ámbito nacional.

Jurisprudencia: En los países dotados de constituciones que no incluyen expresamente los derechos a la privacidad o a la protección de datos, los tribunales nacionales pueden, no obstante, establecer tales derechos por referencia o basándose en una combinación de uno o más derechos. Por ejemplo, el Tribunal Constitucional alemán reconoce un «derecho general de la personalidad» así como un «derecho a la autodeterminación informativa» sobre la base del artículo 2, apartado 1 («derecho a la autodeterminación») en relación con el artículo 1, apartado 1 («dignidad humana») de la Ley Fundamental alemana.[52] Canadá protege ciertos aspectos de la privacidad de las personas como parte de los derechos a la libertad y a no ser objeto de registros e incautaciones irrazonables establecidos en los artículos 7 y 8 de la Carta Canadiense de Derechos y Libertades.[53] Similar es el enfoque que se adopta en Estados Unidos, que protege la «expectativa razonable de privacidad» de una persona como parte de las enmiendas cuarta y decimocuarta (protección contra registros e incautaciones irrazonables y garantías procesales). En Japón, los tribunales han interpretado que el artículo 13 de la Constitución (derecho a la búsqueda de la felicidad) incluye el derecho a la privacidad.[54] Más recientemente, en 2017, el Tribunal Supremo de la India dictaminó que la privacidad es un derecho fundamental porque es parte integrante del derecho a la vida y a la libertad personal garantizado en el artículo 21 de la Constitución india. La decisión enmarcaba la privacidad en todo el espectro de derechos fundamentales enumerados por su Constitución y señalaba cómo así se hacen posibles otros derechos como la libertad de expresión, la libertad de asociación, la libertad religiosa y el derecho a la igualdad.[55]

Acuerdos y tratados internacionales: Alternativamente, los países pueden hacer efectivos en el ámbito interno los instrumentos internacionales de derechos humanos de los que son parte, o pueden adoptar esos instrumentos internacionales como derecho interno vinculante, de forma que permitan su aplicación ante los tribunales nacionales. Por ejemplo, los 55 países que son parte del Convenio 108 han adoptado legislaciones que cumplen las disposiciones del Convenio. La Carta de los derechos fundamentales de la UE se aplica directamente en los 27 Estados miembros de la UE cuando adoptan o aplican una ley nacional de transposición de una directiva de la UE o cuando sus autoridades aplican directamente un reglamento de la UE.[56] Austria

concedió retrospectivamente al CEDH rango constitucional nacional en 1964, mientras que el Reino Unido, tras haber sido uno de los signatarios (y redactores) originales del Convenio, decidió finalmente convertirlo en vinculante y aplicable ante los tribunales británicos en 1998.[57] Un enfoque similar adoptó la Isla de Man, una dependencia de la Corona británica, cuando aprobó su Ley de derechos humanos en 2001.

B. El origen del derecho a la protección de datos

A diferencia del derecho a la privacidad, que se introdujo de manera claramente «descendente» como parte de instrumentos de derechos fundamentales, en su mayoría internacionales, podría argumentarse que el derecho a la protección de datos se desarrolló más bien de forma ascendente. Su aparición suele describirse como una respuesta a los avances tecnológicos y al desarrollo de nuevos modelos de negocio basados en el uso intensivo de datos, fruto del deseo de proteger a las personas de sus efectos potencialmente adversos. En particular, tales efectos incluyen la recogida, utilización, almacenamiento, combinación, intercambio y divulgación no autorizados de datos personales de particulares.

Los orígenes contemporáneos de los marcos modernos de la ley de protección de datos se remontan al estado alemán de Hesse, al que se atribuye la adopción del primer instrumento legal de protección de datos, la Ley de protección de datos de Hesse de 1970.[58] Si bien podría decirse que fue el primero en adoptar una ley de este tipo, rápidamente le siguieron otros países, mayoritariamente europeos, incluida, en 1977, la República Federal de Alemania.[59] No había entonces ningún derecho a la protección de datos incluido expresamente en la Constitución alemana ni en ninguna de las constituciones estatales de los «Länder» alemanes, ni en ninguna otra constitución de un país europeo (CE).[60]

Inspirados por esos cambios y conscientes del flujo creciente de datos personales a través de las fronteras políticas, a finales de la década de 1970, los expertos internacionales redactaron dos documentos internacionales: las Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales y el Convenio 108. Este último fue un instrumento multilateral abierto basado en la Convención de Viena sobre el Derecho de los Tratados que allanó el camino para futuras legislaciones nacionales y regionales de protección de datos, incluida la Directiva 95/46/CE de la UE. Fue el primer instrumento multilateral jurídicamente vinculante sobre protección de datos, que sentó las bases de la legislación moderna sobre protección de datos, al exigir a sus estados parte la aplicación de los principios generales de la protección de datos (como el tratamiento de datos leal y lícito, los fines especificados y legítimos, la calidad de los datos y un régimen de flujo de datos transfronterizo), los cuales rápidamente adquirieron influencia, primero entre los Estados miembros del Consejo de Europa y, a partir de 2013, también en otros continentes. Como abanderada mundial de la protección de datos y con su estructura de gobierno regional/nacional/estatal casi federada, la Unión Europea, sirve de ejemplo útil para analizar este «mito de la creación».

Al adoptar su marco global de protección de datos como «derecho derivado»,[61] la UE mencionó expresamente el Convenio 108 declarando que quería «dar contenido» a los principios que figuran en el Convenio 108 y «ampliarlos».[62] La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos («Directiva de 1995») se

adoptó en 1995 como instrumento del mercado común con la intención de armonizar los marcos nacionales de protección de datos de los Estados miembros de la UE que se habían desarrollado en las dos décadas anteriores.[63] La Directiva de 1995 quería dotar de un nivel básico de protección a todos los Estados miembros con el doble objetivo de proteger «los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la privacidad en lo que respecta al tratamiento de datos personales», y facilitar la libre circulación de datos personales entre los Estados miembros en consonancia con los objetivos del Convenio 108.[64]

Entonces, la UE todavía no había adoptado el marco de derechos fundamentales propio. En su lugar, se basó en gran medida en el entendimiento común de los Estados miembros de que los «derechos fundamentales» mencionados en el artículo 1 de la Directiva incluían las disposiciones del CEDH del Consejo de Europa (que todos los Estados miembros habían ratificado), así como los derechos fundamentales protegidos por las constituciones o cartas de derechos nacionales de los Estados miembros. Así pues, la ausencia de derechos fundamentales no impidió a la UE adoptar un marco global de protección de datos basado en gran medida en el Convenio 108. La Carta de los derechos fundamentales de la UE, que ahora incluye un derecho expreso a la protección de datos en el artículo 8, se adoptó como parte del Tratado de Lisboa y entró en vigor el 1 de diciembre de 2009.[65] Este vínculo tan estrecho, incluso simbiótico, basado en principios y valores compartidos entre los dos marcos de protección de datos emergió una vez más cuando ambos se actualizaron mediante una declaración de la Comisión de la UE sobre la adhesión de la UE al Convenio 108+, una vez que entre en vigor.[66]

En el contexto de las Naciones Unidas, el único instrumento de la ONU cuyo objeto específico es la protección de datos es un conjunto de «directrices para la regulación de los ficheros automatizados de datos personales», no vinculantes, que datan de 1990.[67] Como señala Kuner, pese a que la base normativa de la legislación sobre protección de datos depende mayoritariamente de textos internacionales sobre derechos humanos como la DUDH de 1948 y el ICCPR de 1966, estos instrumentos no mencionan específicamente la protección de datos.[68] Así pues, si bien el derecho a la protección de datos se reconoce explícitamente en algunas constituciones nacionales, la Carta de los derechos fundamentales de la UE es el único instrumento internacional existente que reconoce la protección de datos como derecho fundamental distinto.[69] En 2016, con la adopción del Reglamento general de protección de datos (RGPD) y la Directiva de policía, la UE reformó y actualizó su marco de protección de datos. Ambas legislaciones permanecen ancladas en los principios avanzados en el Convenio 108.

i. Esfuerzos actuales para reforzar los derechos a la protección de datos y a la privacidad en el ámbito internacional

Aunque ahora son de reconocimiento generalizado en países de todo el mundo y en el contexto de una variedad de acuerdos constitucionales, podemos ver que la privacidad y la protección de datos siguen estando poco desarrolladas e infrautilizadas a nivel internacional. El derecho a la protección de datos no ha devenido todavía un derecho reconocido a escala internacional. Por lo tanto, no debe sorprender que se reclame un mayor reconocimiento y aplicación de estos derechos a escala internacional.

Constituye ejemplo destacado de este llamamiento a reforzar estos derechos la Declaración de Montreux de 2005, hecha por la Conferencia Internacional de Comisarios de Protección de Datos y Privacidad (ICDPPC, por sus siglas en inglés), ahora conocida como Asamblea Mundial de la Privacidad (GPA, por sus siglas en inglés).[70] A través de la Declaración de Montreux, la ICDPPC señaló la necesidad de «reforzar el carácter universal de este derecho [a la privacidad y la protección de datos] para obtener un reconocimiento universal de los principios que rigen el tratamiento de los datos personales, respetando al mismo tiempo las diversidades jurídicas, políticas, económicas y culturales».[71] La Declaración instaba a la ONU a preparar un instrumento jurídicamente vinculante, que «establezca claramente y en detalle los derechos a la protección de datos y a la privacidad como derechos humanos exigibles»[72] La Resolución de Madrid de la ICDPPC sobre normas internacionales de protección de datos personales y privacidad fue un llamamiento similar, realizado en noviembre de 2009.[73] Posteriormente, a través de la ICDPPC/GPA, intentó redactar un instrumento jurídico mundial sobre protección de datos en 2009 y abogar por la adopción de un 3.er protocolo facultativo del ICCPR para adoptar una norma internacional sobre privacidad coherente con el artículo 17 del ICCPR.[74]

Estos esfuerzos por reforzar los derechos a la protección de datos y la privacidad a escala internacional son todavía trabajos en curso. Ello podría imputarse a la ineficacia de los mecanismos de aplicación existentes y a las diferencias entre los puntos de vista de las diversas jurisdicciones. También podrían influir los desequilibrios de información y poder en los entornos digitales modernos, o el hecho de que las prioridades reguladoras se distribuyan entre una amplia gama de sectores, temas y partes interesadas. Ambos fenómenos dificultan la percepción de los riesgos para la privacidad o impiden el ejercicio efectivo de los derechos. Sin embargo, el camino de la cooperación internacional es cada vez más claro.

En primer lugar, el éxito de la cooperación internacional existente en estos campos ha sido desigual.[75] Esto se debe a una serie de factores. Algunos tienen que ver con las características de los instrumentos de la ONU. Se trata de un mosaico de normas de diversos instrumentos y esta «dispersión normativa» afecta a su accesibilidad y eficacia. Además, por su carácter de derecho indicativo, el CDH no invoca ni aplica muchos de los instrumentos existentes (como las Directrices para la regulación de los ficheros automatizados de datos personales).[76] También se atribuye la falta de utilidad al calendario, ya que las directrices de la ONU pertinentes se adoptaron después de instrumentos internacionales importantes, como las Directrices de privacidad de la OCDE y el Convenio 108 del Consejo de Europa.[77] Sin embargo, incluso en los regímenes de protección de datos que se consideran un éxito desde la perspectiva de los derechos fundamentales, como el RGPD de la UE, persiste la desconexión entre la letra de la ley y su aplicación práctica.[78]

Sin embargo, aunque debe hacerse más para promover y aplicar los marcos internacionales y regionales de protección de datos existentes, también sería erróneo concluir que estos marcos no han carecido de impacto. El Tribunal Interamericano de Derechos Humanos ha desarrollado una importante línea jurisprudencial que establece una visión polifacética del derecho a la privacidad e impone a los estados la obligación positiva de garantizar el respeto de este derecho por parte tanto de las entidades públicas y privadas como de los individuos.[79] Las disposiciones de los acuerdos internacionales, incluidos los instrumentos de la ONU, también suelen tener rango constitucional en las constituciones nacionales. Por ejemplo, la Ley fundamental de la RAE de Hong Kong da efecto constitucional a las disposiciones del ICCPR. Los instrumentos regionales de derechos humanos que reconocen los derechos a la protección de datos y a la privacidad, como la Carta de los derechos fundamentales de la UE, también se han invocado con efectos significativos al impugnar y, en última instancia, invalidar instrumentos legislativos incompatibles.[80] En resumen, aunque mejorar la eficacia de estos marcos jurídicos supranacionales sigue siendo un reto, estos esfuerzos ya están teniendo repercusiones tangibles y merece la pena proseguirlos.

Las diferentes perspectivas también han limitado el reconocimiento de la protección de datos y la privacidad como derechos.[81] Hoy en día, las opiniones sobre esta cuestión no se dividen tan fácilmente en función de líneas geográficas. Muchos agentes empresariales y funcionarios temen que un compromiso firme y continuado con la protección de los derechos fundamentales exija renunciar al progreso tecnológico y comercial. A pesar del rápido crecimiento y el aumento del margen de beneficios en todos los sectores tecnológicos, esta opinión prevalece. Para otros, erróneamente, la privacidad es una «barrera» o un «impedimento» para la innovación. Y también los hay quienes posiblemente solo reconozcan los aspectos comerciales y empresariales de la innovación, desatendiendo una necesidad igualmente urgente de apoyar la evolución social y jurídica.

Esta perspectiva explica en gran parte por qué, «una vez que se desciende del nivel más alto de abstracción, puede haber diferencias significativas en los detalles» entre los enfoques regionales y nacionales de protección de datos.[82]

Diferencias: libertad de expresión en el Reino Unido

Otro punto común de diferenciación entre los estados es su postura ante la libertad de expresión. Normalmente, en aquellos donde existe una sólida tradición jurídica de libertad de expresión, ha habido reticencia a reconocer o desarrollar plenamente el derecho a la privacidad. En Inglaterra y Gales, los tribunales se negaron a desarrollar un derecho a la privacidad sin un respaldo legislativo. Ya en la década de 1990, el Tribunal de Apelación declaró explícitamente que «es bien sabido que en el Derecho inglés no existe el derecho a la privacidad y, en consecuencia, no existe el derecho de acción por violación de la privacidad de una persona». Sin embargo, este ejemplo también ilustra que, una vez que el derecho a la privacidad se reconoce en un ordenamiento jurídico nacional, como ocurrió en el Reino Unido con la Ley de derechos humanos de 1998 y, en última instancia, por la Cámara de los Lores en su sentencia Campbell de 2004, puede afianzarse rápidamente y convertirse en una parte establecida del panorama jurídico. Los impedimentos culturales e ideológicos a la cooperación son, por tanto, superables. En consecuencia hay margen para el optimismo en cuanto a las posibilidades de desarrollar los derechos a la privacidad y a la protección de datos a escala internacional. **Fuentes:** *Kaye v Robertson* [1991] FSR 62, de Glidewell LJ; *Campbell v Mirror News Group* (MGN) [2004] UKHL 22.

Para el desarrollo y la aplicación de instrumentos regionales de protección de datos y privacidad, podemos diferenciar dos enfoques. Uno de ellos se basa principalmente en el reconocimiento de las implicaciones de los derechos fundamentales del tratamiento de datos personales (como el Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales, el Convenio 108 y el RGPD). Para el otro, los datos son *una mercancía esencial*, un activo comercial o un insumo para bienes y servicios y, por tanto, trata de maximizar su potencial para el intercambio y el comercio minimizando las fricciones normativas (como las *Directrices de Privacidad* de la OCDE y el *Marco de Privacidad* de la APEC). En la práctica, estos regímenes difieren en cinco aspectos importantes.

En primer lugar, la interpretación de los marcos basados en los derechos se guía por el razonamiento de los derechos fundamentales (incluida, por ejemplo, la incorporación de evaluaciones de necesidad y proporcionalidad). En cambio, los enfoques basados en el mercado incluyen supuestos basados en el mercado (como el paradigma de «notificación y elección»). En segundo lugar, los marcos basados en derechos conceden derechos a las personas (los titulares de derechos) como, entre otros, el derecho de acceso, el derecho a obtener la supresión de datos personales y el derecho a oponerse a su tratamiento.
Se trata de derechos que se correlacionan con deberes que los Estados y las entidades privadas (los titulares de deberes), para respetarlos, deben cumplir. Están ausentes o son menos prominentes en los regímenes orientados al mercado. En tercer lugar, los regímenes basados en derechos suelen estar respaldados por estatutos vinculantes y mecanismos de ejecución aplicados por una autoridad independiente con un aspecto de derecho público.

Este sistema basado en los derechos reconoce tanto que una violación de los derechos individuales es un perjuicio para el bien público como que existe un interés público en proteger, hacer cumplir y promover estos derechos exigiendo responsabilidades a quienes los violan. Mientras que en los enfoques basados en el mercado, la rendición de cuentas se plantea más a menudo en forma de acciones de derecho privado, como la resolución de litigios comerciales, o demandas en virtud de la jurisprudencia sobre contratos o agravios. Por último, un enfoque basado en los derechos reconoce el derecho inherente a la dignidad de los ciudadanos, y aborda explícitamente los desequilibrios de poder para proteger a los menos poderosos de los daños, mientras que un enfoque de mercado privado a menudo ignora los desequilibrios de poder y asume que los daños se calcularán automáticamente en el coste de un bien o servicio a través de las fuerzas del mercado.

No obstante, queda todavía margen para la convergencia entre estas lógicas ostensiblemente distintas. El respeto de la protección de datos y la privacidad suele ser un requisito legal previo para la liberalización de los flujos de datos personales, lo que difumina los límites entre los enfoques basados en el mercado y los enfoques basados en los derechos. Del mismo modo, el respeto de estos derechos es también un requisito previo para garantizar la confianza de los usuarios en los usos innovadores de los datos. Por lo tanto, del mismo modo que promover el respeto de los principios medioambientales contribuye a garantizar la sostenibilidad a largo plazo, promover el respeto de la protección de datos y la privacidad puede contribuir a garantizar la innovación sostenible.

C. ¿Qué es la protección de datos y en qué se diferencia de la privacidad?

Como se ha señalado anteriormente, en comparación con el derecho a la privacidad, el origen de la protección de datos como derecho y su carácter preciso y fundamental es un poco más reciente.[83] Desde la primera introducción, en los años setenta y ochenta, del derecho a la protección de datos en las constituciones nacionales, tribunales y académicos han tenido dificultades para identificar líneas de demarcación claras entre ambos derechos. No favorece la situación el hecho de que, aunque el derecho a la protección de datos aparece ahora en un número creciente de constituciones nacionales y estatales, la Carta de la UE sea, hasta la fecha, el único instrumento jurídico internacional que diferencia explícitamente entre los derechos a la protección de datos y a la privacidad.[84]

Los instrumentos jurídicos nacionales e internacionales que incluyen expresamente un derecho a la protección de datos comparten una serie de rasgos comunes.[85] Más notablemente, los que protegen específicamente el derecho a la protección de datos suelen exigir la creación de una autoridad de supervisión independiente para hacer cumplir esos derechos y obligaciones.[86] La naturaleza procedimental de este enfoque ha llevado a algunos a argumentar que, a diferencia del derecho a la privacidad, el derecho a la protección de datos no es tanto un derecho sustantivo como un derecho procedimental que, en última instancia, hace efectivo el derecho a la privacidad de la información mediante el establecimiento de un conjunto de normas detalladas para su desempeño.[87] Para decidir si esto es cierto, es preciso un análisis pormenorizado del carácter específico del derecho a la protección de datos y de cuál debe ser el objeto de su protección según se ha diseñado.

i. La relación entre la protección de datos y la privacidad

Persiste en algunos expertos la duda acerca de si la protección de datos debe considerarse un derecho fundamental. Veil, por ejemplo, sugiere que solo se convierte en un derecho defensivo ante los tribunales cuando se combina con otro derecho fundamental y que, en consecuencia, el tratamiento de datos solo debe ser relevante en el marco de los derechos fundamentales si menoscaba o corre el riesgo de menoscabar, específicamente, la libertad.[88] Entre quienes aceptan la designación de la protección de datos como derecho fundamental, las concepciones de su relación con el derecho a la privacidad difieren. En general, pueden agruparse en tres (o cuatro).[89]

Una primera concepción es que ambos derechos son *completamente distintos aunque complementarios* en la medida en que ambos persiguen el logro de valores de orden superior, como la dignidad, la autonomía o el control y la limitación del poder. Para De Hert y Gutwirth, la privacidad es una «herramienta de opacidad» que ayuda a poner límites al poder y a evitar que se haga de este un uso ilegítimo y excesivo, mientras que la protección de datos es una «herramienta de transparencia» que controla y canaliza el poder a través de la transparencia y la rendición de cuentas.[90]

Una segunda concepción es que *la protección de datos es un mero subconjunto del derecho a la privacidad*. Quizás esta sea la visión más extendida de la relación. Para el Tribunal Europeo de Derechos Humanos, por ejemplo, la protección de datos personales se contempla y regula en relación con el artículo 8 del CEDH, el derecho a la privacidad. Del mismo modo, como señala Solove en Estados Unidos, el «derecho constitucional a la privacidad de la información ha surgido en los tribunales como una escisión de los derechos constitucionales ordinarios».[91] Sin embargo, incluso cuando el derecho a la privacidad subsume la protección de datos, cabe distinguir entre las situaciones en que la protección de datos se trata *como privacidad* y las situaciones en que se considera que el objetivo principal de la protección de datos es la protección de la privacidad.[92]

Una tercera concepción —cada vez con más defensores— es que *la protección de datos y la privacidad son derechos distintos pero fuertemente solapados*, en los que la protección de datos cumple una multitud de funciones que incluyen, entre otras, el respeto a la privacidad. Protección de datos y privacidad son distintas en la medida en que difieren en los ámbitos de aplicación. Así, la privacidad abarca ámbitos que la protección de datos no cubre (por ejemplo, cuestiones de autonomía corporal y vida familiar), mientras que la protección de datos no se ocupa de cuestiones de «expectativas razonables» de privacidad y extiende su protección incondicionalmente a las actividades públicas y voluntarias de tratamiento de datos.[93] Esta noción se refleja en el artículo 1 del Convenio 108+, según el cual «el derecho a la protección de datos es autónomo y contribuye al respeto de los derechos humanos y las libertades fundamentales, en particular el derecho a la privacidad». Define el derecho a la protección de datos como un derecho independiente que contribuye a otros derechos humanos; en particular, el derecho a la privacidad.

Una cuarta concepción considera que la protección de datos surge de un deber positivo del estado. Esto es especialmente relevante en jurisdicciones como la India y Estados Unidos, donde los derechos fundamentales se estructuran principalmente como derechos «verticales», que proporcionan protección contra la acción del Estado. Por el contrario, el derecho a la protección de datos se enmarca muy a menudo como un derecho «horizontal» frente a entidades privadas.[94] La naturaleza evolutiva de los derechos fundamentales no es meramente la de derechos negativos (la protección que impide la acción del Estado), sino también la de derechos positivos, que crean obligaciones para que el Estado proteja los derechos (frente a entidades privadas). Así, la privacidad adquiere una aplicación indirecta, horizontal, incluso en jurisdicciones donde los derechos fundamentales solo están disponibles como derecho vertical.[95] Así concebida, la protección de datos no es un subconjunto de la privacidad; más bien emerge de un deber positivo del estado a través de sus obligaciones de privacidad.

Como sugieren de Hert y Gutwirth, «en las disposiciones de las leyes de protección de datos se pueden encontrar pocas manifestaciones directas de las concepciones de la privacidad orientadas a la privacidad y, a la inversa, los conceptos más amplios de la privacidad no son de naturaleza tal que expliquen principios de protección de datos como la limitación de la finalidad, la calidad de los datos o la seguridad.»[96] La protección de datos también reconoce a las personas diversos derechos en relación con sus datos que van más allá de la privacidad, incluidos los derechos de acceso a los datos e incluso los derechos de portabilidad.[97] Sin embargo, a medida que el alcance del derecho a la privacidad se amplía jurisprudencialmente para abordar las preocupaciones de la era digital, el solapamiento entre estos derechos aumenta.

Por último, en la legislación sobre derechos humanos en general, existe el reconocimiento mutuo de que los derechos se desarrollan de forma concertada entre sí y con la sociedad. Al considerar el aumento de la importancia de la protección de datos y la privacidad, sirve señalar que un marco basado en los derechos reconoce la naturaleza en constante desarrollo de los derechos. Los derechos no se congelan en el tiempo, ni son estáticos: evolucionan a medida que la propia sociedad evoluciona. Esto responde a las necesidades reales de protección de las personas, para que puedan vivir con dignidad y respeto.
La legislación internacional en materia de derechos humanos parte del principio fundamental de que los derechos están interrelacionados y son interdependientes, y que la mejor protección de un derecho contribuye a la mejor realización de otros derechos. En este marco, se podría examinar el contexto moderno como una profundización de la interrelación y las interdependencias entre la privacidad, la protección de datos y otros derechos que simplemente están surgiendo en la conciencia pública y jurídica con ritmos de velocidad e impacto diferentes.

ii. Privacidad de la información y autodeterminación informativa

Con independencia de si consideramos la protección de datos como un subconjunto de la privacidad, como dos derechos «distintos pero que se solapan», o como la evolución inherentemente interrelacionada e interdependiente de los derechos modernos en progreso, es indudable que existe una clara superposición entre el objeto del derecho a la protección de datos, tal como se define en la Carta de la UE y en determinadas constituciones nacionales o estatales, y lo que, a finales de 1960, Westin y Fried describieron como «privacidad de la información». Para Westin, la privacidad de la información es el «derecho de individuos, grupos o instituciones a determinar por sí mismos cómo, cuándo y en qué medida se comunica a otro información que les concierne».98

Esta definición de la privacidad de la información entendida como el derecho de las personas a «determinar» o «controlar» qué se puede hacer con sus datos sugiere una estrecha relación entre este derecho y el derecho general a la privacidad. Sigue la senda marcada por los estudiosos estadounidenses de la privacidad del siglo XIX, Samuel Warren y Louis Brandeis, quienes ya habían ampliado el ámbito material del derecho a la privacidad añadiendo, al elemento físico o de «dimensión espacial» comúnmente reconocido, una nueva dimensión de privacidad que incluía la protección de los «pensamientos, los sentimientos y las emociones» de un individuo.

Otros, como Ruth Gavison o Shoshana Zuboff, apuntan a definiciones más amplias. Reconocen el desequilibrio de poder actual en los campos de los datos y la privacidad, y reconocen que los nuevos y poderosos sistemas de recopilación y comercialización de información digital sobre la vida privada de los ciudadanos son comparables a otros cambios históricos, como el paso de la tierra natural a los mercados inmobiliarios, o de las economías de trueque a los recursos humanos que el trabajo impulsado por el mercado.99.

Tanto el derecho a la autodeterminación informativa (o privacidad de la información) como el derecho a la protección de la esfera privada tienen origen en los mismos valores fundamentales que también ponen de relieve que, aparte de su origen común, ambos derechos comparten el objetivo de la protección de la dignidad humana y de la autonomía individual.

iii. El «valor añadido» de la protección de datos

Reconocido como un derecho fundamental distinto, surge la cuestión de qué valores independientes ofrece el derecho a la protección de datos a los individuos o a la sociedad. Como ya se ha destacado (y se analiza más adelante), cuando nos preguntamos por qué protegemos mediante el derecho a la protección de datos, la autodeterminación informativa es una respuesta habitual.

Más allá de la autodeterminación informativa, hay quienes ven la protección de datos desde la lente de la equidad y el buen gobierno de los datos.[100] Según Post, por ejemplo, el artículo 8 de la Carta de la UE «crea prácticas de información justas que establecen normas burocráticas para estructurar la toma de decisiones de personas que se figuran como asociales y autónomas».[101] Van der Sloot contrasta el «ideal ateniense de vida privada» con el enfoque de la protección de datos sobre «si los datos se utilizan de forma justa y con el debido tratamiento».[102]

Otros, yendo más allá, sugieren que el derecho a la protección de datos proporciona «un derecho a una norma» o un derecho a un marco jurídico que regule el tratamiento de datos. Aplicando la lógica del derecho a la protección de datos de la Carta de la UE, este marco jurídico incluiría, como mínimo, derechos para las personas, impondría obligaciones a quienes traten datos personales y establecería un mecanismo de supervisión y aplicación eficaz e independiente.[103] Así, el valor al que la protección de datos no es otro que el de establecer las reglas del juego para facilitar otros derechos e intereses.[104]

iv. La protección de datos como derecho procesal o sustantivo

Si existe un derecho independiente a la protección de datos para dotar a las personas da más control sobre los datos personales propios, o para garantizar la existencia de un marco jurídico para el tratamiento de datos personales, ¿deviene entonces la protección de datos en un derecho procesal? Sin duda, algunos así lo creen y sugieren que la protección de datos «no representa directamente ningún valor o interés *per se*; solo prescribe los procedimientos y métodos para lograr el respeto de los valores encarnados en otros derechos».[105]

Sin embargo, considerar que la protección de datos es puramente procesal puede constituir una simplificación excesiva. En realidad, es un derecho híbrido. Si busca lograr la autodeterminación informativa, se trata de un fin en sí mismo y, además, de un vehículo para lograr la dignidad humana y promover la democracia.[106] Si es un derecho a un marco jurídico que regule el tratamiento de datos, debemos reconocer que algunos elementos de dicho marco son principalmente procedimentales (por ejemplo, los requisitos de transparencia y responsabilidad), mientras que otros son sustantivos, ya que requieren un proceso jurídico en el que considerar la ponderación de intereses y derechos.[107] Incluso si la protección de datos se considerara un derecho «procedimental», sin ningún valor independiente, esto no es razón para no considerarlo fundamental.[108].

De hecho, la ONU ha reconocido que los derechos específicos que puedan estar surgiendo o que se hayan articulado más recientemente, son igual de fundamentales. Por ejemplo, el artículo 9 de la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad (CDPD) señala que el principio de accesibilidad es clave para la realización de los derechos de las personas con discapacidad. El órgano de tratados de la CDPD ha señalado que la «accesibilidad», más que un derecho procesal, constituye una expresión de un derecho fundamental de acceso garantizado en el ICCPR y el PIDESC.[109] Su irrupción y reconocimiento a lo largo del tiempo no han mermado ese reconocimiento universal. Del mismo modo, la protección de datos podría considerarse una condición previa vital para el disfrute efectivo de los derechos civiles, políticos, económicos, sociales y culturales en nuestra era actual, y merecedora de un reconocimiento similar en el derecho internacional.

Ampliación del derecho a la privacidad: la decisión sobre el censo alemán

El Tribunal Constitucional alemán estableció una instancia práctica para la ampliación del significado del derecho a la autodeterminación en su decisión trascendente sobre el «Censo» de 1984. Respondía a los excesivos poderes de obtención y tratamiento de datos concedidos al gobierno alemán por la *Ley del Censo de 1983*. El Tribunal desarrolló un nuevo derecho a la autodeterminación informativa que limitaba dichos poderes. Reflejando, casi al pie de la letra, las opiniones expresadas por Westin hacía más de quince años, sostuvo que la Constitución alemana protegía específicamente el derecho del individuo «a decidir por sí mismo cuándo y dentro de qué límites deben revelarse detalles de su vida personal». A falta de un derecho específico en la *Ley fundamental alemana*, el tribunal definió el nuevo «derecho a la autodeterminación informativa» como un aspecto del «derecho general a la personalidad» del individuo que, a su vez, se basaba en dos derechos que ya existían. Se trata del derecho a la autodeterminación, recogido en el apartado 1 del artículo 2, y del derecho a la dignidad humana, recogido en el apartado 1 del artículo 1 de la *Ley fundamental alemana*. Dicho derecho general de la personalidad, reconocido por el tribunal desde 1973, y antes reconocido por el Tribunal Civil Federal desde 1954, protegía hasta entonces únicamente al individuo frente a la intromisión ilegítima en su esfera privada. Sin embargo, en lugar de describir el derecho a la autodeterminación informativa como un subconjunto de ese derecho más antiguo, el tribunal pasó a reconocer a ambos derechos un estatus igual pero separado con un origen compartido. En esencia, el derecho a la autodeterminación informativa garantiza el derecho del individuo a controlar tanto la divulgación de los datos personales propios como la forma y los fines del uso de dichos datos. El Tribunal argumentó que, en el contexto de los procedimientos modernos de tratamiento de datos, el individuo requiere protección contra la obtención, el almacenamiento, el uso y la divulgación ilimitados de sus datos personales. Así pues, el derecho ha restringido tradicionalmente a las autoridades públicas la obtención y el tratamiento masivos de datos personales o el uso de identificadores específicos vinculados a dichos datos para tomar decisiones que tengan efectos jurídicos sobre los ciudadanos individuales. Dada la capacidad de los modernos sistemas informáticos para conectar y combinar datos, el Tribunal consideró que los «datos inmateriales» ya no existían (incluso datos que en sí mismos parecían irrelevantes podían adquirir relevancia en conjunción con otros datos). En consecuencia, dictaminó que la protección de los datos personales no podía depender de si dichos datos se referían o no a la esfera privada o íntima de una persona. En cambio, para evaluar la pertinencia del tratamiento a la luz de una posible violación de la dignidad y la autodeterminación de una persona, es esencial establecer la finalidad de la obtención de los datos y la forma en que estos pueden utilizarse o vincularse con otros datos. Nació así la idea de que los datos personales merecían una protección de los derechos fundamentales equivalente al derecho a la privacidad, incluso cuando no pudieran considerarse «privados». **Fuentes:** Ley del censo, BVerfGE 65, 1; traducción al inglés facilitada por la Konrad-Adenauer-Stiftung alemana; disponible en https://freiheitsfoo.de//files/2013/10/Census-Act.pdf; último acceso: 20 de octubre de 2020.

4. ¿Qué protegemos cuando protegemos la privacidad y la protección de datos?

El desarrollo tanto del derecho a la privacidad como del derecho a la autodeterminación informativa en el contexto jurídico de la UE (ya mencionado) quizás pone de relieve algo que puede ser menos evidente en instrumentos de derechos fundamentales posteriores que incluyan un derecho expreso a la protección de datos. Se trata de que la privacidad (como concepto y como derecho jurídico) se deriva a su vez de una serie de intereses, derechos y valores individuales y públicos (y se ha concebido para protegerlos). Incluye el derecho de los individuos a la autorrealización y al desarrollo de la personalidad propia.

La autorrealización comprende el derecho a decidir cómo una persona se presenta ante los demás (por ejemplo, control sobre su imagen pública y reputación) y hasta qué punto se hace accesible a sí misma y a su vida (por ejemplo, consentimiento y control sobre la publicación de datos personales). Cubre su derecho tanto a desarrollar como a comunicar opiniones y convicciones libres de la observación no deseada de otros (por ejemplo, disentir de las políticas gubernamentales o criticar las decisiones políticas). Además, apoya el derecho a tomar decisiones y emprender acciones basadas en las opiniones y convicciones que puedan afectarles no solo a ellos, sino también a los intereses colectivos y públicos.

El punto de partida de todos estos derechos es que sin privacidad y protección de datos —sin el derecho a excluir a otros del acceso a nuestro espacio, nuestras acciones y nuestros pensamientos— no podemos desarrollar y expresar nuestra propia individualidad en todo su potencial. El resultado es que se nos impide participar en interacciones comunitarias y en procesos de toma de decisiones como nosotros mismos (por ejemplo, cuando los empleados se autocensuran en un lugar de trabajo por miedo a represalias). Este ideal de autodeterminación individual, autorrealización y control, expresados tanto en el derecho general a la privacidad como en el derecho a la privacidad de la información, reflejan, por tanto, valores más fundamentales de dignidad humana, libertad y autonomía. Los examinaremos más adelante.

A. Dignidad humana

La dignidad humana quizás sea el más significativo de estos valores, ya que protege la esencia de lo que es vivir como ser humano, ser valorado por ser uno mismo y ser tratado con respeto. Su importancia global se pone de relieve en la Declaración de derechos humanos de la ONU, que reconoce la dignidad inherente a todos los miembros de la familia humana, así como en el Convenio 108+ y en la Carta de los derechos fundamentales de la UE, que incluye el respeto y la protección de la dignidad humana como su primer artículo.[110] El derecho a la dignidad humana es también el primer derecho de la Ley fundamental alemana y uno de los pocos derechos absolutos en ella incluidos. Es uno de los dos únicos derechos incluidos en la Ley fundamental que no pueden modificarse salvo mediante la aprobación de una nueva Constitución. Así, la dignidad humana queda protegida como un importante valor ético y jurídico. Desde un punto de vista más práctico, refuerza, además, las prohibiciones de la esclavitud, la tortura, la trata de personas y otras prácticas inhumanas.

La exigencia de tratar a todos como personas respetando su humanidad y sin someterlos a tratos inhumanos refleja el concepto moral de dignidad de Kant como la necesidad de tratar a la humanidad «tanto en tu persona como en la persona de cualquier otro, siempre con el fin al mismo tiempo y nunca solamente como un medio». [111] De tal requisito se infiere directamente, por tanto, que nadie debe ser utilizado únicamente como medio para alcanzar otros fines.

Sin embargo, esta posibilidad se ha planteado como una preocupación en relación con las prácticas de tratamiento de datos personales que podrían reducir a los individuos de sujetos a meros objetos. Así, Lyon, por ejemplo, advierte de que el uso cada vez más intensivo de datos personales por los ordenadores podría acarrear el riesgo de degradar a los individuos a meras mercancías y someter los valores humanos a la mera eficacia. Citron y Pasquale comparten una preocupación similar, y muestran de qué modo las prácticas actuales de puntuación basada en datos podrían convertir a los individuos en objetos clasificados y puntuados.[113] Muchos estudiosos de la vigilancia se han mostrado muy críticos con la privacidad, como discurso y como régimen de gobierno.[114] Consideran que contribuye poco a corregir los desequilibrios de poder y miran con recelo las protecciones legales y constitucionales del derecho a la privacidad.

Dignidad humana, clasificación social y digitalización

En este contexto, hallamos un ejemplo ilustrativo en la calificación crediticia. Para los sectores financieros, es probable que el uso de Big Data (incluido el uso de información no crediticia, como las redes sociales o los patrones de compra o navegación) para evaluar la calificación crediticia represente un ahorro de costes, ya que los datos pueden utilizarse para identificar patrones de impago potencial que se aplicarían correctamente a la mayoría de sus clientes. Sin embargo, una persona que aparentemente se ajuste a los criterios del patrón, pero en quien la probabilidad de impago sea baja, se verá perjudicada por esta categorización, ya que no se le trata como se le debería haber tratado en función de sus circunstancias individuales. Y, en cambio, simplemente se obvía su situación individual en aras de las estrategias de maximización de ingresos de la empresa. Del mismo modo, empresas y otros usuarios de datos pueden no contemplan la posibilidad de que los datos brutos que alimentan sus algoritmos de toma de decisiones sean incorrectos o estén desfasados. Los efectos pueden producirse en el individuo en cuestión, pero, también, al desarrollo posterior del propio patrón algorítmico (especialmente cuando los datos brutos forman parte de un conjunto de datos de entrenamiento), con consecuencias a largo plazo para aquellos a quienes el algoritmo afecta de modo práctico o legal. Finalmente, en la era del aprendizaje automático, los algoritmos están diseñados para «mejorar» su programa original en función de los datos que se les suministran. Puede suceder que las propias empresas ya no puedan identificar los criterios que utiliza el algoritmo, lo que resulta en situaciones en que «el ordenador dice no», en que la toma de decisiones algorítmica elude la rendición de cuentas y en que el posible sesgo algorítmico hacia determinados tipos de personas pasa a ser indetectable en la práctica, desafiando así la supervisión reglamentaria. La opacidad de la toma de decisiones algorítmica se examina con más detalle en la página 34.

La calificación crediticia es solo individual de los muchos ejemplos.[115] Todos estos casos demuestran que la *datificación* de las personas de una forma que escapa al control de esas personas refleja una falta de respeto a las personas como seres humanos que atenta contra la dignidad humana, ya que los usuarios de los datos no muestran preocupación alguna por el bienestar de esas personas o por su derecho a la igualdad de trato.

En las dos últimas décadas, los cambios en la escala de recopilación de datos digitales (así como en su alcance global y capacidad de almacenamiento) revelan un marcado desequilibrio en el control de la información. Los desequilibrios de poder resultantes (fruto de la digitalización y los mercados de datos) crean riesgos para los derechos políticos, sociales, económicos y culturales (no solo para la dignidad humana).[116] Los desequilibrios de poder en juego y el alcance del daño potencial son un argumento suficiente para justificar por qué la privacidad debe articularse claramente como derecho humano. Por tanto, un derecho a la privacidad de la información que refuerce el control de los individuos sobre sus datos se considera una forma de protección contra tales violaciones.

B. Libertad y autodeterminación

Gran parte del debate en torno al derecho a la privacidad se ha orientado además hacia el objetivo de proteger a las personas de la injerencia de los organismos gubernamentales, especialmente dada la existencia actual de una vigilancia electrónica omnipresente. En este contexto, el derecho a la privacidad de la información se alista para preservar el valor posiblemente aún más fundamental de la «libertad» como derecho último del individuo a estar libre de tal interferencia estatal. De hecho, Lyon argumenta que libertad es un término preferible a privacidad cuando se habla de las tendencias totalitarias en una sociedad de vigilancia.[117] Si bien el significado exacto de libertad no es inmutable, suele entenderse como el derecho natural sin restricciones de los individuos a seguir su propia voluntad.[118] En este contexto, las metáforas del Gran Hermano y el Panóptico a menudo se ven como una restricción del libre albedrío a través de una vigilancia que es a la vez obvia y real o en la que los individuos creen estar bajo observación sin poder verificar exactamente cuándo y en qué condiciones tiene lugar la vigilancia.[119] En ambos casos, según el argumento, los individuos adaptarán su comportamiento para cumplir las normas y expectativas del observador.

C. Autonomía y elección

Por último, la noción de privacidad como control individual se sostiene posiblemente en los conceptos de «autonomía» y «elección». En la teoría liberal, los individuos son, ante todo, agentes autónomos que llegan a la autorrealización incluso a través de decisiones mundanas.[120] Tanto la idea de dignidad humana como la de libertad individual sugieren que nosotros mismos deberíamos ser el autor de nuestra historia, el «dueño de nuestro destino» y el «capitán de nuestra alma».[121] Los marcos económicos liberales también defienden que las elecciones de los consumidores en el mercado son elecciones libres, ya que suponen que ambas partes disponen de información completa: que una elección con sentido implica información completa y transparencia.

Pero lo cierto es que nuestras decisiones se basan en un frágil equilibrio de limitaciones y opciones. Vienen determinados por los entornos económicos, sociales y políticos específicos en los que operamos. En el entorno actual, tanto el Estado como los sectores privados que recopilan, comercian y utilizan macrodatos de los ciudadanos, tienen tanto una enorme ventaja informativa, como la opacidad de cómo utilizan estos datos.[122] Además, los exámenes actuales de los formularios de consentimiento en línea dejan claro que los ciudadanos y los consumidores pueden carecer de opciones significativas y de autonomía para optar por no consentir que su información se recopile y utilice de manera que beneficie a las empresas y los estados, y perjudique a los consumidores y los ciudadanos.[123] Incluso en las democracias, estos datos pueden explotarse para manipular opacamente a los votantes, sin que estos tengan conocimiento y lo consientan. Los derechos y la aplicación de normas justas que los respeten pueden verse como una forma de permitir una autonomía más plena y una elección más significativa.

Como individuos, no existimos en el vacío, y no decidimos al margen de las estructuras de poder imperantes que nos privilegian o nos perjudican (o a veces ambas cosas de distintas maneras). En realidad, la autonomía está limitada por el propio interés existencial, las dependencias económicas, nuestras relaciones con los demás y nuestras obligaciones hacia ellos, y por el poder relativo (así como por cualquier responsabilidad, véase más arriba) que podamos tener como miembros de nuestras respectivas comunidades. Estas cuestiones se presentan para su consideración y reflexión en un anexo a esta narración.

5. La privacidad y la protección de datos como derechos individuales o colectivos

El elemento «comunitario» de los derechos a la privacidad y a la protección de datos es controvertido. Por un lado, el estatus de esos derechos como derechos individuales en la mayoría de los instrumentos liberales de derechos humanos ha sido blanco de muchas críticas procedentes de los defensores del comunitarismo y de la adopción de un mayor enfoque en los intereses colectivos o de la sociedad. Sin embargo, esta crítica no está exenta de dificultades. Si la privacidad equivale esencialmente a un «derecho a no participar en lo colectivo» y a «aislar al individuo de diversos tipos de injerencias»[124], ¿cómo puede entonces la privacidad emplearse de forma fiable para promover las necesidades de la comunidad? Cómo interactúan, por un lado, la privacidad como «derecho a ser dejado en paz» (Warren y Brandeis) y, por otro, el «valor social» de la privacidad (Priscilla Regan).[125]

Podría decirse que un enfoque que combine la mercantilización de los datos personales con una concepción de la privacidad/protección de datos como una herramienta diseñada únicamente para facilitar el control individual, puede convencer más fácilmente a particulares, empresas y legisladores del valor intrínseco y la legitimidad de ciertas «concesiones mutuas en materia de privacidad».[126] Como ya se ha explicado, en esos casos, el «riesgo para la privacidad» asociado a una actividad de tratamiento —ya sea llevada a cabo por responsables del sector privado o público— se percibirá solo como uno de una serie de riesgos en competencia, en que otros riesgos incluyen amenazas existenciales, perjuicios económicos y temor a la exclusión social.

En la práctica, esto propicia que los individuos justifiquen el tratamiento de datos (ante sí mismos y ante otros) que consideran que sirve a intereses superiores individuales, comerciales o comunitarios. Sin embargo, también significa que la privacidad y la protección de datos como derechos fundamentales suelen considerarse secundarios frente a otros derechos y libertades. El derecho a la vida, la libertad de expresión o la libertad de prensa son solo tres ejemplos habituales. Del mismo modo, entre los intereses públicos que compiten con la privacidad, o que con frecuencia la anulan, se encuentran el orden público, la seguridad nacional o la salud pública, que favorecen de forma más evidente tanto a los intereses individuales como a los colectivos o de la sociedad.

A. ¿Diferencias culturales?

Del mismo modo, a menudo se sugiere que la idea de «privacidad» como derecho individual es una construcción liberal que no se ajusta bien a las tradiciones culturales, históricas, religiosas y filosóficas que conforman las visiones del mundo de las comunidades; en particular, en partes de África, algunas partes de las economías de Asia-Pacífico y también en zonas como Canadá y Australia, donde la historia colonial ha perjudicado a las poblaciones indígenas.

No hay duda de que las distintas regiones y políticas debaten cuestiones de derechos, responsabilidades y reparación basándose en la experiencia histórica y social propia. Reconocer dichas divergencias y matices es requisito previo para entender cómo mejorar la protección de datos. No es un obstáculo. El desarrollo de cualquier ecosistema normativo —ya sea en la UE, Norteamérica o Latinoamérica—

representa una evolución consciente y una negociación deliberada. En ningún caso surgió de forma «natural» ni es «inevitable».

De hecho, en la actualidad, gran parte de los países de todo el mundo (en Asia-Pacífico, África y América Latina) que están contemplando la adopción o revisión de su régimen de protección de datos lo hacen *sin el lastre* de la historia y la filosofía en que se sustentaba la adopción de la primera generación de leyes en materia de privacidad. [127] Como ya se ha expuesto (véase «Orígenes del derecho a la privacidad»), muchas de dichas leyes fueron respuestas legislativas concretas a prácticas específicas de vigilancia gubernamental relacionadas con la Segunda Guerra Mundial y los inicios de la Guerra Fría.

Por el contrario, las sociedades del mundo en desarrollo se han distanciado considerablemente de tales secuelas. En cambio, sus gobiernos particulares se han preocupado por la reconstrucción, el desarrollo y la integración en una economía globalizada para proporcionar un futuro mejor a su población.[128] Desde esta perspectiva, ellos y sus ciudadanos apoyan activamente la innovación, la digitalización y el intercambio transfronterizo de datos.[129] Se trata de perspectiva y prioridades que deben reconocerse, validarse y apoyarse, en lugar de marginarse, ignorarse o excluirse.[130].

Por poner solo un ejemplo de esa complejidad, vemos que en la región APEC existen tradiciones, sistemas jurídicos, modelos políticos y modelos socioeconómicos multivalentes. Diríamos que la variación supera incluso a la de Europa o América, y los debates sobre la privacidad son constantes. Por ejemplo, los debates en la Cumbre de Osaka de junio de 2019 reavivaron las tensiones latentes sobre la gobernanza de datos, con muchas naciones asiáticas optando por sendas muy diferentes en cuestiones críticas de datos.[131] India, en particular, defendió que cualquier reglamentación sobre la gobernanza de datos fuera de la Organización Mundial del Comercio (OMC) diluiría las voces de las economías emergentes en el debate y suprimiría su derecho soberano a enmarcar normas que promuevan los mejores intereses de sus ciudadanos.[132].

En la práctica, las leyes de protección de datos se han desarrollado orgánicamente en Asia como en el resto del mundo, en países influenciados por el taoísmo, el budismo y el confucianismo (por ejemplo, Corea o Japón) y que han adoptado este tipo de medidas durante décadas.[133] La PIPA de Corea, por ejemplo, se conoce por ser una de las leyes de protección de datos más estrictas del mundo. En consecuencia, las divergencias van más allá del ámbito político y económico; pueden afectar también a las visiones de las sociedades sobre lo filosófico y lo sagrado.

Según Kitiyadisai, es difícil alinear el concepto liberal occidental de privacidad como derecho individual con, entre otros, los valores budistas, ya que el budismo percibe los conceptos de derechos humanos y derechos a la privacidad como normas creadas por el hombre que «entrarían inevitablemente en conflicto en sí mismas, porque se crearon creadas para servir a la avaricia humana». Dado que «reflejan la fuerza imperante en la sociedad», «conducirían a una mayor competencia y a posturas agresivas para proteger y promover los intereses entre diversos grupos».[134] Significa, pues, que ciertos aspectos de determinadas culturas y sociedades pueden percibir los derechos humanos —incluidas la privacidad y la protección de datos— como herramientas que reflejan y apoyan las estructuras de poder existentes en lugar de desafiarlas.

En un contexto africano, Olinger y Britz han afirmado que «[l]a privacidad como noción no funciona en el pensamiento filosófico africano» porque es incompatible con la idea de *Ubuntu*.[135] *Ubuntu*, a menudo traducido como «yo soy porque nosotros somos», suele describirse como una forma particular de humanismo africano que prioriza el comunalismo y la interdependencia sobre el individualismo y la competencia. Como tal, «[l]a privacidad brillaba por su ausencia como valor o derecho apreciado dentro de las sociedades Ubuntu», porque «[u]n derecho individual se aceptará si sirve a la comunidad».[136]

Aunque parece coincidir con variaciones en algunas de las otras regiones ya identificadas, esta crítica al derecho a la privacidad pone de relieve un problema al que también se enfrentan los defensores de la privacidad y la protección de datos en todas partes: a saber, que siempre ha sido «difícil defender el beneficio social de la privacidad personal».[137] Sin embargo, dado el potencial de perjuicio que la creciente ausencia de privacidad, causada por la apropiación generalizada de datos personales por las nuevas tecnologías y modelos de negocio, puede tener tanto en el individuo como en los intereses colectivos y sociales, argumentaríamos que ahora es el momento de defender esta causa. [138]

Además, las cuestiones relativas a las distintas concepciones culturales de la privacidad están imbricadas en el ámbito filosófico. A lo largo de la historia, se puede observar la *problemática* de nuestra humanidad común frente a la diferencia cultural. De modo semejante, se llega hasta el antiguo problema filosófico de lo individual y lo múltiple, presente en muchos ámbitos de aplicación.[139] Para que la diferencia (lo múltiple) sea inteligible, necesitamos una concepción de lo común o de la identidad. Exactamente como el sentido de la idea de lo común (lo individual) se basa en la diferenciación (lo múltiple). La analogía se aplica también a las concepciones de la vida privada, ya que lo privado solo es inteligible en el contexto del concepto de lo público, del mismo modo que lo público solo tiene sentido en relación con lo privado.[140] Así pues, estrictamente, no es posible que las personas tengan una vida pública y grupal significativa si carecen de una vida privada individual.[141]

Estas diferencias de visión del mundo también existen en las democracias modernas, sobre todo en aquellas en las que viven pueblos indígenas. Dichas visiones del mundo han servido de base para la elaboración de un instrumento internacional, la *Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas*. Los derechos y la visión del mundo de los diversos pueblos indígenas han pasado a ocupar un primer plano en muchas partes del mundo. Y también ha pasado a ocuparlo la importancia de respetar estos derechos, ajustar las leyes y emprender la reconciliación en las naciones donde las repercusiones del colonialismo han sido horribles e injustas. Esta visión del mundo comprende nuevas interpretaciones de los derechos tanto individuales como colectivos.
Así pues, cualquier nuevo instrumento internacional o ley nacional, debe considerar y consultar a las personas indígenas que viven allí.

B. Daños individuales frente a colectivos frente a sociales

Durante mucho tiempo, la defensa convincente de una interpretación de los derechos a la privacidad y a la protección de datos que incluya una perspectiva comunitaria o social ha sido difícil. La razón, principalmente, guarda relación con el fuerte enfoque del pensamiento liberal occidental sobre los derechos fundamentales como derechos

individuales, en los que una interferencia siempre debe también dar como resultado un perjuicio para el individuo que sea verificable.[142] En la legislación sobre privacidad y protección de datos, el concepto de «perjuicio» es complejo y controvertido. Hay quienes sostienen que, para ser recurrible, el impacto debe referirse a algún tipo de perjuicio material o para la reputación. Otros, en cambio, afirman que el concepto de perjuicio debe guardar relación directa con un riesgo específico y con el momento en que dicho riesgo se materializa.

Así, por ejemplo, en el contexto de los debates sobre la conservación obligatoria de datos de comunicaciones con fines policiales, las autoridades han defendido a menudo que la mera obtención y conservación de datos personales no representa ningún riesgo y que, por lo tanto, no existe ninguna interferencia con el derecho a la privacidad y a la protección de datos hasta que se accede realmente a dichos datos. En el ámbito de la UE, este argumento fue rechazado por el TJUE en *Digital Rights Ireland* y la jurisprudencia posterior,[143] pero el argumento en sí prevalece en muchos otros contextos.[144].

El problema de este planteamiento reside en que se basa solo en un concepto de perjuicio a la privacidad, que es a la vez económico e individualizado. Si se adopta este planteamiento, solo existirá perjuicio si el interesado sufre daños o perjuicios (económicos) verificables. Sin embargo, la evolución de los últimos años ha demostrado que con esta conceptualización del daño a la privacidad no basta. Ello se debe tanto a su sesgo económico como al hecho de que omite toda una serie de riesgos y perjuicios que no sufre el interesado, sino otras personas —a menudo aquellas con las que el interesado comparte ciertas características—, así como por el conjunto de la sociedad.

En cambio, un enfoque basado en los derechos humanos sí considera el daño a la dignidad humana, entre otros perjuicios no económicos. Los estatutos de derechos humanos son también de derecho público, y reconocen que un daño a los derechos de un individuo es también un daño al bien público. Por lo tanto, al considerar el derecho a la privacidad y a la protección de datos como derechos fundamentales, debemos tener en cuenta también esos daños más «invisibles» y la medida en que estos afectan tanto a los intereses individuales como a los intereses colectivos y sociales.

Del mismo modo que la autonomía de decisión es un principio clave para el derecho a la privacidad, los intereses de grupo se basan en la idea de autodeterminación, ahora reconocida como principio básico del derecho internacional público. Pese a que en un principio se formuló como principio político, en la era de la descolonización, los aspectos internos de la autodeterminación han adquirido más importancia recientemente. Shaw ha descrito la autodeterminación como «la búsqueda por un pueblo de su desarrollo político, económico, social y cultural en el marco de un estado existente».[145]

i. Daños invisibles

La capacidad de las entidades públicas y privadas para recopilar grandes cantidades de datos personales en diversos contextos, combinarlos con otros datos y analizarlos a gran velocidad ha desembocado en una situación en la que los datos personales circulan libremente. Nuestra información fluye como por un sistema de «puertas giratorias», de lo público a lo privado (y *viceversa)*, de lo público a lo público y de lo privado a lo privado, sin apenas tener en cuenta los fines para los que se recopiló inicialmente. De hecho, actualmente crece constantemente la presión sobre las autoridades públicas para que, en aras de la «innovación», compartan los datos administrativos que poseen con el sector privado. La actitud predominante en muchas prácticas de tratamiento contemporáneas parece consistir en la idea de que «si los datos ya están ahí, deberíamos poder utilizarlos».[146]

Además de ilustrar claramente la existencia de la «base de datos de la ruina» de Ohm —es decir, el riesgo de que datos previamente considerados anónimos puedan correr el riesgo de ser reidentificados mediante su combinación con otros datos— destaca los daños invisibles a la privacidad que pueden producirse cuando se vulnera la integridad contextual de la divulgación de información personal.[147] Como se ha señalado,

> *Desde la perspectiva de los interesados, ahora es casi inevitable que, tarde o temprano, los datos personales que dichos interesados revelen a una entidad se compartan entre dos o más entidades públicas o privadas sin su consentimiento específico y, a menudo, sin su conocimiento consciente. Así, resulta imposible para el interesado apreciar, en el momento de la recogida, durante cuánto tiempo se almacenarán sus datos, cómo se utilizarán en el futuro, con qué fines y por quién. Entonces, al revelar sus datos a cualquier persona, los interesados no pueden decidir de forma informada acerca de los riesgos que esa divulgación entraña y, en consecuencia, se les impide tomar precauciones razonables contra esos riesgos*.[148]

Esto representa un cambio en el equilibrio del «poder de la información» a favor de la entidad ya más poderosa (normalmente la empresa o el organismo público) que facilita la mercantilización de los individuos, permite la discriminación y «más fundamentalmente [...] subordina las consideraciones del bienestar humano y la autodeterminación humana a las prioridades y valores de los actores poderosos».[149] Como consecuencia, hemos presenciado una pérdida de control de los individuos sobre la autoarticulación.[150]

Del mismo modo, las prácticas actuales de procesamiento de datos ignoran cada vez más el principio de minimización de datos, durante mucho tiempo piedra angular del marco de protección de datos del CdE y de la UE.[151] Dicho marco dispone que los datos personales deben ser «adecuados, pertinentes y limitados a lo necesario para los fines para los que sean recogidos». Sin embargo, con demasiada frecuencia, la actitud de los responsables del tratamiento de datos, tanto en el sector público como en el privado, es la de «todos los datos siempre».

Beneficios como innovación: política de vinculación de datos de Google de 2012

En el sector privado, la creciente concentración de sectores enteros en un número cada vez menor de agentes también ha provocado que éstos obtengan gran parte de su «poder sobre los datos» de la combinación de diferentes tipos de datos personales, a menudo recogidos por diferentes partes de su negocio para fines diferentes. En 2012, por ejemplo, Google impuso una nueva política de privacidad a los usuarios en todas sus diversas empresas. Se autoconcedió el derecho a combinar datos de usuarios procedentes de fuentes tan distintas como su negocio de búsquedas, sus negocios de contenidos y su negocio de análisis y a utilizarlos para fines nunca comunicados a dichos usuarios ni previstos por ellos en el momento de la obtención de datos.
Fuente: «Updating our privacy policies and terms of service», blog de Google, 24 de enero de 2012; Disponible en http://googleblog.blogspot.co.uk/2012/01/updating-our-privacy- policies-and-terms.html; último acceso: 18 de octubre de 2020.

En el contexto comercial, Shoshana Zuboff ha descrito este proceso como «capitalismo de vigilancia», que «reclama unilateralmente la experiencia humana como materia prima libre» que luego se «traducirá en datos de comportamiento» y se utilizará para «fabricar productos de predicción».[152] Posiblemente, esta adaptación de la experiencia del usuario a sus preferencias conocidas permite un nivel de manipulación hasta el momento inédito. En el extremo más benigno, puede aumentar las ventas de una empresa a un cliente o simplificar la prestación de servicios públicos.[153]

Sin embargo, también puede atrapar a las personas en un entorno en el que se refuercen y amplifiquen sus prejuicios, en el que ya no estén expuestas a bienes, servicios, información, puntos de vista o experiencias diversos, o en el que se les empuje hacia puntos de vista favorecidos por el Estado u otras organizaciones en intentos de afectar a derechos fundamentales como el derecho al voto o el derecho a formarse una opinión.[154]

ii. Daños colectivos y sociales

Además del impacto directo que pueden tener en los individuos, también debemos considerar el efecto a largo plazo que las nuevas prácticas de uso de datos pueden tener en los intereses colectivos y sociales. Los perjuicios colectivos pueden surgir cuando el tratamiento de los datos personales de una persona afecta a otras con las que comparte rasgos o características particulares. Así suele suceder cuando los patrones se analizan a partir de los datos personales obtenidos de un número suficiente y representativo de individuos, lo que permite extraer inferencias que se aplicarán del mismo modo a otros miembros del mismo grupo aunque sus datos no estuvieran disponibles para el análisis directo. Por ejemplo, en términos psicológicos/emocionales, las pruebas psicométricas pueden permitir identificar sesgos y vulnerabilidades en ciertos tipos de personas que pueden resultar útiles para «empujarlas», a ellas y a otras con características similares, hacia determinados comportamientos deseables o rentables.

En el plano fisiológico, el resultado de las pruebas de ADN, a menudo obtenidas de forma privada por los particulares para su referencia, puede utilizarse en un contexto de investigación para identificar si una persona tiene probabilidades de contraer una determinada enfermedad. En manos de vendedores, profesionales sanitarios y compañías de seguros, esta información podría servir para tomar decisiones sobre el tipo de productos y medicamentos a los que se dirigirán las personas con características similares, las primas de los seguros o incluso el acceso a determinados servicios sanitarios. Del mismo modo, los datos personales que los individuos revelan específicamente para obtener una ventaja financiera u otra ventaja material pueden utilizarse para crear expectativas por parte del usuario de los datos (en términos de comportamientos deseables o aceptables) que luego se imponen a otros que no han consentido este tipo de compensación financiera o de conveniencia. En el ciclo de vida de los datos, este tipo de divulgación suele comenzar como una forma de obtener un incentivo concreto. Sin embargo, rápidamente deviene la norma generalmente adoptada e incuestionada hasta que finalmente pasa a ser una herramienta de exclusión.

Utilizar todos los datos: Snowden y la IA

Un ejemplo obvio de este planteamiento de «recógelo todo, úsalo todo» es el contexto de la aplicación de la ley y la seguridad nacional, en el que las revelaciones de Edward Snowden han mostrado la recogida indiscriminada y masiva por parte de las agencias de seguridad de Estados Unidos y Reino Unido de datos, tanto de contenido como de tráfico, que viajan por los servicios de comunicaciones electrónicas y se generan por dichos servicios. Otras pruebas, si son menester, también pueden encontrarse en otros ámbitos, como el comercio y la investigación. Más recientemente, la promoción casi mesiánica de las tecnologías de IA avala más si cabe la idea de que casi todos los problemas comerciales, administrativos, financieros, de política pública o de salud pública podrían resolverse (o resolverse de forma más barata), si solo tuviéramos acceso a datos suficientes. Así es como tanto las empresas como los gobiernos han empezado a reevaluar el valor de sus bases de datos, no para facilitar las relaciones existentes con sus clientes y ciudadanos, sino a fin de obtener el máximo beneficio o utilidad de los datos que poseen sobre dichos clientes y ciudadanos.

Pueden aparecer daños sociales cuando el tratamiento de los datos personales de una persona contribuye a recopilar datos o facilita actividades de tratamiento de datos que dificultan o imposibilitan el ejercicio de los derechos y deberes democráticos, o permiten manipular a personas y grupos de una manera que pueda modificar las relaciones de poder existentes en la sociedad. El efecto amedrentador de la vigilancia ubicua de las comunicaciones suele citarse como ejemplo de la primera posibilidad. Las personas, conocedoras de que sus comunicaciones se interceptan o pueden interceptarse, descartan el uso de determinados medios de comunicación para fines concretos. En la República Democrática Alemana (Alemania Oriental comunista), por ejemplo, existía el acuerdo de que ciertas conversaciones «no eran para el teléfono». Sin embargo, el cambio en la conducta expuesto también puede tener implicaciones más amplias para la participación política, la resistencia y la capacidad de recuperación general de un cuerpo político.

Información sanitaria, seguros y exclusión

En los últimos años, las aseguradoras de salud han animado cada vez más a sus clientes a introducir datos nutricionales y de forma física en sus sistemas digitales a cambio de puntos que pueden aplicarse a la reducción de las primas del seguro o al recibo de reembolsos en efectivo. Semejante planteamiento supone, evidentemente, la ventaja de fomentar un comportamiento responsable por parte del asegurado, quien, al final, además de ahorrar dinero a la aseguradora se verá beneficiado. Dicho individuo debería disfrutar de prestaciones sanitarias adicionales. Sin embargo, existe el riesgo de que, en lugar de utilizarse como incentivo, el sistema de puntos sirva algún día para calcular primas de seguro para todos los clientes, con el resultado de primas más elevadas para quienes no participen en actividades que se estiman beneficiosas para la salud. De ahí a una situación en la que ya no se les ofrezca ningún tipo de seguro sanitario porque las aseguradoras los consideren un mal riesgo hay un paso. Las aseguradoras habrán obtenido los datos personales que les permitirán tomar esas decisiones, en su opinión puramente comerciales, a partir de tan solo un subconjunto de sus clientes. No obstante, las propias decisiones acabarán afectando al conjunto de las clientes.

Al mismo tiempo, las herramientas del capitalismo de vigilancia ya descritas (seguimiento en línea, elaboración de perfiles, selección de objetivos, priorización) pueden utilizarse para dirigir determinados mensajes a los prejuicios específicos de cada individuo y, como tales, pueden animar a esos individuos a actuar de una determinada manera o, incluso, a no actuar en absoluto. Aunque todavía se discute si triunfó realmente para influir en el comportamiento de las personas —por ejemplo, con respecto a su voto en las elecciones presidenciales estadounidenses de 2016 o en el referéndum sobre el Brexit del Reino Unido del mismo año—, está claro que, en general, la microfocalización política puede amplificar ciertos tipos de información mientras suprime otros.[155].

En la actualidad, los verdaderos perjuicios para la sociedad se derivan del hecho de que, sencillamente, aún no podemos determinar por completo el riesgo real que esas técnicas plantean y, por tanto, carecemos de la capacidad de defendernos contra él. En contextos comparables en los que el daño causado por un dispositivo, un proceso o un comportamiento —de manifestarse— sería desastroso para la sociedad o los valores sociales, esto ha llevado normalmente a pedir que se emplee el «principio de precaución».[156] Sin embargo, en el contexto de la información, a menudo nos enfrentamos a una situación en la que «[l]os negocios de la información [...] han

empezado a desarrollar un nuevo marco metafórico que sitúa el entorno de la información y las comunicaciones en red como un aparato despolitizado y autorregulado de producción de la verdad» cuando, en realidad, no es ni lo individual ni lo otro y sí, en cambio, ha «catalizado cambios tectónicos en las relaciones de rendición de cuentas».157 El desarrollo de una narrativa alternativa y eficaz depende, pues, de poner el acento no solo en el *individuo*, sino también en el *valor público y colectivo de la protección de datos*.

C. El valor público y colectivo de la privacidad y la protección de datos

Los pensadores iniciadores de la privacidad siempre han reconocido que las acciones (u omisiones) de las personas a la hora de controlar (o no) el acceso a sus datos pueden afectar tanto a los intereses propios como a los derechos ajenos y al interés público. Ya en 1995, Regan, uno de los primeros estudiosos estadounidenses que abordó la cuestión, destacó que, en una sociedad cada vez tecnológicamente dependiente, «la privacidad se está convirtiendo cada vez menos en un atributo de los individuos y los registros y cada vez más en un atributo de las relaciones sociales y los sistemas de información o comunicación».158.

Afirma que la privacidad, además de valor individual, es un valor público y colectivo, y sostiene que el valor colectivo de la privacidad es decisivo para apuntalar las instituciones y prácticas democráticas. Las distinciones entre la privacidad como valor colectivo, valor público y valor común cobran significados muy diferentes en su marco. Anticipándose a los avances más recientes en relación con los perjuicios colectivos y sociales ocasionados por las actividades de tratamiento de datos basadas en el consentimiento individual, argumentó, ya entonces, que existe el riesgo de que «[s]i un individuo o un grupo de individuos renuncia al derecho a la privacidad, el nivel de privacidad de todos los individuos disminuye porque el valor de la privacidad disminuye».159

Incluso antes, en 1987, Spiros Simitis afirmaba que «las formas modernas de tratamiento de datos han alterado el debate sobre la privacidad en tres sentidos principales».160 Primero: expresan conflictos que afectan a todos, pero lo hacen de una forma que los representa como preocupaciones individuales. Segundo: gracias a las nuevas tecnologías, permiten registrar y reconstruir las actividades individuales con todo lujo de detalles, de modo que la vigilancia perpetua se normaliza. Tercero: se utilizan cada vez más para imponer normas de comportamiento, con lo que se confiere un poder adicional a quienes están en condiciones de determinar cuáles deben ser esas normas. Estos tres desarrollos se consolidaron en el seguimiento en línea omnipresente del comportamiento de las personas, la creación de perfiles detallados sobre ellas y el uso de dichos perfiles para influir en sus creencias y en sus decisiones comerciales y políticas.161

Remitiéndose a la decisión del Tribunal Constitucional alemán de 1984, *Census*, Simitis subraya en qué medida la privacidad facilita el ejercicio de otros derechos, como las libertades de expresión, de asociación y de reunión. Como ninguno de esos derechos «puede ejercerse plenamente mientras permanezca la incertidumbre de las circunstancias y los fines de la obtención y el tratamiento de la información personal», sostiene que una pérdida de privacidad siempre constituirá también una pérdida de «sustancia democrática».162 La protección de la privacidad debe convertirse en algo más que la mera protección de un derecho concreto. Más bien, el nivel de protección concedido a los individuos puede «determinar la elección entre

una sociedad democrática y una autoritaria».[163]

El Tribunal hizo una observación similar en su decisión.[164] En particular, señaló que las personas que no están seguras de si su comportamiento se percibe realmente por quienes tienen poder sobre ellas podrían verse significativamente inhibidas en el ejercicio de otros derechos que, en general, se perciben como importantes derechos de participación política (lo que incluye, por ejemplo, su libertad de asociación o reunión).[165] Esto, según el tribunal, tiene efectos que van más allá de los propios individuos. Por el contrario, la autodeterminación informativa es «un requisito previo elemental para el funcionamiento de una sociedad democrática libre basada en la libertad de acción y participación de sus miembros». A diferencia de las visiones tradicionales de la libertad y la autodeterminación, el tribunal consideró que esos derechos no existen de forma independiente. Al contrario: la libertad individual y el interés público (en la existencia de una sociedad libre) se enmarcan como objetivos iguales de protección constitucional.

6. Relación de la privacidad con otros derechos y valores

Los derechos a la privacidad y a la protección de datos no son derechos absolutos. Uno de los principios fundamentales de los derechos humanos es que todos ellos están relacionados entre sí y dependen los unos de los otros. Las incursiones en estos derechos y las excepciones a los mismos son posibles cuando son necesarias para conciliar la privacidad y la protección de datos con otros derechos e intereses de la sociedad. En su Observación general sobre el artículo 17 del ICCPR, el CDH de la ONU establece que, a menos que esté motivado por la ley y solo cuando sea esencial en interés de la sociedad, no se debe interferir en la vida privada.[166]

El artículo 8 del CEDH reconoce, asimismo, que las injerencias en el derecho al respeto de la vida privada son permisibles cuando persiguen un fin legítimo, son conformes a derecho y son proporcionadas, es decir, vayan más allá de cuanto se requiera para alcanzar dicho fin. Tales disposiciones habilitantes garantizan que los derechos a la protección de datos y a la privacidad cedan el paso a otros derechos e intereses cuando sea deseable, si bien solo en la medida necesaria para lograrlos.[167]

Por citar un ejemplo de estas interacciones, consideremos el artículo 27 de la DUDH, que establece que «toda persona tiene derecho a participar libremente en el progreso científico y en los beneficios que de él resulten». Dados los actuales protocolos de investigación, no cuesta imaginar escenarios en los que, si alguien se viera obligado a ceder datos personales para compartir la innovación científica de la era digital, esto podría suponer una contravención del artículo 27. Asimismo, el artículo 29 establece que «en el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática».

Por lo que —debe decirse— incluso la privacidad como derecho fundamental debe contextualizarse. Como ya se ha comentado, la conciliación de la privacidad y la protección de datos con otros derechos e intereses es posible y, en diversas circunstancias, el respeto de tales derechos es clave o, como mínimo, facilita el logro de otros derechos e intereses relevantes de las personas como, por ejemplo, la libertad de expresión. Otro ejemplo es el derecho a formarse y mantener libremente una opinión en virtud de la DUDH (artículo 19), donde se establece un claro vínculo entre la privacidad y los derechos a la autonomía y a formarse una opinión.[168] Por tanto, estos derechos podrían clasificarse correctamente como derechos cualificados y derechos habilitantes.

A. Seguridad

La seguridad pública y nacional suele citarse más a menudo como un derecho que entra en conflicto con los derechos a la privacidad y a la protección de datos. Así es, especialmente, desde los atentados del 11 de septiembre de 2001 en Estados Unidos, que desencadenaron una serie de nuevas leyes que otorgaron a las fuerzas del orden y a los servicios de seguridad/inteligencia poderes amplios para recopilar y tratar los datos personales de los ciudadanos. De hecho, la seguridad nacional es uno de los intereses que se enumeran, de forma específica, en muchos instrumentos de derechos humanos, como motivo para restringir derechos cualificados como la

privacidad y la protección de datos.[169]

Como consecuencia, los instrumentos de derechos humanos y los tribunales de derechos humanos han desarrollado robustas salvaguardias sustanciales y procesales para limitar la interferencia por los servicios policiales y de seguridad a lo necesario y proporcionado. Por ejemplo, en *Klass contra Alemania,* el Tribunal Europeo de Derechos Humanos insistió en que cualquier excepción al derecho a la privacidad, especialmente cuando la medida en cuestión facilita la vigilancia de las comunicaciones de los ciudadanos, debía interpretarse de forma restrictiva. Sostuvo que, «los poderes de vigilancia secreta de los ciudadanos, que caracterizan como lo hacen el estado policial, son tolerables en virtud del Convenio solo en la medida estrictamente necesaria para salvaguardar las instituciones democráticas».[170] Además, en 2021 el TJUE determinó en el asunto C-746/18 (Prokuratuur) que el acceso a un conjunto de datos de tráfico o de localización con fines de investigación criminal, que proporciona conclusiones precisas sobre la vida privada de una persona, «solo está permitido para combatir delitos graves o prevenir amenazas graves para la seguridad pública». [171]

B. Participación política

Relacionada con la cuestión de la seguridad, está la amenaza que las restricciones a la privacidad y la protección de datos representan para las instituciones democráticas. Así lo ha documentado, por ejemplo, el relator especial de la ONU sobre los derechos a la libertad de reunión pacífica y de asociación.[172] Bennett y Raab han argumentado que, en el contexto de gran parte de las políticas públicas actuales, la privacidad se considera un obstáculo que debe superarse porque entra en conflicto con valores públicos o comunitarios como la seguridad nacional o, actualmente, la sanidad pública.[173] Sin embargo, esto ignora el hecho de que la privacidad es en sí misma un valor social o público que respalda otros objetivos de la administración pública. Por ejemplo, una buena protección de la privacidad de los votantes (por ejemplo, voto secreto, voto por correo y anticipado, etc.) crea una mayor participación electoral y satisfacción con el proceso y, por tanto, fomenta el objetivo de la participación política.[174]

En otros ámbitos, esto también sugiere que la comodidad y eficacia que las entidades, tanto públicas como privadas, obtienen de la creación de grandes almacenes de datos (por ejemplo, registros sanitarios nacionales centralizados) o métodos de vigilancia ubicua (como las cámaras de seguridad, las tecnologías de reconocimiento facial o el seguimiento del comportamiento en línea) deben sopesarse considerando la posibilidad de abusos. Unas medidas de seguridad técnicas y reglamentarias eficaces pueden evitar que el «estado de base de datos» se convierta en el equivalente virtual del famoso modelo carcelario del Panóptico de Jeremy Bentham. Se debe a que la «mirada desigual» que caracteriza a este tipo de vigilancia conlleva el riesgo de provocar la interiorización de una mentalidad disciplinaria en las personas observadas. Si bien, por un lado, esto significa que los individuos que viven bajo esa mirada tienen menos probabilidades de infringir las normas o las leyes; por otro, pueden verse disuadidos de ejercer sus derechos y libertades individuales o de participar en general en el proceso democrático. Según Bloustein, «la privacidad protege nuestros deseos individuales frente a la presión conformista».[175]

Además, es probable que el uso incontrolado de datos personales por las autoridades públicas tenga también otras repercusiones negativas en la sociedad, como en la confianza social y la coherencia social. Lyon ha defendido que los medios automatizados de tratamiento de datos pueden conducir a una situación en la que «los seres humanos son desviados como flujos de datos, para su reconstitución como «imágenes de datos» en las bases de datos de las autoridades».[176] Lo que ha quedado claro en los últimos años es que, si los usuarios de datos pueden utilizar esas imágenes de datos con el fin de elaborar perfiles de riesgo, dicha elaboración de perfiles puede acabar siendo una forma de «categorización social» que puede privilegiar a algunos ciudadanos y perjudicar a otros al incluirlos en «categorías sospechosas» antes de delinquir.[177] Significa, pues, que lo que empieza como un problema de recopilación excesiva sin objetivos concretos deviene en posible discriminación y maltrato de personas concretas.

Además, los sistemas de elaboración de perfiles también representan un riesgo «de reproducir y reforzar las divisiones sociales, económicas y culturales en las sociedades de la información». [178] Las medidas que socavan la confianza social también socavan, al enfatizar el comportamiento individual, la solidaridad social.[179] En este contexto, Regan resalta la importancia de la privacidad para evitar la fragmentación del ámbito público al animar a los individuos a operar en él basándose en sus puntos en común y no en sus diferencias.[180] Bennett y Raab señalan, además, que la categorización social puede acarrear desigualdades en materia de privacidad cuando el «ámbito público político se ve perjudicado si la restricción del poder arbitrario solo puede ejercerse por determinadas personas o categorías, tal vez privilegiadas por su privacidad».[181] La existencia de «los que tienen privacidad» y «los que no la tienen» puede, por tanto, ser tan perjudicial para el tejido social como las intrusiones en la privacidad practicadas por instituciones públicas y privadas.

C. Sanidad pública y otros intereses públicos

En los últimos tiempos, la cuestión de la sanidad pública ha estado en el primer plano de la conciencia pública. Muchos estados han propuesto respuestas a la pandemia de COVID-19 basadas en los datos, lo que suscita preocupación, por un lado, sobre la compatibilidad de tales iniciativas con los derechos fundamentales y, por otro, sobre la posibilidad de que la protección de los derechos fundamentales impida dar respuestas eficaces a la pandemia.[182] Un ejemplo principal de respuesta a la pandemia basada en los datos ha sido el despliegue de aplicaciones de «rastreo de contactos» en estados de todo el mundo. Se trata de aplicaciones que constituyen un excelente ejemplo de la naturaleza cualificada de los derechos a la privacidad y a la protección de datos, así como del papel que el respeto de estos derechos desempeña en el fomento de la confianza pública.[183]

Aplicaciones móviles de localización de contactos

Las aplicaciones de rastreo de contactos detectan cuándo un dispositivo móvil se acerca a otro y registran este encuentro. El registro de contactos puede mantenerse en el dispositivo o en un servidor centralizado. Si una persona presenta síntomas relevantes o da positivo en las pruebas de COVID-19, esta información puede introducirse en la aplicación. Seguidamente, se calcula el riesgo de que otros contactos contraigan la enfermedad, ya sea en el dispositivo o en un servidor centralizado, y se notifica a los contactos «de riesgo». Las aplicaciones basadas en el tratamiento de datos personales, tanto centralizado como descentralizado, suponen una injerencia en los derechos a la privacidad y a la protección de datos. No obstante, siempre que tales injerencias sean cumplan la ley y se establezcan las salvaguardias pertinentes para minimizarlas, tales aplicaciones se consideran compatibles con estos derechos. Por ejemplo, en Inglaterra y Gales, la aplicación original propuesta por el Servicio Nacional de Salud (NHS) y apoyada por el gobierno recogía los detalles de los encuentros próximos en un servidor centralizado en el que también se calculaba el riesgo de infección antes de comunicarlo a las personas afectadas. Atrajo mucha publicidad negativa por no articular claramente los fines del tratamiento centralizado de datos y quién accedería a ellos, así como por no cumplir el requisito de la limitación del almacenamiento y otras salvaguardias básicas de protección de datos. Respetar estos derechos fundamentales podría reforzar la confianza del público en estas aplicaciones, lo que mejoraría su eficacia general, ya que las investigaciones sugieren que tasas de uso elevadas (del 60 % de la población o más) son fundamentales para su eficacia.

Así pues, pese a que pueda existir la tentación de dejar de lado o limitar la aplicación de estos derechos en momentos de agitación como una pandemia, la existencia de marcos jurídicos que den expresión a estos derechos puede ayudar. De hecho, la ausencia de regulación para proteger estos derechos, o una regulación muy limitada (por ejemplo, que solo se aplique a los proveedores de servicios de la sanidad pública), podría dejar la puerta abierta a una amplia gama de actores que ofrecen aplicaciones de rastreo de contactos. En el contexto de las aplicaciones de rastreo de contactos, una aplicación fiable respetuosa con los derechos humanos es infinitamente superior a una diversidad de aplicaciones competidoras de calidad cuestionable.

D. Libertad de expresión

Se atribuye a internet el mérito de desintermediar la palabra: antes, la comunicación de masas solo estaba al alcance de interlocutores privilegiados —como las cadenas de televisión y radio y la prensa escrita—; ahora, cualquiera que disponga de un dispositivo conectado a internet tiene la capacidad de transmitir a las masas. Al permitir a individuos y grupos conectar con nuevas audiencias y descubrir nuevos contenidos, internet también desafió las fronteras territoriales tradicionales. En general, se considera una evolución positiva desde el punto de vista de la libertad de expresión e información. Sin embargo, ha hecho que la libertad de expresión e información entre en tensión cada vez con más frecuencia con los derechos a la privacidad y a la protección de datos. Constituye su ejemplo más destacado la aplicación del llamado «derecho al olvido». Sin embargo, lo que la aplicación del «derecho al olvido» ilustra es que, si no se tratan como derechos absolutos, ni la libertad de expresión e información, ni la protección de datos y la privacidad pueden conciliarse de manera que se respete la esencia de todos los derechos.

El «derecho al olvido»

El «derecho de supresión» recogido en la legislación de protección de datos de la UE puede invocarse por una persona contra un motor de búsqueda cuando se utiliza su nombre como término de búsqueda para que se eliminen ciertos enlaces de los resultados obtenidos. En la sentencia *España* TJUE el Tribunal indicó que esa supresión, en ese caso de información relativa a una insolvencia de casi dos décadas antes, podía producirse cuando el tratamiento de datos fuera incompatible con la legislación de protección de datos. En la práctica, la conclusión obligó al Tribunal a conciliar los derechos a la protección de datos y a la privacidad de la persona afectada con la libertad de expresión e información de los usuarios del motor de búsqueda de Google. Al hacerlo, el Tribunal sostuvo que, por regla general, los derechos a la protección de datos y a la privacidad del individuo tendrían prioridad sobre el interés del público en recibir esta información, a menos que exista un interés preponderante del público en recibirla. El Tribunal indicó que, dada la sensibilidad de la información para la persona afectada y el que los acontecimientos a los que se refería habían ocurrido 16 años antes, había circunstancias determinadas en que el vínculo debía suprimirse. La jurisprudencia subsiguiente en el Reino Unido y Alemania ha reajustado la «norma general» para equilibrar más la balanza entre la protección de datos y la privacidad y la libertad de expresión. Aunque el ajuste es inevitable, el carácter cualificado de las conclusiones del Tribunal siempre ha permitido esta conciliación. Debe señalarse una serie de salvedades importantes.

- Si bien la sentencia provocó alegaciones de que se estaban suprimiendo materiales «legales» de los motores de búsqueda, los materiales suprimidos son «ilegales» por ser incompatibles con la ley de protección de datos. El derecho de supresión no confiere al individuo el derecho a que se suprima la información que desee. Lo decisivo es la compatibilidad con el marco jurídico, y no las preferencias subjetivas individuales o el hecho de que la información haya perjudicado al individuo afectado.

- El derecho no exige que los datos personales se supriman del registro histórico. El Tribunal distinguió entre la publicación por el sitio web original y la disponibilidad de la información en el motor de búsqueda de Google, que, en comparación con los editores de sitios web, afecta «significativa y adicionalmente» a los derechos fundamentales a la privacidad y a la protección de datos. (*Google España*, apartado 38). El razonamiento anterior reconoce que la publicación y distribución en diferentes contextos puede surtir efectos cualitativamente diferentes en los derechos a la protección de datos y a la privacidad.

- El derecho no se aplica cuando el interesado desempeña un papel en la vida pública; por ejemplo, «altos funcionarios públicos, empresarios y miembros de profesiones (reguladas)». Significa, en la práctica, que las solicitudes de exclusión de la lista «tendrán sistemáticamente en cuenta el interés del público en poder acceder a la información». Si el interés del público prevalece sobre los derechos del interesado, la exclusión de la lista no procederá». Al reconocer que no toda la información que interesa al público es de interés público, estos derechos pueden conciliarse en el marco del respeto hacia los principios básicos de todos.

También es importante recordar el papel de la protección de datos y la privacidad para posibilitar el derecho a la libertad de expresión e información. La privacidad es co-constitutiva de la libertad de expresión[184] y se ha descrito por un antiguo relator de la ONU sobre la libertad de expresión «como una puerta de entrada para la libertad de opinión y expresión».[185] Richards explica elocuentemente esta función facilitadora al defender nuestra «privacidad intelectual»: un tipo de privacidad necesaria tanto para los intelectuales como para todos nosotros mismos. [186] Desde una perspectiva normativa, sostiene que la privacidad intelectual es el fundamento de la libertad de expresión. Reconoce que la libertad de pensamiento y creencia es necesaria para el desarrollo de nuevas ideas y para que los ciudadanos puedan «decidir por sí mismos sobre ideas grandes y pequeñas, políticas y triviales».[187] La privacidad es condición previa para este tipo de pensamiento.

Desde un punto de vista empírico relacionado, en ausencia de privacidad, cuando se nos vigila (por agentes públicos o privados), hay pruebas que sugieren que nuestra libertad de pensamiento y acción se ve afectada. Richards sostiene que «cuando se nos vigila mientras desempeñamos actividades intelectuales, definidas en sentido amplio —pensar, leer, navegar por Internet o comunicarnos en privado——, se nos disuade de participar en pensamientos o actos que otros podrían considerar relevantes».[188] Podemos ver, por consiguiente, que la privacidad protege aspectos clave de la expresión, que van desde la formación inicial de la opinión hasta su difusión subsiguiente. Establece las condiciones ambientales en que la libertad de expresión puede florecer.

Además, más allá de la necesidad de privacidad intelectual, es posible prever muchas circunstancias en las que la denegación de acceso a la información puede constituir en sí misma una violación del derecho a la vida privada. Tenemos un vívido ejemplo de ello en la causa emprendida contra el gobierno irlandés por *Open Door y Dublin Well Woman*.[189] Los demandantes habían sido objeto de una medida cautelar que les impedía proporcionar determinada información a las mujeres embarazadas mediante asesoramiento no directivo sobre los servicios de aborto. Alegaron que la denegación del acceso a la información relativa al aborto en el extranjero constituía una injerencia injustificable en su derecho al respeto de la vida privada, además de una violación de su libertad de recibir esta información.[190]

La relación entre privacidad y protección de datos y libertad de expresión e información es polifacética. Como ocurre con el derecho al olvido, cuando entran en conflicto, cada uno de estos derechos cede terreno para dar cabida al otro. En otras circunstancias, estos derechos son dos caras de la misma moneda, que se complementan y apoyan mutuamente. Por ejemplo, la experiencia de muchos grupos marginados es que su derecho a la libertad de expresión a menudo solo puede protegerse y ejercerse con un derecho tangible a la privacidad (por ejemplo, los adolescentes LGBTQ2SI que viven con adultos homófobos o transfóbicos, o las mujeres en situaciones de maltrato doméstico).[191]

E. Igualdad y no discriminación

En la era moderna, la igualdad, la no discriminación y la privacidad están intrínsecamente unidas».

El derecho a la privacidad puede permitir a grupos de personas marginadas buscar una comunidad común sin miedo, organizarse y protestar, y defender sus derechos

de igualdad.[192] También puede proteger a los niños de cualquier daño y contribuir a su desarrollo pleno e igualitario. Puede permitir a las personas con discapacidad recibir servicios accesibles y espacios o entornos adaptados sin verse obligadas a revelar en exceso información médica personal. Puede ayudar a las mujeres y a las personas LGBTQ2SI a encontrar seguridad y aceptación, y a buscar salidas a la violencia doméstica o los malos tratos. Puede ayudar a protegerlas del acoso en línea y de los delitos de odio en el mundo real.[193].

También puede permitir una realización más significativa de otros derechos de igualdad.

Los nuevos usos de la IA son especialmente preocupantes cuando se utilizan donde las personas son vulnerables y pueden tener poca información o recursos sobre cómo hacer valer su privacidad o sus derechos humanos. Esto es especial y alarmantemente cierto en el caso de los niños,[194] cuyas vidas se ven cada vez más profundamente afectadas por la tecnología de vigilancia desde que nacen.[195] En medio de los debates críticos y en rápido desarrollo de la ONU,[197] regionales,[198] y nacionales[199] sobre gobernanza, regulación y orientación,[200] y la importancia de los derechos humanos en estos marcos y debates.[201] Organismos de la ONU,[202] organizaciones de la sociedad civil,[203] defensores de los derechos humanos,[204] institutos académicos y de investigación,[205] comisionados de privacidad[206] e instituciones nacionales de derechos humanos[207] tienen importantes funciones que desempeñar en estos debates sobre cómo garantizar la protección plena de los derechos humanos y su mejora a medida que la tecnología avanza.

Afrontar la discriminación algorítmica

En su informe *Más cerca de la máquina*, la Oficina del Comisionado de Información de Victoria ofrece varios ejemplos de formas algorítmicas de discriminación en contextos tanto del sector público como del privado; incluido, por ejemplo, el uso por Amazon de una herramienta de contratación experimental que escaneaba y puntuaba los currículos de los solicitantes de empleo, y que estaba sesgada hacia los hombres, ya que la IA había sido entrenada utilizando un conjunto de datos compuesto predominantemente por currículos masculinos (p. 29/30). El informe (p.32) identifica factores que actúan como barreras para comprender cuándo se ha producido discriminación algorítmica. Entre dichos factores se incluyen los siguientes:

- La persona afectada puede no darse cuenta de que la decisión ha sido tomada por un sistema de IA.
- El usuario del sistema de IA puede no estar obligado a dar explicaciones, sobre todo en un entorno comercial.
- El diseñador del sistema de IA puede resistirse a revelar su proceso de razonamiento para mantener las ventajas comerciales y competitivas y el secreto.
- La pista de auditoría del sistema de IA puede no identificar qué factores se consideran especialmente relevantes para la decisión o recomendación realizada por el sistema de IA.

El RGPD de la UE establece el derecho a una explicación, que incluye la obligación de informar al individuo sobre la «existencia de la toma de decisiones automatizada, incluida la elaboración de perfiles» e «información significativa sobre la lógica implicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado». Esta obligación se aplica tanto en la primera obtención de datos personales en un plazo razonable a partir de entonces (artículo 13, apartado 2, letra f), y artículo 14, apartado 2, letra g), del RGPD) como cuando que el tratamiento de datos personales está en curso (artículo 15, apartado 1, letra h), del RGPD). En una línea similar, el Convenio 108 modernizado otorga a las personas físicas el derecho a obtener, previa solicitud, «el conocimiento de los motivos en que se basa el tratamiento de datos cuando los resultados se apliquen al interesado» (artículo 9, apartado 1, letra c)). Por consiguiente, la legislación sobre protección de datos ayuda a superar los obstáculos que impiden comprender la discriminación algorítmica y detectar las prácticas discriminatorias.

También cabe señalar que, desde el punto de vista operativo, en muchos estados, aunque un instrumento internacional o una constitución nacional con disposiciones en materia de igualdad puedan vincular las acciones del estado, es posible que no se ofrezca responsabilidad o remedio frente a las acciones de las empresas privadas. Los códigos nacionales de derechos humanos, de naturaleza cuasiconstitucional, constituyen una importante protección legislativa adicional. Pueden fomentar la igualdad y el derecho a la privacidad, y hacer que tanto el sector público como el privado rindan cuentas por igual en caso de discriminación. En muchos Estados, las instituciones nacionales de derechos humanos (como las comisiones de derechos humanos) coexisten con comisionados nacionales o regionales de protección de la privacidad, y pueden apoyar y complementar mutuamente su labor tanto en el ámbito de la igualdad como en el de la protección de la privacidad.

Otro tipo de relación entre la protección de datos y la privacidad y el derecho a la igualdad se centra principalmente en el papel de la protección de datos y la privacidad en la ocultación o revelación de prácticas discriminatorias. En ocasiones, se dice que las normas sobre el tratamiento de información personal sensible frenan los esfuerzos de recopilación de datos con el fin de evaluar y mitigar la discriminación.[208] Por ejemplo, Binns y Veale sugieren que muchos métodos para abordar la discriminación en los sistemas algorítmicos suponen implícitamente que las organizaciones disponen de estos datos confidenciales, cuando es posible que no sea así para garantizar el cumplimiento del marco de protección de datos.[209]

Sin embargo, lo más frecuente es que los derechos a la privacidad y a la protección de datos sirvan de apoyo a los esfuerzos para combatir la discriminación. De hecho, algunos de los primeros documentos internacionales sobre protección de datos y privacidad —dos Resoluciones del Consejo de Europa sobre la protección de la privacidad en los bancos de datos electrónicos— establecen salvaguardias que deben aplicarse «especialmente cuando los bancos de datos electrónicos procesan información relativa a la vida privada íntima de las personas o cuando el procesamiento de la información puede dar lugar a una discriminación injusta».[210] Además, muchos marcos modernos de protección de datos contienen un principio general de procesamiento «justo» de los datos personales, que se entiende como «no discriminatorio», entre otras cosas.[211] Por ejemplo, el «Marco Civil da Internet» brasileño enumera entre los principios generales para el tratamiento de datos personales la «no discriminación» en lugar de la equidad, lo que indica que el legislador brasileño consideró que la no discriminación era el elemento crítico de equidad que debía protegerse.[212] De forma similar, la Autoridad Francesa de Protección de Datos, en un reciente informe sobre Algoritmos e IA, ha concluido que «un *algoritmo justo* no debería acabar generando, replicando o agravando ninguna forma de *discriminación*».[213]

7. Pasos siguientes: Opciones para el desarrollo de los derechos a la privacidad y a la protección de datos

Visto el valor, tanto inherente como instrumental, que los derechos a la protección de datos y a la privacidad tienen para las personas y la sociedad, está justificado el esfuerzo por reforzar su reconocimiento y aplicación. No obstante los claros vínculos entre la protección de datos y la privacidad y otros derechos, como se ha señalado, todavía no hemos logrado una protección óptima de ninguno de ellos. Si bien son muchos los factores que contribuyen a esta falta de remedio eficaz, merece la pena mencionar dos.

En primer lugar, como ya se ha dicho, pese a la proliferación de regímenes de protección de datos en todo el mundo,[214] existen distinciones cada vez mayores entre los marcos de protección de la privacidad y de protección de los datos. Por un lado, hay regímenes que se apoyan en los derechos fundamentales y garantizan los derechos de los individuos y de la sociedad. Por el contrario, los hay más orientados al mercado y que anteponen la garantía de los intereses de la liberalización de los datos. Ambos modelos tienen poderosos defensores. Sin embargo, desde la óptica del recurso individual, cuantos más países se orienten hacia el modelo de los derechos fundamentales e interpreten sus marcos normativos de manera que promuevan la protección de los derechos, más eficaz será la protección.

En segundo lugar, para los países que sí abogan por un enfoque de derechos fundamentales para la protección de datos personales, es importante que la ley se implemente de forma efectiva en la legislación local y, seguidamente, se aplique y se haga cumplir. Esto incluye la creación de una autoridad independiente que supervise la aplicación de la protección de datos y garantice que se facilita su labor dotándola de los recursos adecuados y que no haya interferencias externas. La regulación pública debe reforzarse mediante procedimientos de recurso privado, que reconozcan y faciliten las acciones individuales por daños y perjuicios, así como las acciones representativas para abordar fallos colectivos y sistémicos en la protección de datos.

En la actualidad, a escala tanto nacional como internacional, los instrumentos de protección de datos y privacidad existentes no se aplican del modo adecuado. El no abordaje de estas dificultades vaciará de contenido la legislación sobre protección de datos, de modo que el que debería ser un mecanismo eficaz para la protección de los derechos y la mejora de la confianza y la rendición de cuentas en la era digital pasará a consistir en el mero marcado de una casilla que legitima el uso indebido y el abuso en lugar de oponerse a ellos.

Habida cuenta de la importancia de garantizar la protección efectiva de los datos y la privacidad, surge la cuestión de cómo garantizar esa protección efectiva de los derechos. En este caso, la opción principal es abogar por nuevos instrumentos jurídicos que reconozcan explícitamente la dimensión de derechos fundamentales de la protección de datos y la privacidad, o abogar por el refuerzo y la mejora de las protecciones jurídicas nacionales e internacionales existentes.

En las últimas décadas, muchos estados europeos han introducido la protección constitucional de los datos en sus ordenamientos jurídicos internos. Más recientemente, por ejemplo, en Luxemburgo, un proyecto de reforma constitucional prevé la inclusión de un derecho a la «autodeterminación informativa» en la Constitución (además del actual derecho a la privacidad recogido en el artículo 11(3)). El derecho a la protección de datos de la Carta de la UE y la jurisprudencia alemana sobre autodeterminación informativa inspira explícitamente esta propuesta.[215] Si bien ofrece la ventaja de una base jurídica firme para los derechos a la protección de datos y a la privacidad, este enfoque también corre el riesgo de ser un engorro en los estados en los que la reforma constitucional requiere importantes pasos procedimentales (como la aprobación por referéndum). El cambio de los tratados de nivel internacional puede ser aún más prolongado. He ahí por qué el segundo enfoque, el refuerzo de la protección nacional e internacional existente, es preferible. Además de ser más realista, es más respetuoso con los diferentes contextos constitucionales y culturales de los estados.

A. Maximizar el potencial de la protección existente en el ámbito doméstico

El enfoque inmediato, y, por tanto, pragmático, para garantizar el reconocimiento generalizado de la naturaleza basada en los derechos de la legislación sobre protección de datos consiste en abogar por el reconocimiento explícito de los derechos a la protección de datos y a la privacidad en los estatutos y los marcos constitucionales nacionales, según proceda. Las constituciones nacionales y los tribunales supremos suelen disponer del recurso a las disposiciones constitucionales existentes para reconocer estos derechos. Como se ha comentado, esta ha sido la vía seguida por el Tribunal Constitucional alemán al desarrollar un derecho a la autodeterminación informativa basado en los derechos existentes a la dignidad humana y a la autodeterminación en la Ley fundamental alemana.

Este fue también el enfoque adoptado por el Tribunal Supremo de la India en la sentencia *Puttaswamy* de 2017. En ella, el Tribunal Supremo concluyó por unanimidad que el derecho a la privacidad es un derecho constitucionalmente protegido en la India, aunque la Constitución india no lo prevea explícitamente. El tribunal, de nueve jueces, emitió seis dictámenes distintos, cada uno de los cuales difería sutilmente en cuanto al razonamiento. Sin embargo, los dictámenes compartían la opinión de que la privacidad no podía desvincularse de otros derechos constitucionales existentes, como la libertad, la dignidad y la libertad de expresión. Como dice la sentencia:

> La privacidad no se ha formulado como un derecho fundamental independiente. Sin embargo, una vez comprendida la verdadera naturaleza de la privacidad y su relación con aquellos derechos fundamentales expresamente protegidos, ello no le resta protección constitucional. Abarca todo el espectro de libertades protegidas.[216]

Este razonamiento ofrece un ejemplo prometedor para el desarrollo de los derechos de privacidad y protección de datos en otras jurisdicciones. Lo que también es pertinente acerca de la sentencia principal (de DY Chandrachud J) es que, además de su compromiso detallado con la jurisprudencia nacional sobre privacidad y los derechos constitucionales, también examinó muchas otras jurisdicciones, incluido el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos, así como los principales estudios sobre privacidad, y se inspiró en ellos. Este intercambio de ideas y desarrollos jurisprudenciales también podría servir para facilitar el reconocimiento de estos derechos en otras jurisdicciones.

Este enfoque presenta la ventaja de que, si el ordenamiento jurídico nacional lo permite, no requiere ninguna reforma constitucional radical ni ninguna otra reforma legal. Para evaluar la viabilidad de la promulgación de la privacidad de esta manera, podría partirse del examen del marco constitucional y la jurisprudencia existentes e identificar los elementos comunes en los que se podría basar un derecho a la privacidad, así como las competencias de los tribunales para interpretar y reconocer los derechos fundamentales. Cuando esto parezca plausible, la comunidad de protección de datos y privacidad (reguladores; organizaciones internacionales, como el Consejo de Europa, académicos y otras partes interesadas) podría trabajar con organizaciones locales para aportar conocimientos especializados y participar en la capacitación y concienciación sobre cuestiones de protección de datos y privacidad.

B. Fomentar la convergencia en torno a los instrumentos internacionales existentes basados en derechos

En lugar de intentar alcanzar un consenso en torno a un nuevo instrumento internacional de protección de datos, quizás sea preferible asegurar la convergencia en torno a un instrumento internacional existente basado en los derechos. Al considerar qué instrumento sería el mejor, hay tres candidatos que deben tenerse en cuenta.

La primera opción podría ser fomentar una mayor convergencia sobre los principios de protección de datos y privacidad bajo los auspicios de la disposición existente sobre privacidad en el ICCPR. En concreto, se perseguiría fomentar el cumplimiento y la aplicación del derecho consagrado en el ICCPR y garantizar que su interpretación y aplicación se adaptan a la era digital. Por ejemplo, el CDH de la ONU podría adoptar una «Observación General» nueva y actualizada sobre el artículo 17 del ICCPR, reconociendo los intereses colectivos a los que el derecho a la privacidad sirve y modernizando su interpretación del artículo 17.

Sin embargo, dado que los enfoques existentes de la ONU en este ámbito no han triunfado, el planteamiento es arriesgado. En particular, la amplia composición de la ONU incluye estados firmemente comprometidos con enfoques de protección de datos basados en la economía, así como con enfoques basados en los derechos. Existe el riesgo de que estas perspectivas mixtas sobre el papel adecuado de la protección de datos en un entorno digital acaben debilitando cualquier protección que se ofrezca a través de la ONU.

La segunda opción consistiría en fomentar la convergencia en torno al RGPD de la UE como norma internacional. Las disposiciones sustantivas del RGPD para el tratamiento de datos personales son innumerables y están minuciosamente detalladas, ya que se redactaron en el considerando que el tratamiento de datos

personales tiene ramificaciones en los derechos fundamentales y que, por lo tanto, debe estar sujeto a sólidas salvaguardias. Además, muchos estados de todo el mundo ya conocen estas normas. En algunos, el RGPD se ha tenido en cuenta explícita o implícitamente al redactar la legislación nacional en un intento de garantizar una conclusión de «adecuación» necesaria para garantizar los flujos de datos transfronterizos entre estados de la UE y de fuera de la UE.[217].

No obstante, la opción de la convergencia en torno a la norma del RGPD puede no ser la más deseable por varias razones. Y lo que es más importante, puesto que se anuncia como un «patrón oro» para la protección de datos y se ha diseñado para garantizar más integración europea mediante disposiciones estrictas y prescriptivas, el RGPD puede estar fuera del alcance inmediato como norma jurídica para muchos estados. Además, en la actualidad los únicos países no pertenecientes a la UE que han firmado el RGPD son estados del espacio económico europeo (Islandia, Liechtenstein y Noruega). Actualmente, no hay otro mecanismo previsto para que los Estados no pertenecientes a la UE ni al EEE se adhieran oficialmente a las normas del RGPD.

La tercera opción — y quizás la más viable— es, por tanto, fomentar la convergencia en torno al Convenio 108+ del Consejo de Europa. El Convenio 108+ «moderniza» el Convenio 108 original mediante un Protocolo modificativo (STCE n.º 223). Las ventajas de apoyar una mayor convergencia internacional a través del Convenio 108+ se describen a continuación.

En primer lugar, si bien el Convenio 108+ no entrará en vigor antes del 2023, los Estados signatarios no europeos ya pueden solicitar la adhesión a este instrumento.[218] Pese a que todavía no se han ultimado los detalles del «mecanismo de evaluación y seguimiento» previsto por el Convenio 108+, las solicitudes de adhesión al Convenio se evaluarán inicialmente por el «Comité del Convenio», el cual valorará la eficacia de las medidas que el estado (u organización internacional) solicitante haya adoptado para hacer efectivas las disposiciones del Convenio.[219] Tras esta evaluación, el Comité del Convenio emite un dictamen positivo o negativo sobre la admisibilidad del estado solicitante, que se envía al Comité de Ministros del Consejo de Europa.[220] En la actualidad, ocho estados no miembros del Consejo de Europa han ratificado el Convenio 108, mientras que tres han firmado y uno ha ratificado el Convenio 108+.[221] Los estados no europeos también actúan actualmente como observadores en el «Comité Consultivo» del Convenio 108 (que se sustituirá por el Comité del Convenio).[222].

Una gran ventaja del Convenio 108+ es que ya se ha diseñado para ser una norma internacional y multilateral de protección de datos y cuenta con los procedimientos pertinentes para la adhesión.[223] De hecho, el Consejo de Europa ha declarado que mantiene su compromiso de ayudar a las partes en

una rápida adhesión al Protocolo (STCE n.º 223) por parte del mayor número posible de los actuales estados parte en el Convenio n.º 108, con el fin de facilitar la formación de un régimen jurídico global de protección de datos en el marco del Convenio modernizado y, además, de garantizar la mayor representación posible de los Estados en el seno del Comité del Convenio.[224].

El Consejo de Europa ya tiene un modelo al fomentar la adopción de sus Convenios más allá de las fronteras europeas y garantizar que adquieran un carácter verdaderamente mundial. Por ejemplo, 21 partes no europeas han ratificado el Convenio sobre la Ciberdelincuencia.[225]

En segundo lugar, las normas previstas en el Convenio 108+ son más estrictas que las del Convenio 108, lo que garantiza que el instrumento esté en consonancia con la generación más reciente de leyes de protección de datos. Sin embargo, estas normas no son tan prescriptivas como las del RGPD de la UE, de modo que ofrecen un posible «término medio» y, a menudo, un importante margen de apreciación para muchos países. Como señala Greenleaf, entre las ventajas que la adhesión al Convenio 108+ ofrece a los estados se encuentra el «reconocimiento de las mejores prácticas», es decir, el reconocimiento de que «las normas de protección de datos de un país han alcanzado las “mejores prácticas internacionales”, en opinión de un grupo cada vez más global de homólogos del país».[226] Además, para los estados que deseen ir más allá de las normas establecidas en el Convenio 108+, esto no es óbice (véase el artículo 13 del Convenio 108+). Por tanto, el Convenio 108+ podría considerarse una norma mundial de protección de datos «lista para usar», preparada al nivel adecuado para una adhesión generalizada.

Una tercera ventaja de fomentar la convergencia en torno al Convenio 108+ como norma mundial de protección de datos, apoyada en los derechos fundamentales, es que dicho fomento ya existe. La Comisión Europea ha fomentado, por ejemplo, la adhesión de países no europeos al Convenio 108+ como «único instrumento multilateral vinculante en el ámbito de la protección de datos» y «ha promovido la rápida adopción del texto modernizado con vistas a que la UE se convierta en Parte».[227] Igualmente, el relator especial de la ONU sobre el derecho a la privacidad ha sugerido que se anime a los Estados miembros a ratificar el Convenio 108+ como «respuesta mínima provisional para acordar normas detalladas sobre la privacidad armonizadas a escala mundial».[228].

Esto no significa que la adhesión al Convenio 108+ deba considerarse una panacea para la privacidad y la protección de datos. Presenta dos dificultades fundamentales. El primer reto se refiere a las normas sustantivas. Como señala Greenleaf, para muchos países es poco probable que se cumplan pronto algunos de los requisitos previos para la adhesión (en particular, ser reconocido como estado y ser un estado democrático).[229] Por tanto, la adhesión, para estos estados, es una perspectiva poco realista a corto plazo. También es necesaria para la accesión la presencia de una autoridad de supervisión independiente y de normas que abarquen el tratamiento de datos tanto del sector público como del sector privado. Aunque factibles para otros estados, exigirían un cambio jurídico y cultural. Finalmente, no está claro que los reguladores existentes (por ejemplo, las instituciones nacionales de derechos humanos), los titulares de derechos o los defensores de la sociedad civil en general estén a favor de este enfoque específico. Así pues, antes de emprender reformas importantes, el gobierno debe consultar abiertamente a estos grupos y organismos.

Greenleaf señala varias formas de facilitar la adhesión de quienes quieran hacerlo. Son las siguientes:

- La publicación de un documento político por parte del Comité Consultivo que haga hincapié en los elementos más importantes de la evaluación de la adhesión;[230]
- La necesidad de que el Comité del Convenio 108+ (que acabará sustituyéndose por el Comité Consultivo) y el Comité de Ministros sean flexibles al aplicar la norma de adhesión del Convenio;[231]
- La evaluación de las perspectivas de adhesión por «analistas independientes o “no oficiales”, como “académicos”», para garantizar que se priorizan las solicitudes de adhesión viables y que existe una «base adecuada para el debate público sobre las perspectivas futuras de dichos acuerdos internacionales».[232]

Considerando estas recomendaciones, es evidente que, aunque todos los estados no pueden alcanzar actualmente las normas del Convenio 108+, existen formas de facilitar y agilizar la adhesión que el Consejo de Europa está dispuesto a apoyar.
Una segunda dificultad se refiere a la aplicación de las normas del Convenio 108+. Actualmente, el régimen vigente solo puede exigir responsabilidades a los signatarios del CEDH en caso de incumplimiento. No obstante, es necesario el establecimiento de un mecanismo sencillo, aunque no convencional, basado en el artículo 17 del Convenio 108+. El nuevo procedimiento podría representar un poderoso instrumento para la aplicación de casos individuales, incluso en contextos transfronterizos, y se basaría en la obligación de las autoridades supervisoras de cooperar entre sí, en particular a) prestándose asistencia mutua mediante el intercambio de información pertinente y útil y cooperando entre sí (...)

y b) coordinando sus investigaciones o intervenciones, o llevando a cabo acciones conjuntas. Sin embargo, si se considera que un estado parte ha infringido el Convenio modernizado, el apartado 3 del artículo 4 del Convenio 108+ debería aportar base suficiente al Comité del Convenio para a) evaluar la situación, b) recomendar medidas para conseguir el cumplimiento de las disposiciones del Convenio y c) aplicar sanciones basadas en las disposiciones del propio Convenio (como el apartado 1 del artículo 14) o en el Convenio de Viena sobre el Derecho de los Tratados. Sin duda, estas medidas podrían contribuir al cumplimiento nacional del Convenio o ser coherentes con este. Sin embargo, aún deben desarrollarse e implantarse para todas las partes existentes y futuras, lo que podría representar cierta dificultad.

Mientras tanto, otras partes y los órganos de la Convención (el Comité Consultivo, la Secretaría y el Consejo de Ministros) podrían intentar imponer el cumplimiento por medios diplomáticos, ya que se trata de un mecanismo no vinculante. Sin embargo, existen diversas posibilidades alternativas. Lo más evidente es que el 1.er Protocolo Facultativo del ICCPR se ha ratificado por 115 Estados miembros de la ONU. Permite, a quienes alegan que un signatario del Protocolo ha violado sus derechos reconocidos en el ICCPR y que han agotado todos los recursos internos disponibles, presentar una «comunicación» al Comité para su examen.[233] El CDH puede entonces emitir recomendaciones no vinculantes para el estado en cuestión.

También podría considerarse la posibilidad de hacer cumplir las disposiciones del Convenio 108+ a través de marcos regionales de derechos humanos, como el sistema interamericano de derechos humanos o el Tribunal Africano de Derechos Humanos y de los Pueblos. Las redes de protección de datos existentes (como APPA, GPEN, AFAPDP y el GPA) también podrían colaborar más de forma más activa con los mecanismos existentes de la ONU (como el Alto Comisionado para los Derechos Humanos, el relator especial del derecho a la privacidad y diversos comités) que ya participan en el análisis y la promoción del derecho a la privacidad en la era digital.[234]

C. Conclusión

Las pruebas, las tendencias, la jurisprudencia y los resultados examinados y comunicados —tanto en el cuerpo de este informe como en la revisión jurisdiccional que lo acompaña— conducen a nuestro grupo de trabajo de la GPA a las conclusiones que se enumeran a continuación. Algunas pueden parecer evidentes (incluso axiomáticas) para quienes trabajan en los ámbitos de la regulación de datos o la protección de derechos, ya que son fenómenos que llevan desarrollándose más de dos décadas. A continuación los reafirmamos con énfasis para orientar mejor las deliberaciones y las acciones futuras encaminadas a mejorar la situación del derecho a la privacidad en todo el mundo.

1. **La falta de una protección clara y rigurosa y una aplicación efectiva de los derechos de privacidad y protección de datos, pone en peligro otros derechos civiles y políticos de los ciudadanos de todo el mundo.** Al igual que la dignidad humana y la igualdad, la libertad de creencia, la libertad de circulación, el derecho a la libre asociación y la disidencia pacífica dependen de la protección de la privacidad y los datos. Cada uno está sometido a una presión constante por parte de agentes estatales y comerciales. Un mundo en el que los individuos encuentran, inevitablemente, la mirada de la vigilancia gubernamental y empresarial no puede calificarse de abierto, libre o justo.
2. **Toda solución o reforma propuesta a los problemas actuales debe ser viable más allá de las fronteras nacionales y aplicarse a todos los sectores de las distintas economías.** Los enfoques aislados de la regulación (como en los esfuerzos por lograr la equidad fiscal, la protección del medioambiente o la mejora de la salud pública) solo crean más lagunas, desigualdades, puntos ciegos y excepciones. Los derechos de los que disfrutan las personas fuera de línea deben aplicarse igualmente a su yo digital, y los derechos de privacidad que los ciudadanos esperan que respeten sus gobiernos deben ser igualmente observados por las entidades comerciales. Libre empresa no significa «todo gratis», y «laissez-faire» no puede significar que las empresas decidan lo que es justo. Las últimas décadas también han mostrado los defectos y limitaciones de la autorregulación de la industria y la necesidad de una protección vinculante y de recursos para que se apliquen los derechos.
3. **Las protecciones que las constituciones y leyes locales, los acuerdos bilaterales o los convenios y pactos internacionales ofrecen necesitan análisis, apoyo, promoción, educación y aplicación reales y efectivos en el mundo real.** Los derechos humanos, desvinculados de la realidad, que no permiten una reparación significativa o cuya búsqueda es demasiado compleja y costosa, son promesas vacías. Para que la rendición de cuentas sea realmente efectiva, los órganos de supervisión deben disponer de los recursos adecuados, ser políticamente independientes, disponer del personal apropiado y poder cooperar a nivel local y nacional con los titulares de derechos y sus defensores, y a nivel mundial con sus homólogos, los INDH, los órganos estatales, las organizaciones regionales e internacionales y los mecanismos de la ONU. Estos principios se aplican por igual a la regulación del gobierno y del comercio y a los instrumentos multilaterales existentes promulgados por la OCDE, la UE, el Consejo de Europa y la APEC. Sin una aplicación significativa y proactiva, los conjuntos de reglas revisados, las normas reeditadas y los nuevos protocolos no se respetarán ni serán creíbles.

4. **Las infracciones y violaciones de la privacidad y la protección de datos abarcan daños que van mucho más allá de la pérdida de datos personales.** Los intentos de la industria por limitar los debates sobre el tratamiento de la información y las salvaguardias de los sistemas minimizan gravemente los daños sufridos por las personas y las comunidades. La autonomía personal, la dignidad personal básica, la libertad de conciencia y el derecho inalienable a la autodeterminación individual (elección significativa) se ven erosionadas activamente por las malas prácticas en materia de datos, la aplicación desigual, el excepcionalismo jurídico, la captura reguladora o el retraso constante de los esfuerzos de reforma.
5. **Es necesario recordar a los gobiernos la importancia de la privacidad y la protección de datos para los fundamentos de la democracia.** La privacidad y la protección de datos no son un detalle social, una novedad urbana o una observación pintoresca de la sociedad educada. Por el contrario, son un cimiento de la imparcialidad electoral (por ejemplo, el voto secreto), las comunicaciones privadas (por ejemplo, los requisitos de orden judicial), y el debido proceso (por ejemplo, el derecho a acceder, revisar y solicitar que se corrija la información que se encuentra en poder del gobierno).
6. **Legisladores, cargos electos, miembros del poder judicial y reguladores designados tienen, todos, un papel en la reforma y el refuerzo de las instituciones de protección de los derechos.** Los derechos fundamentales no son libertades que externalicemos o dejemos en manos de los mercados y sus orientaciones. Significa maximizar los efectos de la aplicación local (por ejemplo, árbitros más fuertes y mejor acceso a la reparación), al tiempo que se dirige la cooperación internacional para que sea una prioridad relevante para los organismos gubernamentales (por ejemplo, ampliando los esfuerzos de la OCDE, el Convenio 108+ y el RGPD).

Reforzar conjuntamente la protección de datos, la privacidad y los derechos humanos exigirá tanto un compromiso constante de medios tangibles como claridad sobre los fines que perseguimos. Como se señala a lo largo de este informe, todos los indicadores ponen de relieve que, a menos que haya una coordinación inmediata, la privacidad, la dignidad humana, la libertad esencial y la libertad de expresión continuarán erosionándose. La alternativa —la continua fragmentación de los esfuerzos de reforma, los esfuerzos localizados y esporádicos de regulación, y las incursiones desiguales y prolongadas en la aplicación en línea— no hacen más que reforzar el statu quo de la autorregulación, tanto en el sector comercial como en el sector gubernamental.

Para que quede claro, las opciones que aquí se presentan no se excluyen las unas a las otras, sino que se complementan. Por ejemplo, aunque dar prioridad a instrumentos como el Convenio 108 y el 108+ constituya una vía expeditiva para la mejora, deben continuar los llamamientos a otras acciones internacionales (por ejemplo, en cuanto a las Naciones Unidas). Es posible imaginar vías duales para continuar mejorando y garantizando el reconocimiento y la protección de los derechos a la privacidad y a la protección de datos. Una vía se basa en las disposiciones constitucionales existentes, incluidos los derechos a la autonomía, la libertad, la personalidad y la dignidad, para reconocer el derecho a la privacidad y a la protección de datos en el ordenamiento jurídico interno de un estado. A falta de disposiciones explícitas sobre privacidad o protección de datos, Alemania e India, entre otros estados, ya han adoptado esta vía. El efecto resultante ha sido poderoso.

La segunda vía, potencialmente acumulativa, es la de fomentar la convergencia en torno a un instrumento mundial existente basado en los derechos. El principal candidato es el Convenio 108+. Se ha actualizado para adaptarlo a la generación más reciente de leyes de protección de datos. Esencialmente, se trata de un instrumento sólido, basado en los derechos, aunque sus disposiciones no son preceptivas, lo que deja cierto margen de maniobra en diferentes contextos jurídicos y culturales. Además, existe un proceso claro para la adhesión de los estados no pertenecientes al Consejo de Europa. Siguiendo este planteamiento y aprovechando al máximo el potencial de los instrumentos jurídicos existentes para la protección de la privacidad, queda al alcance de la mano un enfoque más eficaz y basado en los derechos.

Anexo: Vinculado a la autonomía: interés propio, dependencia económica, relaciones sociales y obligaciones

1. Interés propio existencial

Podría decirse que las limitaciones del interés propio existencial representan los límites más fuertes a nuestra autonomía individual. Solemos consentir voluntariamente el uso de nuestros datos, cuando hacerlo es condición previa para recibir tratamientos médicos específicos o cuando la recogida continua de datos forma parte del funcionamiento de un dispositivo médico innovador, por ejemplo, un implante coclear o un marcapasos. Denegar el consentimiento a que nuestros datos se traten, cuando hacerlo pondría realmente en peligro nuestra salud o incluso nuestra vida, o la salud o la vida de otras personas, puede parecer, a primera vista, contraproducente y, por tanto, no verse por el individuo como una gran limitación en absoluto. No obstante, significa que el despliegue efectivo de medidas de salud individual o pública está, de hecho, condicionado al tratamiento de datos personales identificables y no puede lograrse de otra manera.

Esto puede ser cierto en determinados casos, pero, en otros, puede bastar con recoger los datos de forma anónima. Así pues, un derecho efectivo a la protección de datos protegería la autonomía individual al hacer recaer en los innovadores la responsabilidad de desarrollar nuevas tecnologías respetando principios establecidos de protección de datos como, entre otros, la minimización de los datos, la limitación de su finalidad y la limitación de su almacenamiento.

2. Limitaciones económicas

Las limitaciones económicas que influyen en nuestras decisiones resultan principalmente de nuestro poder relativo de negociación cuando interactuamos con otros agentes comerciales. En este contexto, nuestro propio poder relativo viene determinado, entre otras cosas, por la riqueza, los conocimientos, la destreza y la habilidad que poseemos. En la práctica, incluye las cosas que no podemos hacer, no sabemos hacer o no podemos permitirnos hacer.

Las limitaciones económicas suelen observarse en contextos en que una persona se encuentra en una situación de dependencia o subordinación económica o en que está dispuesto a hacer concesiones en materia de privacidad a cambio de bienes o servicios. La relación entre un empleado y su empleador o entre un beneficiario de prestaciones y la autoridad pública que las proporciona son ejemplos del primer contexto. En él, será casi imposible que el individuo rechace una solicitud de divulgación de sus datos personales sin arriesgarse a sufrir un perjuicio económico considerable. Los intercambios entre proveedores y usuarios de servicios «gratuitos» de redes sociales pertenecen a la segunda categoría. Los usuarios se han acostumbrado a “pagar con sus datos”, tanto porque disfrutan sin tener que pagar una contraprestación económica a cambio como porque, muchos de ellos, no podrían permitirse el uso de todos esos servicios si se les ofreciesen a precio de coste. Así, el uso de los datos como forma de pago oculta una preocupación más fundamental que surge de nuestra economía digital de datos y financiada por la publicidad. Se trata del hecho de que la compensación monetaria haría aflorar la desigualdad económica, de la que podría decirse que es una característica y no un defecto de la economía política capitalista imperante.

Las limitaciones económicas pueden observarse también en otros contextos; por ejemplo, cuando una persona se encuentra en una situación de dependencia o subordinación económica. Lo vemos, por ejemplo y principalmente, en la relación entre empresario y empleado, pero puede también manifestarse en otras relaciones. Por ejemplo, en nuestro mundo basado en la tecnología y los datos, quienes dependen económicamente de las prestaciones del Estado —personas perceptoras rentas bajas, personas en situación de desempleo y personas con discapacidad— suelen tener que facilitar una cantidad excepcionalmente grande de datos personales sobre sus circunstancias personales, educación, salud, etc. antes de que se tome una decisión sobre el pago de dichas prestaciones.

Siendo estas las circunstancias, inevitablemente, dichas personas cederán sus datos. De lo contrario, si se niegan a cederlos, es probable que se queden literalmente sin un céntimo. Entre las cosas que podemos comprar con dinero están las que satisfacen las necesidades más fundamentales de la jerarquía de necesidades de Maslow; por ejemplo, comida y vivienda. Probablemente, en la mente del individuo medio, estas necesidades fisiológicas y de seguridad siempre prevalezcan sobre otras de mayor nivel, como la autorrealización, incluida la capacidad de ejercer control sobre nuestros datos personales.
Sin embargo, al argumentar que el individuo ejerce su autonomía en esas circunstancias, probablemente se ignoraría absolutamente el desequilibrio de poder, así como la pura necesidad económica que influirá en la decisión de los individuos en tales circunstancias.
Por el contrario, es probable que los desequilibrios de poder político y económico preexistentes sirvan de restricción eficaz al ejercicio de la autonomía individual en la economía de los datos.

Como antes, el derecho a la protección de datos puede contribuir a corregir estos desequilibrios y devolver al individuo un sentido de verdadera autonomía, imponiendo restricciones a determinados usos de los datos que los responsables del tratamiento específicos proponen. Aunque una restricción de este tipo también limitaría inevitablemente —a primera vista— la autonomía del individuo para hacer un mal negocio, en algunos casos puede ser necesaria una restricción de la autonomía precisamente para preservarla.

3. Limitaciones sociales/colectivas

Finalmente, nuestras decisiones individuales también se ven influidas por la coacción social y colectiva; es decir, lo que haremos o dejaremos de hacer para cumplir nuestras obligaciones sociales. Muestra muy actual de este tipo de restricción es la disposición que mostramos a permitir que nuestros datos se utilicen en interés público; por ejemplo, en respuesta a llamamientos a la «donación de datos» con fines de salud pública.

Aunque el interés propio existencial habrá desempeñado un papel al persuadir a un individuo para que participe en tales medidas de salud pública, también hubo una creciente presión «social» sobre los individuos para que participaran. Supuso una restricción adicional a la autonomía de las personas al decidir si divulgaban o no sus datos para esos fines. Las restricciones sociales y colectivas dificultan que las personas nieguen su consentimiento y, por tanto, ejerzan realmente su autonomía, aunque les preocupe la falta de confianza o la posibilidad de que sus datos, una vez compartidos, puedan utilizarse posteriormente para fines no

relacionados.

La legislación sobre protección de datos, basada en la noción de autonomía individual, podría abordar algunas de estas preocupaciones mediante restricciones a los usos no esenciales de los datos y la exigencia de salvaguardias efectivas. Como antes, la transparencia, la minimización de los datos, la limitación de la finalidad y la limitación del tiempo de conservación de los datos podrían contribuir a infundir la confianza que los individuos necesitan para participar en sistemas de tratamiento de datos altruistas o con valor social sin temor que de ello resulten perjuicios futuros.

Al mismo tiempo, la tensión entre los intereses individuales y colectivos en este escenario concreto también pone de relieve el hecho de que puede haber llegado el momento de replantearse el individualismo que tradicionalmente ha informado el concepto de derechos fundamentales en las democracias liberales occidentales. Como señaló el Tribunal Constitucional alemán en su sentencia sobre Censos, las acciones (u omisiones) de los individuos pueden afectar no solo a ellos mismos, sino también a los derechos e intereses de otros y de la comunidad a la que pertenecen. En consecuencia, también deberíamos considerar si los derechos a la privacidad/protección de datos deben considerarse derechos puramente individuales o derechos colectivos o comunitarios.

Bibliografía / fuentes citadas

Estatutos

Bloustein, «Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser» (1964) 39 *New York University Law Review* 1000

Bradford et al., «COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes» (2020)7 *Journal of Law and the Biosciences* (pendiente de publicación)

Brandeis, L. D. y S. D. Warren, «The Right to Privacy» *Harvard Law Review*, Vol. 4, n.º 5. (15 de diciembre de 1890), p. 193-220. — http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Crawford y Schultz, «Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms» (2014) 55 *Boston College Law Review* 93

de Hert y Papakonstantinou, «Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency» (2013) 9 *Journal of Law and Policy* 271

de Schutter y Ringelheim, «Ethnic Profiling: A Rising Challenge for European Human Rights Law» (2008)71 *Modern Law Review* 358

Diggelmann and Cleis, «How the Right to Privacy became a Human Right» (2014) 14 *Human Rights Law Review* 441

Ess, «Lost in Translation?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)» (2005) 7 *Ethics and Information Technology* 1.

Fried, «Privacy» (1968) 77(3) *Yale Law Journal* 475

Greenleaf, «Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside Europe» (2016) *UNSWLRS* 52

Greenleaf, «How far can Convention 108+ "globalize"? Prospects for Asian accessions» (2020) *Computer Law & Security Review* (pendiente de publicación).

Hoofnagle, van der Sloot y Borgesius, «The European Union general data protection regulation: what it is and what it means» (2019) 28 *Information & Communications Technology Law* 65

Keats Citron y Pasquale, «The Scored Society: Due Process for Automated Predictions» (2014) 89 *Washington Law Review* 1

Kitiyadisai, «Privacy rights and protection: foreign values in the modern Thai context» (2005)7 *Ethics and Information technology* 17

Kuner, «An International Legal Framework for Data Protection: Issues and Prospects» (2009)25 *Computer Law and Security Review* 307

Lynskey, «Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order» (2014) *International & Comparative Law Quarterly* 569

Madison, *Federalist Papers, n.º 51* (1788) - https://billofrightsinstitute.org/primary-sources/federalist-no-51.

McStay, «Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy», enero 2020, *Big Data & Society* 1

Newman, «The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google» (2014)40(2) *William Mitchell Law Review* 849

Ohm, «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization» (2010) 57 *UCLA Law Review* 1701

Olinger, Britz y Olivier «Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa» (2007)39 *The International Information & Library Review* 31

Petkova, «Privacy as Europe's First Amendment» (2019) 25 *European Law Journal*. 140

Post, «Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere» (2018) 67 *Duke Law Journal* 980

Prins, «When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter» (2006) 3 *SCRIPTed* 270.

Prosser, «Privacy» (1960) *California Law Review* 48

Rengel, «Privacy as an International Human Right and the Right to Obscurity in Cyberspace» (2014), *Groningen Journal of International Law,* 33,

Richards, «The Dangers of Surveillance» (2013) 126 *Harvard Law Review* 1934

Simitis, «Die informationelle Selbstbestimmung—Grundbedingung einer verfassungskonformen Informationsordnung» (1984) *Neue Juristische Wochenschrift* 394

Simitis, «Reviewing Privacy in an Information Society» (1987)135 *University of Pennsylvania Law Review* 709

Spina, «Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?» (2014) 2 *European Journal of Risk Regulation* 248

Veale y Binns, «Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data» (2017) 4 *Big Data & Society* 1

Veil, «The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law» (2018). Disponible en: https://ssrn.com/abstract=3305056

Yilma, «The United Nations data privacy system and its limits» (2019) 33 *International Review of Law, Computers & Technology* 224

Warren y LD Brandeis, «The right to privacy» (1890), 4 *Harvard Law Review* 193.

Libros

Acemoglu y Robinson, *The Narrow Corridor: states, societies and the fate of liberty* (Penguin Random House, 2019)

Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (University Press of Kansas, 2007)

Bennett y Raab, *The Governance of Privacy* (2.ª ed., MIT Press, 2006)

Cohen, J. E. *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019)

Cohen, S. A. *Invasion of Privacy: Police and Electronic Surveillance* (Carswell, 1983)

Cooley, *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract,* (2.ª ed., Chicago, Callaghan & Company, 1880).

Donohue, *The future of foreign intelligence: privacy and surveillance in the digital age* (Oxford University Press, 2016)

Emerson, *The system of freedom of expression* (Random House Trade, 1970)

Foucault, *Discipline & Punish: The Birth of the Prison* (Vintage, 1995 edition, 1975)

González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2004)

Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016)

Kant, *Groundwork for the Metaphysics of Morals* (Abbott Thomas K. tr, 2005)

Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2011)

Landau, *Surveillance or security? The risks posed by new wiretapping technologies* (MIT Press, 2010)

Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015)

Lyon, *Surveillance after September 11* (Polity Press, 2003)

Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994)

Mayer-Schönberger y Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2018)

McStay, *Emotional AI* (Sage, 2018)

Raz, *The Morality of Freedom* (Oxford University Press, 1986)

Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995)

Schoeman, *Privacy and Social Freedom* (Cambridge University Press, 1992)

Shattuck, *Rights of Privacy* (American Civil Liberties Union, 1977)

Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004)

Solove, *Understanding Privacy* (Harvard University Press, 2008)

Westin, *Privacy and Freedom* (Atheneum, 1967)

Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)

Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International, 2015)

Capítulos de libros

Andrade, «Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights» en Fischer-Hübner et al. (ed.), *Privacy and Identity Management for Life* (Springer, 2010)

Dalla Corte, «A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection» en Hallinan et al. (ed.), *Data Protection and Privacy: Data Protection and Democracy* (Hart, 2020)

de Hert y Gutwirth, «Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action», en Gutwirth et al. (ed.), *Reinventing Data Protection?* (Springer, 2009)

de Hert y Gutwirth, «Privacy, data protection and law enforcement. Opacity of the individual and transparency of power» en Claes et al. (ed.), *Privacy and the criminal law* (Intersentia, 2006)

Larsen, Boulanger y Vandendriessche, «Luxembourg» en *The New EU Data Protection Regime: Setting Global Standards for the Rights to Personal Data Protection* (The Hague, 2020)

Oguru, «Electronic government and surveillance-oriented societies» en D. Lyon (ed.), *Theorizing Surveillance: the Panopicton and Beyond* (Routledge, 2006)

Rauhofer, «Round and round the garden?: Big data, small government and the balance of power in the information age» en Schweighofer et al. (ed.), *Transparenz* (Oesterreichische Computer Gesellschaft, 2014)

Rouvroy y Poullet, «The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy» en Gutwirth et al. (ed.), *Reinventing Data Protection?* (Springer, 2009)

W Webster, «Public administration as surveillance» en Ball, Haggerty y Lyon (ed.), *Routledge Handbook of Surveillance Studies* (Routledge, 2012)

Jurisprudencia

Amann v. *Switzerland, recurso n.º* 27798/95, (TEDH, 16 de febrero de 2000)

Big Brother Watch and ors v United Kingdom, recursos n.º 58170/13, 62322/14 y 24960/15, (TEDH, 4 de febrero de 2019).

Botta contra Italia, recurso n.º 21439/93, (TEDH, 24 de febrero de 1998)

Burghartz v. Switzerland, recurso n.º 16213/90, (TEDH, 22 de febrero de 1994)

Campbell v Mirror News Group (MGN) [2004] UKHL 22

Carpenter v United States 138 TS 2206 (2018)

Copland v. *United Kingdom,* recurso n.º 62617/00, (TEDH, 3 de julio de 2007)

Digital Rights Ireland Ltd v Minister Commc'n Marine and Nat. Res. And Others & Karntner Ladesregierung and Others (Acumulación de causas C-293/12 & C-594/12) [2014] ECR 238

Douglas v Hello! Ltd [2005] EWCA Civ 595

Fontevecchia and D'Amico c. Argentina, sentencia de 29 de noviembre de 2011, Tribunal Interamericano de Derechos Humanos, (Fondo, Reparaciones y Costas, Serie C núm. 238).

French Data Network and Others (Acumulación de causas C-511/18, C-512/18, C-520/18) ECLI:EU:C:020:791

Halford v. *United Kingdom,* recurso n.º 20605/92, (TEDH, 25 de junio de 1997)

Justice K.S.Puttaswamy (Retired). vs Union of India And Ors., 2017 *Katz v. United States*, 389 EE. UU. 347 (1967).

Kaye v *Robertson* [1991] FSR 62

Kennedy v. *United Kingdom*, recurso n.º 26839/05 (TEDH, 18 de agosto de 2010)

Klass v*. Germany* (1978), recurso n.º 5029/71, (EHRR, 1978)

La Quadrature du Net and Others (C-511/18) ECLI: EU:C:2020:791

Leander v*. Suecia,* recurso n.º 9248/81, (TEDH, 26 de marzo de 1987).

Liberty and Others v. United Kingdom, recurso n.º 58243/00 (TEDH, 1 de octubre de 2008)

Malone v. *United Kingdom*, recurso n.º 8691/79 (TEDH, 2 de agosto de 1984)

Mosley v News Group Newspapers [2008] EWHC 1777 (QB)

Murray v Big Pictures (UK) Ltd, [2008] EWCA Civ 446

Niemietz v. Germany recurso n.º 13710/88, (TEDH, 16 de diciembre de 1992)

Olmstead v. U.S. (277) EE.UU. 438 (1928)

Open Door and Dublin Well Woman v Ireland, recurso n.º 14235/88 (TEDH, 29 de octubre de 1992)

Ordre des barreaux francophones et germanophone and Others (Acumulación de causas C- 511/18, C-512/18, 52/18) ECLI:EU:C:2020:7

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (C-623/17) ECLI:EU:C:2020:790

Rotaru v. *Romania* , recurso n.º 28341/95 (TEDH, 4 de mayo de 2000)

Schüssel v. Austria, recurso n.º 42409/98, (TEDH, 21 de febrero de 2002)

Smith v. Maryland, 442 EE. UU. 735 (1979

Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others (Acumulación de causas C-203/15 y C-698/15) ECLI:EU:C:2016:970

United States v. Jones, 565 EE. UU. 400 (2012)

United States v. Miller, 425 EE. UU. 435 (1976)

Volker und Markus Schecke and Eifert (Acumulación de causas C-92/09 y 93/09) EU:C:2010:662

Von Hannover v Germany, recurso n.º 59320/00 (TEDH, 24 de septiembre de 2024)

Weber and Saravia v. *Germany,* recurso n.º 54934/00. (TEDH, 29 de junio de 2006)

Zhu Yingguang v Lianyungang City Branch of China United Network Communications Co., Ltd, Ltd, Tribunal Intermedio de la ciudad de Lianyungang, provincia de Jiangsu, n.º 0006 de 2014.

Legislación e instrumentos internacionales

Convención Americana sobre Derechos Humanos adoptada en 1969. Convención Americana sobre Derechos Humanos, adoptada en la Conferencia Especializada Interamericana sobre Derechos Humanos, San José de Costa Rica, 22 de noviembre de 1969

Austria, BGBl. N.º 59/1964 1958

Bundesgesetz uber den Schutz personenbezogener Daten BGBl 565/1978 (AT)

BVerfGE 35, 202 — Lebach y BVerfGE 65, 1 — Ley Census

Ley Census, BVerfGE 65 2020 (DE)

Convenio 108+ Convenio para la protección de las personas con respecto al tratamiento de datos personales, STE n.º 108, 1 de octubre de 1985

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 14 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [1995] DO L 281/31.

Reglamento 2016/679/CE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se revoca la Directiva 95/46/CE, DO L 119/1.

Datenschutzgesetz de 7 de octubre de 1970 (HDSG)

Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet) 2014

Unión Europea, Carta de los Derechos Fundamentales de la Unión Europea [2012] DO C 326/02.

Principios generales del Derecho civil《民法通则 1987

Ley federal alemana de protección de datos de 1977.

Conferencia Internacional Americana, Declaración Americana de los Derechos y Deberes del Hombre, 9.ª sesión, Documento de las Naciones Unidas / CN.4/122(1948)

Loi du 31 mars 1979 reglementant l'utilisation des données nominatives dans les traitements informatiques) 1979 (LU)

Loi n8 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés 1978 (FR)

Lov nr 294 af 8 juni 1978 om offentlige myndigheders register (DK) Lov om personregistre

mm av 9 juni 1978 nr 48 (NO)

Nihon-koku kenpō, 1947

La Constitución belga de 1831

Orden Constitucional de Bermudas de 1968

Ley de Canadá de 1982 (Reino Unido)

La Carta Canadiense de Derechos y Libertades de 1982

La Constitución de Colombia de 1991

La Constitución de Gabón de 1991

La Constitución de la República de Corea 1987

La Constitución de Trinidad y Tobago 1976

El Datalagen de Suecia en 1973 (Datalagen, 11 de mayo de 1973)

La Ley Fundamental de Hong Kong de 1982

La Ley de Derechos Humanos de 1998

La Constitución mexicana de 1917

La Constitución filipina de 1987

La Constitución portuguesa de 1976

La Constitución suiza de 1999

Derecho de responsabilidad civil (《侵权责任法) 2010

Demanda (Civil) núm. 494 de 2012, 2017

Informes y resoluciones
The Citizen Lab and Canadian Internet Policy & Public Interest Clinic, "Shining a Light on the Encryption Debate" (mayo de 2018) - https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

Comisión Mundial sobre la Gobernanza de Internet, «One Internet» (junio de 2016) - https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf.

Asamblea Mundial de la Privacidad, «International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other Fundamental Rights» (octubre de 2019) - http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on- privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf.

Conferencia Internacional de Comisarios de Protección de Datos y Privacidad, «The protection of personal data and privacy in a globalised world: a universal right respecting diversities» (2005) Disponible en: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf

Conferencia Internacional de Comisarios de Privacidad y Protección de Datos, «Resolution on anchoring data protection and the protection of privacy in international law» (2013). Disponible en: www.globalprivacyassembly.org/wp-content/uploads/2015/02/International-law-resolution.pdf

Comisión de Derecho Internacional, «Informe de la Comisión a la Asamblea General sobre la labor realizada en su 58.º período de sesiones» (2006), A 61/10, anexo D. Disponible en: https://legal.un.org/ilc/reports/2006/spanish/annexes.pdf

The Law Society of England and Wales, "Algorithms in the Criminal Justice System", junio de 2019. Disponible en: https://www.lawsociety.org.uk/topics/research/algorithm- use-in-the-criminal-justice-system-report

Relator especial de las Naciones Unidas sobre la libertad de expresión. «Informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión», Consejo de Derechos Humanos: Vigésimo noveno periodo de sesiones, punto 3 del orden del día, 22 de mayo de 2015. Disponible en: https://www.undocs.org/A/HRC/29/32

Relator especial de la ONU sobre el derecho a la privacidad, «Informe del relator especial sobre el derecho a la privacidad»: Septuagésimo tercer periodo de sesiones de la Asamblea General de la ONU, 17 de octubre de 2018. Disponible en: https://undocs.org/A/73/438

Relator especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Informe al Consejo de Derechos Humanos sobre Vigilancia y Derechos Humanos, 28 de mayo de 2019. Disponible en: https://undocs.org/A/HRC/41/35

Otros
Agencia Española de Protección de Datos, «Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data» (borrador inédito, enero de 2009; borradores actualizados de 24 de febrero y 24 de abril de 2009).

Bedingfield, «Everything that went wrong with the botched A-Levels algorithm», Wired, 19 de agosto de 2020. Disponible en: https://www.wired.co.uk/article/alevel-exam-algorithm.

Clifford, *The Legal Limits to the Monetisation of Online Emotions* (2019, tesis doctoral, KU Leuven). Disponible en: https://www.law.kuleuven.be/citip/en/research/phd-research/finalized/phd-damian-clifford.

CNIL, «How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence» (2017). Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

Coughlan, «A-levels and GCSEs: Boris Johnson blames "mutant algorithm" for exam fiasco», BBC, 26 de agosto de 2020. Disponible en: https://www.bbc.co.uk/news/education- 53923279.

Commission Européenne pour la Démocratie par le Droit (Commission de Venise), Luxembourg - Proposition de revision portant instauration d'une nouvelle constitution, Strasbourg, le 27 février 2019 (Rapport de la Luxembourg, CDL-.
REF(2019)006

deNisco Rayome, «The US, China and the AI arms race: Cutting through the hype», CNet, 8 de julio de 2020. Disponible en: https://www.cnet.com/news/the-us-china-and-the-ai- arms-race-cutting-through-the-hype/.

de Terwangne, «Convention 108+ evaluation and follow-up mechanisms», 1 de julio de 2020. Disponible en: https://www.coe.int/en/web/data-protection/follow-up-and-evaluation-mechanism

Comisión Europea, «Comunicación de la Comisión al Parlamento Europeo y al Consejo: Exchanging and Protecting Personal Data in a Globalised World» COM (2017)7 final

González-Fuster e Hijmans, «The EU rights to privacy and personal data protection: 20 years in 10 questions», documento de debate, Brussels Privacy Hub

Google, «Updating our privacy policies and terms of service», 24 de enero de 2012; disponible en http://googleblog.blogspot.co.uk/2012/01/updating-our-privacy-policies-and-terms.html

Kuner, «Extraterritoriality and Fundamental Right to Data Protection» (EJIL: Talk, 16 de diciembre de 2013). Disponible en: https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/comment-page-1/ .

Levin, «Facebook told advertisers it can identify teens feeling "insecure» and "worthless"», The Guardian, 1 de mayo de 2017. Disponible en: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

Malgieri, «The concept of fairness in the GDPR: a linguistic and contextual interpretation», FAT* '20: Actas de la 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020).

Sitaropoulos «States are Bound to Consider the UN Human Rights Committee's Views in Good Faith» (Blog OxHRH, 11 de marzo de 2015). Disponible en: www.humanrights.dev3.oneltd.eu/states-are-bound-to-consider-the-un-human-rights-committees-views-in-good-faith/

Comité de Derechos Humanos de la ONU, Observación General 16, emitida el 23.3.1988 (UN Doc A/43/40, 181-183)

UN, Guidelines for the Regulation of Computerized Personal Data Files, informe final presentado por Louis Joinet, relator especial, 21 de julio de 1988 (E/CN.4/Sub.2/1988/22).

Asamblea General de la ONU, Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, 19 de diciembre de 1966, Naciones Unidas, Serie de Tratados, vol. 999, p. 171,
Artículo 2

Notas finales y referencias

1 *International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other Fundamental Rights* (octubre 2019) - http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf

2 Ver, respectivamente: Organización de Cooperación y Desarrollo Económicos (OCDE), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, 23 de septiembre de 1980 (en lo sucesivo, Directrices de la OCDE sobre protección de la privacidad), modernizadas por la Recomendación del Consejo relativa a las Directrices que Regulan la Protección de la Intimidad y los Flujos Transfronterizos de Datos Personales ("Directrices de Privacidad") (2013) [C(80)58/FINAL, modificada el 11 de julio de 2013 por C(2013)79] (en lo sucesivo, Directrices revisadas de la OCDE que regulan la protección de la privacidad); Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter individual, 28 de enero de 1981, STE 108 (en lo sucesivo, Convenio 108), modernizado por el Protocolo por el que se modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE núm. 108), CM(2018)2-final, 18 de mayo de 2018 (en lo sucesivo, Convenio 108+); Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281/31 23.11.1995 (en lo sucesivo, Directiva de 1995), modernizada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, DO L 119 de 4 de mayo de 2016 (en lo sucesivo, RGPD).

3 S Landau, *Surveillance or security? The risks posed by new wiretapping technologies* (MIT Press, 2010), 10. «La privacidad es un aspecto fundamental del funcionamiento de una sociedad humana, una necesidad evidente para la libertad y la dignidad humanas... incluye el derecho a controlar la información sobre uno mismo, el derecho a asociarse como se desee, tan privadamente como se desee, a compartir confidencias en confianza, a disfrutar de la soledad y la intimidad. Incluye el derecho al anonimato».

4 T Oguru, «Electronic government and surveillance-oriented societies» en D. Lyon (ed.), *Theorizing Surveillance: the Panopticon and Beyond* (Routledge, 2006), 280. «Los sistemas jurídicos modernos se encuentran ante un punto de inflexión importante en la regulación del poder político; la ley se dirige a la regulación del comportamiento humano, pero no puede controlar los ordenadores... la regulación democrática basada en el estado de derecho ha perdido poder regulador».

5 Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «The Right to Privacy in the Digital Age» (2018) - https://www.ohchr.org/ES/Issues/DigitalAge/Pages/ReportDigitalAge.aspx; véase también Rengel, Alexandra, «Privacy as an International Human Right and the Right to Obscurity in Cyberspace» (diciembre de 2014). *Groningen Journal of International Law*, Vol. 2, N.º 2, 2014, Disponible en: https://ssrn.com/abstract=2599271

6 OCDE, «Data-driven innovation for growth and well-being» - http://oe.cd/bigdata; véase también Martin Abrams, «The Origins of Personal Data and its Implications of Governance» de la Information Accountability Foundation (2016) - disponible en: https://informationaccountability.org/publications/

7 D Acemoglu y J Robinson, *The Narrow Corridor:. States, societies and the Fate of Liberty* (Penguin Random House, 2019), 492. «Los derechos están íntimamente ligados a nuestra noción de libertad como protección personal frente al miedo, la violencia y la dominación. Aunque el miedo y la violencia han sido los motores principales ... la dominación —la incapacidad de las personas para decidir y seguir su vida de acuerdo con sus propios valores- también es asfixiante. Los derechos son fundamentalmente vías para que la sociedad codifique en sus leyes y normas la capacidad de todos los individuos para decidir.

8 W Webster, «Public administration as surveillance» en Ball, Haggerty y Lyon (ed.), *Routledge Handbook of Surveillance Studies* (Routledge, 2012), 313. «En un esfuerzo por lograr que gobiernos y servicios públicos sean más eficaces y rentables, se han invertido enormes sumas de dinero en infraestructuras electrónicas, bases de datos y administración electrónica... Las sociedades construidas en torno a prácticas de vigilancia mediadas tecnológicamente dependen significativamente de la plataforma y el aparato de vigilancia creados por las administraciones públicas... al hacer de la vigilancia una parte normal del día a día».

9 Alan Westin, *Privacy and Freedom* (1967), 359

10 Canadá. *Department of Justice. Privacy and Computers*: informe del grupo de trabajo creado por los Departamentos de Comunicaciones y Justicia (Ottawa, 1971), 10.

11 Harold Innis, «Industrialism and cultural values» de *The Bias of Communication* (1951), 140.

[12] V Mayer-Schönberger y K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2018), 83-84.
[13] Andy McStay, *Emotional AI* (Sage, 2018), 115.
[14] Vea el sitio web de Eye Q disponible en: https://eyeq.tech/retail/.
[15] S Levin, «Facebook told advertisers it can identify teens feeling "insecure" and "worthless"», The Guardian, 1 de mayo de 2017. Disponible en: https://www.theguardian.com/technology/2017/may/01/facebook- advertising-data-insecure-teens.
[16] D Clifford, *The Legal Limits to the Monetisation of Online Emotions* (2019, tesis doctoral, KU Leuven), 266-288. Disponible en: https://www.law.kuleuven.be/citip/en/research/phd- research/finalized/phd-damian-clifford.
[17] A McStay, «Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy», enero 2020, *Big Data & Society*, 1-12.
[18] Esto también lo destaca Cohen, según el cual «en los procedimientos gubernamentales y en la prensa popular, las industrias de tratamiento de información han trabajado para posicionar la innovación y la regulación protectora como intrincadamente opuestas. Esa estrategia ha resultado en un proceso discursivo que infunde a la "innovación" un significado particular y contingente vinculado a la libertad económica y a la ausencia de supervisión gubernamental»; véase J. Cohen, Between Truth y Power: The Legal Construction of Information Capitalism, 2019, OUP, p. 90
[19] Por ejemplo, compárese el trabajo de la Ada Lovelace Foundation en «Data for the Public Good» - https://www.adalovelaceinstitute.org/our-work/library/, con el trabajo similar llevado a cabo por la Royal Society en «Using Data for the Public Good» https://royalsociety.org/blog/2020/07/using-data-for-the-public- good/,con el trabajo desarrollado por la OCDE en «Enhancing access to and sharing of data» - https://www.oecd.org/digital/ieconomy/enhanced-data-access.htm.
[20] Grupo de trabajo de la Royal Society de Canadá sobre Infovigilancia (marzo de 2021) - https://rsc-src.ca/sites/default/files/Infoveillance_EN_0.pdf
[21] J Rauhofer (2014) «Round and round the garden?: Big data, small government and the balance of power in the information age» en Erich Schweighofer, Franz Kummer, Walter Hoetzendorfer (ed.), Transparenz (OCG, 203), 606-617, p. 615.
[22] Para un análisis del uso de algoritmos en el sistema de justicia penal véase: The Law Society de Inglaterra y Gales, «Algorithms in the Criminal Justice System», junio de 2019, p. 15-17,
[23] A deNisco Rayome, «The US, China and the AI arms race: Cutting through the hype», CNet, 8 de julio de 2020. Disponible en: https://www.cnet.com/news/the-us-china-and-the-ai-arms-race-cutting-through- the-hype/.
[24] S Coughlan, «A-levels and GCSEs: Boris Johnson blames "mutant algorithm" for exam fiasco», BBC, 26 de agosto de 2020. Disponible en: https://www.bbc.co.uk/news/education-53923279.
[25] W Bedingfield, «Everything that went wrong with the botched A-Levels algorithm», Wired, 19 de agosto de 2020. Disponible en: https://www.wired.co.uk/article/alevel-exam-algorithm.
[26] Ibíd.
[27] Evgeny Morozov, «The tech solutions for coronavirus take the surveillance state to the next level», *The Guardian* (15 de abril de 2020) - https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt
[28] Véase, por ejemplo, Budd, J., Miller, B.S., Manning, E.M. et al. Digital technologies in the public- health response to COVID-19. *Nat Med* 26, 1183–1192 (2020). https://doi.org/10.1038/s41591-020- 1011-4, y, De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171
[29] Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)
[30] Cicero, *De Officiis (On Obligations),* traducido por P. G. Walsh (Oxford, 2008), Libro I, sec. 85, p. 30
[31] F. D. Schoeman, *Privacy and social freedom* (1992), 116
[32] Daniel Solove, *Understanding Privacy* (2008), p. 61-62
[33] Laura K. Donohue, *The future of foreign intelligence: privacy and surveillance in a digital age* (Oxford, NY: 2016), p. 75-76.
[34] John H. Shattuck, *Rights of Privacy* (1977), p. 3-5.
[35] Stanley A. Cohen, *Invasion of Privacy* (1983), p. 20-21, 34, 52.
[36] James Madison, *Federalist Papers*, N.º 51 (1788) - https://billofrightsinstitute.org/primary-sources/federalist-no-51; también Louis D. Brandeis i Samuel D. Warren, «The Right to Privacy»

Harvard Law Review, Vol. 4, N.º 5. (15 de diciembre de 1890), p. 193-220. - http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

37 Georges Duby, «Introduction: Private Power, Public Power', en *A History of Private Life. II. Revelation of the Medieval World*, editado por Georges Duby (Cambridge MA: Belknap Press, 1988) 38 Diane Shaw, «The Construction of the Private in Medieval London», *Journal of Medieval and Early Modern Studies*, 26 (1996), p. 450.

39 David Vincent, *Privacy: A Short History* (Wiley, 2016), p. 2.

40 SD Warren y LD Brandeis, «The right to privacy» (1890), 4 *Harvard Law Review* 193-220 De hecho, el juez Cooley había acuñado la expresión «derecho a ser dejado en paz» varios años antes. Véase Cooley, *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract,* (2.ª ed., Chicago, Callaghan & Company, 1880).

41 ibíd, p. 198.

42 Mientras que el artículo 8 del CEDH ha tenido una amplia repercusión en la protección de la privacidad en los Estados miembros del Consejo de Europa, el impacto del ICCPR de la ONU ha sido menor. Se ha encomendado a un Comité de Derechos Humanos (CDH) formado por expertos independientes la misión de interpretar y garantizar el cumplimiento del ICCPR. El CDH dirige la interpretación de las disposiciones del ICCPR emitiendo «observaciones generales» dicha interpretación. Ya ha ejercido esta facultad para emitir una observación general sobre el artículo 17 del ICCPR. Véase la Observación General 16, emitida el 23.3.1988 (UN Doc A/43/40, 181-183)

43 Puesto que, si se presentan, no necesariamente evalúan con precisión la observancia de los derechos del ICCPR por los Estados, estos informes de los estados a menudo se complementan con «informes alternativos» presentados por actores de la sociedad civil. El Comité debate estos informes con los estados parte y adopta observaciones y recomendaciones. Si bien es una buena práctica que los Estados se adhieran a estas recomendaciones, no existe ningún mecanismo para hacerlas cumplir. Además de este mecanismo de supervisión, cuando un estado ha suscrito el primer Protocolo Facultativo, el Comité puede recibir quejas o peticiones de particulares.

44 La cifra se basa en una consulta en la base de datos de jurisprudencia de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Base de datos disponible en: www.juris.ohchr.org (búsqueda exacta a 10 de septiembre de 2020).

45 N Sitaropoulos «States are Bound to Consider the UN Human Rights Committee's Views in Good Faith» (Blog OxHRH, 11 de marzo de 2015). Disponible en www.humanrights.dev3.oneltd.eu/states-are-bound-to-consider-the-un-human-rights- committees-views-in-good-faith/

46 ACNUDH Naciones Unidas, «Relator Especial sobre el derecho a la privacidad: Informes Temáticos Anuales» - https://www.ohchr.org/ES/Issues/Privacy/SR/Pages/AnnualReports.aspx

47 Véase además, www.legal.un.org/ilc/.

48 En el caso de América Latina, deben considerarse los casos de México y Brasil. Ya en 1917, en México se reconocía constitucionalmente el derecho a la privacidad, mientras que su ley de protección de datos fue posterior; tras las reformas constitucionales de los años 90 y 2000, que reconocían la protección de datos de distintas formas. Por ejemplo, América Latina es única en la codificación del concepto de «habeas data» (el reconocimiento expreso del derecho de acceso y el derecho a conocer la información propia del individuo). En cambio, en la Constitución brasileña, con el término «igualdad y no discriminación», se afirma que «muchos marcos modernos de protección de datos contienen un principio general de tratamiento personal "leal", que se entiende como no discriminatorio entre otras cosas». La cuestión es que, en la mayoría de los países de la región, la no discriminación es un valor en sí mismo, por lo que los términos «justo» (o equidad) no siempre se traducen plenamente. La no discriminación es un valor en sí mismo en Brasil y también, por ejemplo, en Argentina, donde está goza de reconocimiento expreso en la Constitución como condición previa para el habeas data (art. 43).

49 Véanse los artículos 6.A.II y III y 16 de la Constitución mexicana de 1917 (en la versión vigente); artículo 13 de la Constitución suiza de 1999 (en la versión vigente); artículo 22 de la Constitución belga de 1831 (en la versión vigente); artículo 17 de la Constitución de la República de Corea de 1987 (en la versión vigente); artículos 2.11 y 3.3 de la Constitución filipina de 1987 (en la versión vigente); artículo 30 de la Ley Fundamental de Hong Kong de 1982 (en la versión vigente); artículo 6 de la Constitución portuguesa de 1976 (en la versión vigente); artículo 15 de la Constitución colombiana de 1991 (en la versión vigente); artículo 4(c) de la Constitución de Trinidad y Tobago de 1976 (en la versión vigente) y artículo 1(5) y (12) de la Constitución de Gabón de 1991 (en la versión vigente).

50 Artículo 7 de la Orden Constitucional de Bermuda de 1968 (en la versión vigente).

51 Incluye los estados de Brandeburgo, Mecklemburgo-Pomerania, Sajonia, Turingia, Sajonia-Anhalt, Schleswig Holstein, Hesse, Renania del Norte-Westfalia, Renania-Palatinado y Sarre.

52 BVerfGE 35, 202 - Lebach y BVerfGE 65, 1 - Ley Census.

53 *Carta Canadiense de Derechos y Libertades*, artículos 7 y 8, parte 1 de la *Ley de la Constitución, 1982*, que es el anexo B de la *Ley de Canadá de 1982* (UK), 1982, c 11.

[54] *Nihon-koku kenpō*, 3 de mayo de 1947
[55] *Justice K.S.Puttaswamy (Retired). vs Union of India And Ors*., 2017, Demanda (Civil) N.º 494 de 2012, (2017) 10 SCC 1.
[56] Carta de la UE (n **¡Error!**) **Marcador no definido.** anterior) Artículo 51(1).
[57] Véase, en Austria, BGBl. n.º 59/1964, tras firmar y ratificar el propio Convenio en 1958, véase BGBl. n.º 210/1958 y, en el Reino Unido, Ley de derechos humanos (HRA) de 1998. Si bien el Reino Unido es uno de los cofundadores y signatarios originales del CEDH, hasta la adopción de la HRA, los demandantes tenían que agotar todos los recursos internos antes de poder plantear cuestiones de derechos fundamentales ante el Tribunal Europeo de Derechos Humanos de Estrasburgo. Sin embargo, cabe señalar que, incluso tras la entrada en vigor de la HRA, el principio constitucional de soberanía parlamentaria significa que los tribunales no pueden invalidar las leyes del Parlamento. Simplemente pueden emitir una «declaración de incompatibilidad» de dichas leyes con el CEDH. Es, pues, competencia del legislador modificar o derogar la ley pertinente; véase el art. 4 de la HRA.
[58] Datenschutzgesetz de 7 de octubre de 1970 (HDSG), GVBl. I, 625.
[59] Véase, por ejemplo, la Datalagen de Suecia de 1973 (Datalagen, 11 de mayo de 1973), la primera Ley federal alemana de protección de datos de 1977 (Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung, Bundesdatenschutzgesetz (BDSG 1977), BGBl. I, 201), y otras leyes nacionales en Francia (Loi no. 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés), Dinamarca (Lov nr 294 af 8 juni 1978 om offentlige myndigheders register), Noruega (Lov om personregistre mm av 9 juni 1978 nr 48) y Austria (Bundesgesetz uber den Schutz personenbezogener Daten BGBl. 565/1978) en 1978, y Luxemburgo (Loi du 31 mars 1979 reglementant l'utilisation des donnees nominatives dans les traitements informatiques) en 1979.
[60] Por tanto, como hecho histórico, podría afirmarse que el derecho de protección de datos fue inicialmente una criatura del derecho primario y no del derecho constitucional. En función del tipo de usuarios de datas que pretendan regular, el enfoque de las leyes pertinentes puede ser de derecho privado o de derecho público. Sin embargo, parece evidente que, en sí mismo, el derecho a la protección de los datos personales de un individuo no se percibió inicialmente como derecho fundamental autónomo.
[61] En la jerga de la UE «derecho derivado» es derecho no constitucional de primer rango, ya que el término «derecho primario» se reserva a los tratados de la UE.
[62] El considerando 11 de la Directiva 95/46 «Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales».
[63] En ese momento, la naturaleza diversa de esos marcos nacionales significaba que los Estados miembros de la UE corrían el riesgo de crear barreras comerciales entre sí debido a los diferentes niveles de protección que proporcionaban y a la creciente falta de voluntad de los distintos Estados miembros para permitir transferencias transfronterizas de información personal a países que proporcionaban niveles inferiores.
[64] Punto 1 del artículo 1 de la Directiva de 1995 (n.º 2).
[65] Una versión anterior de la Carta se redactó por primera vez y se proclamó solemnemente el 7 de diciembre de 2000 para que acabara formando parte de los instrumentos constitucionales vinculantes de la UE. Una versión modificada del texto original formaba parte de la propuesta de Constitución Europea, con el objetivo de sustituir los tratados vigentes de la UE por un texto único. Sin embargo, aunque la firmaron todos los Estados entonces miembros, al no ser ratificada por todos ellos, la Constitución nunca entró en vigor. Finalmente, se abandonó en 2004. El derecho a la protección de datos también está recogido en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), que incluye la obligación del legislador de la UE de adoptar normas que regulen el tratamiento de datos personales por las instituciones de la UE y los Estados miembros cuando desarrollen actividades que entren en el ámbito de aplicación de la legislación de la UE.
[66] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO Intercambio y protección de datos personales en un mundo globalizado COM/2017/07 final - Punto 3.3.1 - https://eur-lex.europa.eu/legal- content/ES/TXT/?uri=COM%3A2017%3A7%3AFIN
[67] Guidelines for the Regulation of Computerized Personal Data Files, informe final presentado por Louis Joinet, relator especial, 21 de julio de 1988 (E/CN.4/Sub.2/1988/22).
[68] Kuner, «An International Legal Framework for Data Protection: Issues and Prospects» (2009)25 *Computer Law and Security Review* 307, p. 309.
[69] Unión Europea, Carta de los Derechos Fundamentales de la Unión Europea [2012] DO C 326/02, artículo 8.
[70] Conferencia Internacional de Comisarios de Protección de Datos y Privacidad, «The protection of personal data and privacy in a globalised world: a universal right respecting diversities» (2005),

www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf. Con este fin, el Comisario también hizo un llamamiento: a todos los gobiernos del mundo para que promoviesen la adopción de instrumentos jurídicos de protección de datos y de la privacidad acordes con los principios básicos de la protección de datos y también para que la hiciesen extensiva a sus relaciones mutuas; al Consejo de Europa para que, de conformidad con el artículo 23 del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, invitasen a los estados no miembros del Consejo de Europa que ya dispusiesen de legislación de protección de datos a que se adhirieran a este Convenio y a su Protocolo adicional.

71 ibíd., par. 12.

72 ibíd, p. 3.

73 ICDPPC, Resolución de Madrid (noviembre de 2009) - http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

74 Ver, respectivamente: Agencia Española de Protección de Datos, «Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data» (borrador inédito, enero de 2009; borradores actualizados de 24 de febrero y 24 de abril de 2009); Conferencia Internacional de Comisarios de Privacidad y Protección de Datos, «Resolution on anchoring data protection and the protection of privacy in international law» (2013), disponible en: www.globalprivacyassembly.org/wp-content/uploads/2015/02/International- law-resolution.pdf.

75 Si la cooperación se percibe ineficaz, esto puede conducir a una resistencia a afianzar la protección jurídica internacional y darle más repercusión en las normas nacionales de protección de datos. Por ejemplo, en la escena internacional, los instrumentos existentes de la ONU reciben escaso reconocimiento.

76 KM Yilma, «The United Nations data privacy system and its limits» (2019) 33 *International Review of Law, Computers & Technology* 224, p. 230.

77 Véase, P de Hert y V Papakonstantinou, «Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency» (2013) 9 Journal of Law and Policy 271, p. 282.

78 Informe del Parlamento Europeo sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (17 de marzo de 2021) - https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.pdf; Acceda ahora, *Two Years Under the EU GDPR: An Implementation Progress Report* (mayo de 2020) - https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf; Nathan Eddy, «How EU Authorities See GDPR Effectiveness Two Years In», *e-Week* (17 de junio de 2020) - https://www.eweek.com/security/how-eu-authorities-see-gdpr-effectiveness-two-years-in/

79 Tribunal IDH, Caso *Fontevecchia y D'Amico c. Argentina*, sentencia de 29 de noviembre de 2011 (Fondo, Reparaciones y Costas, Serie C núm. 238), apartado 49

80 Véase, por ejemplo, la acumulación de causas C-92/09 y 93/09, *Volker und Markus Schecke y Eifert* UE:. C: 2010: 662, apartado 89.

81 Un área de continua controversia es ver si los beneficios de la innovación pueden conciliarse con la protección de los derechos fundamentales y cómo hacerlo. La división al respecto ya era evidente en la década de 1970, cuando la Asamblea General de la ONU adoptó una «Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad». Los países del Norte Global y Occidente boicotearon esta declaración y se abstuvieron en la votación de las resoluciones posteriores, ya que estas naciones más industrializadas querían que se insistiese en el efecto potencialmente negativo de los avances tecnológicos en los derechos humanos. Véase Yilma (n **¡Error! Marcador no definido.**), p. 227 y 228.

82 Kuner (n **¡Error! Marcador no definido.**), p. 310.

83 González Fuster G. (2014) «Privacy and the Protection of Personal Data Avant la Lettre». en: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Serie Law, Governance and Technology, vol. 16. Springer, Cham. https://doi.org/10.1007/978-3-319-05023-2_2

84 Sin embargo, como señalan González Fuster e Hijmans, su coexistencia ha desencadenado muchos interrogantes, muy pocos de los cuales «han tenido desde entonces una respuesta clara, coherente o consensuada». G González-Fuster e Hijmans, «The EU rights to privacy and personal data protection: 20 years in 10 questions», documento de debate, Brussels Privacy Hub Disponible en: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_González_Fuster_Hijmans.pdf.

85 Por regla general, tiene por finalidad que las personas («interesados») puedan controlar el acceso a la información que les concierne, vinculando el tratamiento de datos personales a su consentimiento o a la existencia de leyes que autoricen dicho tratamiento. El derecho a la protección de datos suele reconocer a los interesados diversos derechos legales, entre los que destaca el de acceder a sus datos cuando están en poder de terceros. También impone a los usuarios de datos («responsables del tratamiento») una serie de obligaciones legales correspondientes.

[86] Por ejemplo, para adherirse al Convenio 108+, los estados deben disponer de una autoridad de supervisión independiente (artículo 15, apartado 5, del Convenio 108+, n 1 supra). El artículo 8, apartado 2, de la Carta de los Derechos Fundamentales de la UE y el artículo 16 del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea (versión consolidada, Diario Oficial C 326 , 26/10/2012 P. 0001
- 0390) disponen que el cumplimiento de las normas de protección de datos debe someterse al control de una autoridad independiente.

[87] Por ejemplo, véanse las normas y procedimientos detallados por el Servicio de Investigación del Congreso de EE.UU. en su informe *Data Protection Law: An Overview* (marzo de 2019). Disponible en https://fas.org/sgp/crs/misc/R45631.pdf

[88] W Veil, «The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law» (2018), p. 22. Disponible en SSRN: https://ssrn.com/abstract=3305056

[89] O Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015), p. 91-105.

[90] P de Hert y Gutwirth, «Privacy, data protection and law enforcement. Opacity of the individual and transparency of power» en Claes et al (ed.), *Privacy and the criminal law* (Intersentia, 2006) 61, p. 66-67

[91] D Solove, *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, 2004), p. 8.

[92] G Gonzalez-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2004), p. 257.

[93] O Lynskey, «Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal
Order» (2014) 63 *International and Comparative Law Quarterly* 569, p. 584-585.

[94] Mark Chinen, «Complexity Theory and the Horizontal and Vertical Dimensions of State Responsibility», *European Journal of International Law*, volumen 25, número 3, agosto de 2014, páginas 703-732, https://doi.org/10.1093/ejil/chu048.

[95] Corrin, Jennifer. «From Horizontal and Vertical to Lateral: Extending the Effect of Human Rights in Post-Colonial Legal Systems of the South Pacific». *The International and Comparative Law Quarterly* 58, n.º 1 (2009): 31-71. Último acceso: 26 de julio de 2021 http://www.jstor.org/stable/20488273.

[96] P de Hert y Gutwirth, «Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action», en Gutwirth et al (ed.), Reinventing Data Protection? (Springer, 2009) 5 p. 8.

[97] Lynskey (n **Error! Marcador no definido.**), p. 586-587.

[98] AF Westin, *Privacy and Freedom* (1967, Atheneum), p. 324-325.

[99] Gavison, Ruth E., Privacy and the Limits of Law (16 de mayo de 2012).. *The Yale Law Journal,* Vol. 89, No. 3 (enero, 1980), p. 421-471, Disponible en SSRN: https://ssrn.com/abstract=2060957, o Zuboff, Shoshana, Big Other:. Surveillance Capitalism and the Prospects of an Information Civilization (4 de abril de 2015). *Journal of Information Technology* (2015) 30, 75-89. doi:10.1057/jit.2015.5, disponible en SSRN: https://ssrn.com/abstract=2594754

[100] Para una elaboración de esta distinción, véase González-Fuster e Hijmans (n **¡Error!. Marcador no definido.**), p. 6.

[101] R Post, «Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere» (2018)67 *Duke Law Journal* 980

[102] CJ Hoofnagle, B van der Sloot y FZ Borgesius, «The European Union general data protection regulation: what it is and what it means» (2019) 28 *Information & Communications Technology Law* 65.

[103] L Dalla Corte, «A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection» en Hallinan et al (ed.), *Data Protection and Privacy: Data Protection and Democracy* (Hart, 2020) p. 27; Véase también Veil (n **Error! Marcador no definido.**), p. 22.

[104] H Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016), apartado 2,13. [105] N Andrade, «Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights», p. 7. Disponible en: www.hal.inria.fr/hal-01559453.

[106] A Rouvroy y Y Poullet, «The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy» en S Gutwirth et al (ed.), Reinventing Data Protection?. (Springer 2009), p. 45.

[107] Andrade sugiere, por ejemplo, que «solo después de la ponderación y equilibrio de los intereses y derechos sustantivos en cuestión, entran en juego los derechos procesales estableciendo las condiciones legales

y procedimientos mediante los cuales se aplicarán efectivamente dichos derechos sustantivos». Andrade (n **¡Error! Marcador no definido.)** 6.

[108] En el Derecho Constitucional de los EE. UU., persisten los debates sobre el carácter de derecho sustantivo o procesal del debido proceso. Sin embargo, nunca se ha cuestionado su condición de derecho constitucional. Igual podría decirse del derecho a un juicio justo, que goza de reconocimiento en múltiples instrumentos jurídicos internacionales. Más recientemente, los derechos procesales medioambientales se han incluido en los documentos constitucionales nacionales y en los acuerdos jurídicos internacionales.

[109] Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Observación general sobre el artículo 9 de la CDPD de la ONU (Accesibilidad*) - https://www.ohchr.org/ES/HRBodies/CRPD/Pages/GC.aspx.

[110] Articulo 1, Carta de la UE (n **¡Error Marcador no definido.)** Aunque el CEDH no incluye expresamente el derecho a la dignidad humana, en el Protocolo n.º 13 sobre la protección de los Derechos Humanos y de las Libertades Fundamentales, relativo a la abolición de la pena de muerte en cualquier circunstancia, se refiere a la necesidad del «pleno reconocimiento de la dignidad inherente a todos los seres humanos».

[111] I Kant, *Groundwork for the Metaphysics of Morals* (Abbott Thomas K. tr., 2005), 88 (énfasis omitido)..

[112] D Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994), p. 109.

[113] D Keats Citron y Pasquale, «The Scored Society: Due Process for Automated Predictions» (2014) 89 *Washington Law Review* 1, 3.

[114] Colin J. Bennett, «In Defence of Privacy: the concept and the regime» de *Surveillance and Society* 8(4) 2011, p. 485-496 - https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4184/privacy_debate.

[115] Frederik J. Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International, 2015), p. 43.

[116] Justin Sherman, «Data Brokers Are A Threat To Democracy», *Wired* (abril de 2021) - https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/.

[117] Lyon (n 112), p. 13.

[118] K Crawford y Schultz, «Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms» (2014) 55 *Boston College Law Review* 93, p. 111.

[119] Lyon (n 112), p. 70-71. Véase también A Spina, «Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?» (2014) 2 *European Journal of Risk Regulation* 248, p. 251.

[120] J Raz, *The Morality of Freedom* (Oxford University Press, 1986), p. 369.

[121] «Invictus», WE Henley en «A Book of Verses» (D. Nutt, 1888), p. 56-57.

[122] Acquisti, Alessandro, Curtis Taylor y Liad Wagman. 2016. «The Economics of Privacy». *Journal of Economic Literature*, 54 (2):442-92 - https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442

[123] Por ejemplo, véase «The Failure of Fair Information Practice Principles», de Fred H. Cate, de *Consumer Protection in the Age of the Information Economy* (2006) - https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf

[124] TI Emerson, *The system of freedom of expression* (Random House Trade, 1970), p. 549.

[125] Regan, Priscilla M. Legislating Privacy: Technology, Social Values and Public Policy. Chapel Hill, Carolina del Norte: University of North Carolina Press, 1995; o,

[126] Sobre la mercantilización véase: C Prins, «When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter» (2006) 3 SCRIPTed 270.

[127] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (7.ª Ed., enero 2021) (11 de febrero de 2021). (2021) 169 *Privacy Laws & Business International Report.* 6-19, Disponible en SSRN: https://ssrn.com/abstract=3836261 o http://dx.doi.org/10.2139/ssrn.3836261.

[128] Graham Greenleaf, A*sian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, 2014) y *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) - https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia

[129] Un ejemplo sería Singapur. con su política de derechos humanos, informada por objetivos estatales primordiales y objetivos de desarrollo nacional, que priorizan activamente el crecimiento económico y el orden social. Los imperativos del desarrollo económico y la referencia cultural al comunitarismo neoconfuciano matizan el alcance y la aplicación de los derechos humanos. Véase Prof Thio Li-Ann, «Pragmatism and realism do not mean abdication: a critical and empirical inquiry into Singapore's

engagement with international human rights law» en *Singapore Year Book of International Law* (2004) 8, p. 41-91 - http://www.asianlii.org/sg/journals/SGYrBkIntLaw/2004/4.pdf.

130 Por ejemplo, algunas de las primeras leyes de protección de datos del mundo tienen origen en jurisdicciones de Asia-Pacífico, como Hong Kong, Nueva Zelanda, Australia, Corea del Sur y Japón. Pese a su eficacia y robustez, constituyen su núcleo las obligaciones organizativas y los derechos de los titulares de los datos, en contraposición a la preocupación por los derechos humanos.

131 China, la UE y EE.UU. se adhirieron a la Vía de Osaka. India, Indonesia y Sudáfrica, en cambio, optaron por no participar, lo que indica una clara división en el futuro de las negociaciones sobre comercio electrónico y gobernanza de datos en la OMC.

132 La visión de la política exterior de la India en torno a las normas de protección de datos está estrechamente vinculada a las concepciones de «soberanía de datos» o, más críticamente, de «colonialismo de datos» (afín a la noción de capitalismo de vigilancia de Zuboff). Véase Arindrait Basu, «Sovereignty in a "datafied" world: A framework for Indian diplomacy» en *Observer Research Foundation* (2 de mayo de 2021) - https://www.orfonline.org/expert-speak/sovereignty-datafied- world-framework-indian-diplomacy.

133 Véase, por ejemplo, «Asia's Family Values Give Way to Data Privacy Concerns» https://www.voanews.com/silicon-valley-technology/asias-family-values-give-way-data-privacy-concerns, e IAPP, «Why China's cultural attitudes toward privacy may be in flux» - https://iapp.org/news/a/why-chinas-cultural-attitudes-toward-privacy-may-be-in-flux/.

134 K Kitiyadisai, «Privacy rights and protection: foreign values in the modern Thai context» (2005)7. *Ethics and Information technology* 17, p. 19.

135 HN Olinger, JJ. Britz, y MS. Olivier «Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa» (2007)39 *The International Information & Library Review* 31

136 Ibíd, p.35.

137 Ibíd.

138 Este argumento es esgrimido, por ejemplo, por Shoshana Zuboff, Véase S Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).

139 *A History of Private Life: from Pagan Rome to Byzantium*, vol. 1, ed. Paul Veyne (Harvard, 1987), 415

140 Evgeny Morozov, *To Save Everything, Click Here: the folly of technological solutionism* (2013), 346; véase también Ursula Franklin, “Liberty, technology and hope” from The Ursula Franklin Reader (2006), 172

141 John Stuart Mill, *On Liberty* (NY, 1947, 4-5.

142 Además, en un contexto de información ha resultado difícil identificar un perjuicio real para los intereses individuales, por no hablar del interés de los demás o de la comunidad. Sin embargo, las nuevas formas de uso (y abuso) de los datos han puesto de manifiesto que dichos intereses colectivos no deben ignorarse al contemplar tanto la necesidad como el alcance de ambos derechos.

143 Ver nota **¡Error! Marcador no definido.**

144 En el pasado, los anunciantes en línea han argumentado que el mero rastreo de los usuarios de Internet mediante el uso de cookies no debe estar sujeto a ninguna forma de regulación porque, según ellos, «no se produce daño alguno», y que las normas de privacidad y protección de datos solo deberían comprometerse cuando se extraen los datos de comportamiento de los usuarios y los perfiles del comportamiento de los usuarios se crean por los propios usuarios.

145 En 1962, la Asamblea General de las Naciones Unidas reconoció el «derecho de los pueblos y naciones a la soberanía permanente sobre sus riquezas y recursos naturales». Es una articulación clara tanto de los intereses del grupo como del derecho que estos tienen a opinar sobre los recursos considerados cruciales para los intereses colectivos del grupo. Véase Malcolm Shaw, *International Law, Fifth Edition* (2003, Cambridge University Press).

146 El planteamiento es especialmente evidente en el sector público, donde diversas entidades proclaman que es necesario acceder a datos personales que están en poder de otros departamentos o de empresas para promover intereses públicos legítimos como la seguridad, la salud pública o el uso responsable de los fondos públicos.

147 P Ohm, «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization» (2010) 57 UCLA Law Review 1701, p. 2010

148 J Rauhofer (n 21), pp. 606-617.

149 J Cohen (n 18), p. 72.

150 M Adrejevic, «iSpy: Surveillance and Power in the Interactive Era», (University Press of Kansas, 2007), p. 2-4 y 104-11.

151 Artículo 5, apartado 1, letra c), del RGPD.

[152] Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019), p. 8.
[153] Sin embargo, existe también la preocupación de que la elaboración de perfiles y la posterior selección de personas puedan acarrear discriminación de precios y comercialización predatoria dirigida a determinados grupos de consumidores. Para un análisis más reciente de estas cuestiones, véase N Newman, «The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google» (2013); disponible en SSRN: http://ssrn.com/abstract=2310146, última visita el 20 de octubre de 2020.
[154] Para una exploración detallada de este fenómeno, véase E Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2011).
[155] También parece fuera de toda duda que este uso concreto de los datos personales —para elaborar perfiles y dirigirse a personas concretas— ha sido, si más no, notablemente eficaz al hacer llegar ciertos mensajes políticos a un público más amplio, explotando el descontento existente y conectando a los afines entre sí de un modo que antes no era posible. Por supuesto, como todas las tecnologías, estas herramientas pueden utilizarse para el bien o para el mal, y lo que se considere una u otra cosa puede estar aún en el ojo del que observa. Sin embargo, la difusión de las técnicas de vigilancia del comportamiento puede, como argumenta Cohen, haber «producido poderosas oportunidades para la volatilidad, la polarización y la sinrazón pública», Cohen (n 18), p. 86.
[156] El uso de la energía nuclear, los daños medioambientales o ciertos tipos de investigación suelen citarse como elementos de comparación.
[157] J Cohen (n 18), p. 90.
[158] PM Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995), p. 230.
[159] ibíd, p. 233.
[160] S Simitis, «Reviewing Privacy in an Information Society» (1987)135 University of Pennsylvania Law Review 709.
[161] Con rara clarividencia, Simitis también apuntó que la cuestión de quién puede acceder a los datos personales y qué puede hacer con ellos ya no debe ser una preocupación principalmente individual (por ejemplo, de los famosos, que desean ocultar sus actividades a un público curioso): el debate debe considerar los intereses públicos o colectivos. Según él lo ve, esto es cierto, en especial, para el tipo de tratamiento de datos ubicuo que normaliza la vigilancia del público por quienes detentan el poder, y apoya su capacidad para determinar y hacer cumplir las normas legales y sociales.
[162] ibíd, p. 734. Véase también S Simitis, «Die informationelle Selbstbestimmung—Grundbedingung einer verfassungskonformen Informationsordnung» (1984) Neue Juristische Wochenschrift 394-405, p. 399.
[163] S Simitis, n 160.
[164] Si bien estableció el derecho a la autodeterminación informativa específicamente con el fin de otorgar al individuo un control (cualificado) sobre sus datos personales, (uno de) los fundamentos subyacentes para otorgar a los individuos tal protección era equiparlos para el ejercicio de dichos derechos en beneficio de sus comunidades.
[165] Ver nota **¡Error! Marcador no definido.**
[166] Observación General (n **¡Error**! **Marcador no definido.**), apartado 3 y 7.
[167] Las alegaciones de que la protección de datos y la privacidad constituyen un obstáculo para el logro de otros derechos e intereses no suelen, por tanto, aplicar adecuadamente este método de conciliación o ni tan solo comprender que dicha conciliación es posible.
[168] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Artículo 19: Libertad de opinión y de expresión* - https://www.ohchr.org/ES/NewsEvents/Pages/DisplayNews.aspx?NewsID=23944&LangID=E
[169] Véase, por ejemplo, el artículo 8, apartado 2, del CEDH. Partiendo de la noción de que la seguridad nacional se ha concebido para proteger el derecho a la vida, suele resultar difícil argumentar que, con todo, debe alcanzarse un equilibrio entre ambos intereses. Sin embargo, la seguridad es también una cuestión de perspectiva y del modelo de amenaza que se utiliza para justificar las intrusiones en la privacidad. Por lo general, quienes abogan por restringir los derechos fundamentales en aras de la seguridad se basan generalmente en un modelo de amenaza exterior; a saber, la posibilidad de un ataque del enemigo exterior en el contexto del terrorismo o la delincuencia organizada. Las medidas de seguridad preconizadas en este contexto suelen presentarse como protectoras de los individuos, cuyos derechos a la privacidad o a la protección de datos pueden vulnerarse por dichas medidas, y el estado asume el papel de protector. El equilibrio que debe alcanzarse en este caso se representa así como un juego de suma cero en el que mayor seguridad (proporcionada por el Estado) requerirá forzosamente una injerencia en la privacidad del individuo (perpetrada por el Estado). Sin embargo, existen contemporáneamente otros modelos de amenaza que deben tenerse presentes al intentar encontrar el equilibrio entre privacidad y seguridad.

Uno de esos modelos de amenaza está orientado hacia el interior, a saber, la amenaza a la que se exponen los individuos —solos y colectivamente— ante un modelo de gobierno autoritario o totalitario. Los instrumentos de derechos humanos se han desarrollado mayoritariamente como derechos de defensa negativos creados para proteger al individuo del estado prepotente. Así, en el contexto referido, la seguridad podría definirse como la seguridad frente a las propias instituciones que tratan de justificar la necesidad de interferir en los derechos y libertades del individuo cualesquiera que sean las protecciones que dichos instrumentos aporten. En esta situación, los individuos recurren al derecho a la privacidad y a la protección de datos justamente para contrarrestar la amenaza que emana del Estado, tanto para la seguridad personal propia como para las instituciones democráticas creadas para proteger sus derechos y libertades. Así, pues, que la seguridad requiera la vulneración o la protección de la privacidad informativa depende de cómo se enmarque la amenaza.

170 Véase *Klass contra Alemania* y *Amann contra Suiza* (n **¡Error!**. **Marcador no definido.)**

171 Véase *Sentencia del Tribunal de Justicia en el asunto C-746/18 Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* (n 45).

172 Naciones Unidas, *Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación al Consejo de Derechos Humanos* (mayo de 2019) - https://undocs.org/A/HRC/41/41.

173 CJ Bennett y Raab, *The Governance of Privacy* (2.ª ed., MIT Press, 2006) p. 23.

174 En otros ámbitos, esto también sugiere que la comodidad y eficacia que las entidades, tanto públicas como privadas, obtienen de la creación de grandes almacenes de datos (por ejemplo, registros sanitarios nacionales centralizados) o métodos de vigilancia ubicua (como las cámaras de seguridad, las tecnologías de reconocimiento facial o el seguimiento del comportamiento en línea) deben sopesarse considerando la posibilidad de abusos. Unas medidas de seguridad técnicas y reglamentarias eficaces pueden evitar que el «estado de base de datos» se convierta en el equivalente virtual del «panóptico» de Jeremy Bentham, el famoso modelo carcelario en el que los reclusos podían ser vigilados desde un punto central sin que supieran cuándo —o incluso si— se les observaba. Se debe a que la «mirada desigual» que caracteriza a este tipo de vigilancia conlleva el riesgo de provocar la interiorización de una mentalidad disciplinaria en las personas observadas. Si bien, por un lado, esto significa que los individuos que viven bajo esa mirada tienen menos probabilidades de infringir las normas o las leyes; por otro, pueden verse disuadidos de ejercer sus derechos y libertades individuales o de participar en general en el proceso democrático.

175 Bloustein, «Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser» (1964) 39 *New York University Law Review* 1000.

176 Lyon, *Surveillance after September 11* (Polity Press, 2003), p. 27.

177 Esta es, de hecho, la premisa de la película «Minority Report», en que las fuerzas del orden han hallado una forma de predecir la comisión de un delito y, por tanto, son capaces de evitarlo. Por desgracia, en algunos casos, el método de predicción resultó ser defectuoso. Los miembros de categorías «sospechosas» (por ejemplo, los miembros de comunidades musulmanas) pueden interiorizar la sospecha, lo que se resulta en una percepción de «observación no deseada» y en una evitación de actividades y asociaciones que puedan malinterpretarse. Esto puede conducir a una pérdida de participación política de grupos minoritarios específicos, probablemente en perjuicio del tejido político de una sociedad democrática. También puede animar a los miembros de ese grupo a recurrir a formas alternativas de protesta y contraacción y, en última instancia, a su completa alienación de la sociedad y sus valores.

178 Lyon (n 176) p.142

179 Ibíd.

180 PM Regan (n 158), p. 227

181 Benett y Raab (n 173).

182 Relator Especial de las Naciones Unidas sobre el derecho a la privacidad, *Evaluación preliminar de las dimensiones de privacidad de la pandemia de la enfermedad por coronavirus (COVID-19)* (julio 2020) - https://undocs.org/A/75/147

183 Otro ejemplo podría ser que el Tribunal Supremo israelí prohibiera al servicio de seguridad israelí seguir accediendo a los datos móviles de los ciudadanos sin autorización legislativa específica. (Uso no consentido). Ver Reuters, «Israel's top court says government must legislate COVID-19 phone-tracking» (26 de abril de 2020)- https://www.reuters.com/article/us-health-coronavirus-israel-monitoring-idUSKCN2280RN.

184 B Petkova, «La privacidad como primera enmienda de Europa» (2019) 25 *European Law Journal* 140, p. 152. 185 D Kaye, «Informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión», Consejo de Derechos Humanos: vigésimo noveno periodo de sesiones, punto 3 del orden del día, 22 de mayo de 2015, p. 15.

186 NM Richards, *The Dangers of Surveillance*, (2013)126 *Harvard Law Review* 1934, p. 1945-1952.

187 Ibíd, p. 1935.

188 ibíd, p. 1948.
189 *Open Door and Dublin Well Woman v Ireland*, recurso n.º 14235/88, (TEDH, 29 de octubre de 1992)
190 ibíd., apartado 81.
191 Comité de los Derechos del Niño de las Naciones Unidas, *Observación general nº 25 (2021) sobre los derechos del niño en relación con el entorno digital* (marzo de 2021) - https://digitallibrary.un.org/record/3906061?ln=es; véase también Women's Legal Education and Action Fund (LEAF), *De-platforming misogyny* (abril de 2021) - https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
192 Marie-Claude Landry (Comisaria Jefe de la Comisión Canadiense de Derechos Humanos), «los derechos humanos y el derecho a la privacidad deben evolucionar a la par....». Es necesario un enfoque de derechos humanos en la reforma de la legislación sobre privacidad en este país para abordar las preocupaciones emergentes sobre cómo la tecnología y el mundo digital afectan cada vez más a nuestra vida cotidiana. La tecnología y la privacidad son fundamentales para la próxima generación de derechos humanos. Todo el mundo en Canadá debería poder beneficiarse de la tecnología sin temor». (July, 2020) - https://www.chrc-ccdp.gc.ca/en/resources/supreme-court-decision-a-human- rights-victory-protection-genetic-discrimination
193 Comité de los Derechos del Niño de las Naciones Unidas, *Observación general nº 25 (2021) sobre los derechos del niño en relación con el entorno digital* (marzo de 2021) - https://digitallibrary.un.org/record/3906061?ln=es; véase también Women's Legal Education and Action Fund (LEAF), *De-platforming misogyny* (abril de 2021) - https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
194 El Comité de la ONU emite recomendaciones para proteger los derechos de los niños en el entorno digital https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26944&LangID=E
195 https://www.unicef.org/globalinsight/featured-projects/ai-children.
196 *DERECHOS HUMANOS EN LA ERA DE LA INTELIGENCIA ARTIFICIAL - AI-and-Human-Rights.Pdf*..https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.
197 *UN Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression - AI and Human Rights 2018 AI-and-FOE-GA.Pdf*. https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf.
198 *The OECD Artificial Intelligence Policy Observatory*. https://www.oecd.ai/ ; *EU White Paper on Artificial Intelligence – a European Approach to Excellence and Trust | Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/consultations/white-paper-artificial-intelligence- european-approach-excellence-and-trust. ; *Kung - Building an AI World Report on National and Regio.Pdf*. https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf. ; «Council of Europe and Artificial Intelligence». *Artificial Intelligence*, https://www.coe.int/en/web/artificial-intelligence/home ;
Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights 1680946e64.Pdf. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.
199 *Artificial Intelligence: Governance and Leadership Whitepaper (2019) | Comisión Australiana de Derechos Humanos*. https://humanrights.gov.au/our-work/rights-and-freedoms/publications/artificial-intelligence-governance-and-leadership.
200 Orientaciones políticas sobre IA para niños: *Borrador para consulta | Recommendations for building AI policies and systems that uphold child rights* https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children
201 Krishnamurthy, Vivek. «It's Not Enough for AI to Be "Ethical"; It Must Also Be "Rights Respecting"». *Medium*, 10 oct. 2018, https://medium.com/berkman-klein-center/its-not-enough-for-ai-to-be-ethical-it-must-also-be-rights-respecting-b87f7e215b97 ; Raso, Filippo A., et al. *Artificial Intelligence & Human Rights: Opportunities & Risks*. SSRN Scholarly Paper, ID 3259344, Social Science Research Network, 25 de septiembre de 2018. *papers.ssrn.com*, doi:10.2139/ssrn.3259344.
202 Tales como el Grupo de trabajo intergubernamental de composición abierta sobre las empresas transnacionales y otras empresas comerciales en la esfera de los derechos humanos, a quien se ha encomendado la elaboración de un instrumento internacional jurídicamente vinculante sobre derechos humanos para regular las actividades de las empresas transnacionales y otras empresas comerciales https://www.ohchr.org/en/hrbodies/hrc/wgtranscorp/pages/igwgontnc.aspx ; https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.. pdf
203 Y «AI, ADM and the Justice System». *LCO-CDO*, https://www.lco-cdo.org/en/our-current- projects/ai-adm-and-the-justice-system/.
204 Revised draft U.N. treaty on business and human rights: a few steps forward, a few unanswered questions https://www.accessnow.org/revised-draft-u-n-treaty-on-business-and-human-rights-a-few-steps-forward-a-few-unanswered-questions/

205 *INFOVEILLANCE | The Royal Society of Canada*. https://rsc-src.ca/en/research-and-reports/infoveillance.
206 Canadá, Oficina del Comisario de Privacidad *Comunicado de prensa: El Comisario, animado por las propuestas para modernizar la Ley de Privacidad del Sector Público*. 24 mar. 2021, https://www.priv.gc.ca/en/opc- news/news-and-announcements/2021/nr-c_210324/.
207 *Equinet Report: REGULATING FOR AN EQUAL AI: A NEW ROLE FOR EQUALITY BODIES. https://equineteurope.org/2020/equinet-report-regulating-for-an-equal-ai-a-new-role-for-equality- bodies/ ;*
208 O De Schutter and J Ringelheim, «Ethnic Profiling: A Rising Challenge for European Human Rights Law» (2008)71 Modern Law Review 358
209 M Veale y R Binns, «Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data» (2017) 4 *Big Data & Society*. Disponible en: https://journals.sagepub.com/doi/epub/10.1177/2053951717743530 .
210 Resolución 74/29, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público. (Adoptada por el Comité de Ministros el 20 de septiembre de 1974, durante la 236ª reunión de los Delegados de los Ministros). Anexo , apartado 3.
211 G Malgieri, «The concept of fairness in the GDPR: a linguistic and contextual interpretation», FAT* '20: Actas de la 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020).
212 Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Article IX.
213 CNIL, «How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence» (2017), p. 49. Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.
214 Según Greenleaf, en escrito de 2016, al final de cada década, el número de leyes se ha ampliado de 10 (década de 1970) a 20 (década de 1980), a 40 (década de 1990), a 80 (década de 2000), y ahora a 111 (dos tercios a través de la década de 2010). Señala que el «indicador más interesante de la mundialización de las leyes de privacidad de datos es que, desde 2015, la mayoría de dichas leyes (57/111) son de fuera de Europa». G Greenleaf, «Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside Europe» [2016] UNSWLRS 52, p. 1.
215 Avis n° 934/2018, Commission Européenne pour la Démocratie par le Droit (Commission de Venise), Luxembourg – Proposition de revision portant instauration d'une nouvelle constitution, Strasbourg, le 27 février 2019 (Rapport de la Luxembourg, CDL-REF(2019)006); see also, TA Larsen, C Boulanger y A Vandendriessche, «Luxembourg» en *The New EU Data Protection Regime: Setting Global Standards for the Rights to Personal Data Protection* (The Hague, 2020), 411 y 412.
216 Lynskey (n **Error! Marcador no definido.** anterior), apartado 169.
217 La Ley de privacidad de datos de 2012 (Ley n.º 10173) de Filipinas, aprobada en 2012, se inspira en parte
en la propuesta legislativa de la Comisión Europea sobre el RGPD. Contiene, por ejemplo, un derecho a la portabilidad de los datos (sección 18) cuya redacción es similar a la del derecho que ahora se encuentra en el artículo 20 del RGPD y que, por lo demás, es exclusivo de este.
218 Convenio 108+ (n 2), artículo 37, apartados 1 y 2.
219 ibíd., artículo 4, apartado 3.
220 Véase, presentación de la profesora Cécile De Terwangne, «Convention 108+ evaluation and follow-up mechanisms», 1 de julio de 2020. Disponible en: https://www.coe.int/en/web/data-protection/follow-up-and- evaluation-mechanism.
221 Los signatarios no europeos del Convenio 108 son Argentina; Cabo Verde; Marruecos; Mauricio; México; Senegal; Túnez; y Uruguay (https://www.coe.int/en/web/conventions/full-list/-). /conventions/treaty/108/signatures?p_auth=TAAIBf9O). De ellos, Argentina, Mauricio, Túnez y Uruguay han firmado el Convenio 108+, que Mauricio también ha ratificado (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures).
222 Los Estados no europeos que se adhieran hasta la entrada en vigor del Protocolo de enmienda deberán depositar instrumentos de adhesión tanto para el Convenio 108 como para el Protocolo de enmienda. La lista de observadores (actualizada por última vez en marzo de 2020) está disponible aquí: https://rm.coe.int/list-of-observers-nov-2018-en/1680938538.
223 Colin J. Bennett, «The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession» CIGI Paper No. 246 (30 de noviembre de 2020) - https://www.cigionline.org/publications/council-europes-modernized-convention-personal-data-protection-why-canada-should/

[224] Así se indica en la respuesta del Consejo de Europa al Cuestionario de la GPA (PSWG3 - Privacidad/Protección de datos y otros derechos y libertades).
[225] Para consultar la lista completa de los Estados no europeos que han ratificado el Convenio, véase: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Ryk2y1sX (última accesp: 20 de octubre de 2020).
[226] G Greenleaf, «How far can Convention 108+ "globalise"? Prospects for Asian accessions» (2020) Computer Law & Security Review. Acceso anticipado: https://doi.org/10.1016/j.clsr.2020.105414 . Las trece ventajas clave de la adhesión al Convenio 108 identificadas por Greenleaf son: «(i) perspectivas realistas; (ii) ninguna alternativa realista; (iii) obligaciones voluntarias; (iv) reconocimiento internacional de las "mejores prácticas"; (v) exportaciones recíprocas de datos; (vi) normas moderadas; (vii) normas mínimas; (viii) un sustituto de la "lista blanca"; (ix) ayuda a la "adecuación"; (x) ayuda al desarrollo; (xi) beneficios empresariales con exportaciones e importaciones; (xii) beneficios individuales de las protecciones mínimas; y (xiii) ayuda a las organizaciones internacionales».
[227] Comisión Europea, «Comunicación de la Comisión al Parlamento Europeo y al Consejo: Intercambio y protección de datos personales en un mundo globalizado» COM (2017)7 final
[228] Relator Especial de las Naciones Unidas sobre el derecho a la privacidad - Informe anual; Septuagésimo tercer período de sesiones de la Asamblea General de las Naciones Unidas 2018 [2018] UNSRPPub 11 (17 de octubre de 2018), párr. 117(e).
[229] G Greenleaf, «How far can Convention 108+ "globalise"? Prospects for Asian accessions» (2020) Computer Law & Security Review. Acceso anticipado:
[230] Ibíd, p. 19.
[231] Ibíd, p. 19.
[232] ibíd, p. 4.
[233] Asamblea General de la ONU, Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, 19 de diciembre de 1966, Naciones Unidas, Serie de Tratados, vol. 999, p. 171, artículo 2
[234] Por ejemplo, el Pacto Internacional de Derechos Civiles y Políticos de la ONU sigue siendo una Convención pertinente con la que empezar (o continuar). Sin embargo, deben tenerse en cuenta otras Convenciones, especialmente las que dialogan o interactúan con la protección de datos y la privacidad (aunque sea de forma inferida), como la Convención sobre los Derechos del Niño, la Convención para erradicar cualquier forma de discriminación contra la mujer, entre otras.