

Fundación de los Principios de la Soberanía Digital Individual

Nota preliminar de alcance conceptual

El uso del término Soberanía Digital Individual en este manifiesto no pretende sustituir, negar ni disputar la soberanía del Estado en sentido jurídico-político clásico. Se utiliza como una categoría doctrinal destinada a describir una esfera reforzada de autodeterminación de la persona frente al poder informacional ejercido por actores públicos y privados en la sociedad digital.

La Soberanía Digital Individual no propone un poder individual absoluto, una propiedad patrimonial ilimitada sobre toda información relacionada con la persona, ni una forma de anonimato inmune a la ley. Su fundamento principal es la dignidad, la autonomía, la personalidad, la libertad y el control efectivo sobre los usos de la identidad digital que puedan afectar a los derechos, oportunidades o condiciones de vida de una persona.

Este manifiesto defiende que la identificación, la autenticación, la verificación de atributos y el acceso a información personal deben someterse a criterios de legalidad, necesidad, proporcionalidad, minimización, transparencia, responsabilidad y debido proceso. La protección de la identidad digital no exige aislar al individuo del Derecho, sino impedir que la participación en la sociedad digital dependa de una exposición permanente, innecesaria o desproporcionada de la persona.

Por tanto, esta propuesta no pretende sustituir los marcos existentes de protección de datos, privacidad, identidad o responsabilidad tecnológica, sino señalar la necesidad de evolucionar desde un modelo centrado principalmente en el tratamiento de datos hacia un modelo centrado en la persona como titular de una identidad digital que merece protección reforzada.

Introducción

La humanidad se encuentra ante una transformación comparable a los grandes cambios que definieron la Edad Moderna y la Revolución Industrial.

Durante siglos, la libertad individual estuvo vinculada al control del propio cuerpo, de la propiedad privada y de la participación en la vida pública sin sometimiento arbitrario. Sin embargo, el siglo XXI ha introducido una nueva dimensión de la existencia humana para la cual nuestras instituciones jurídicas, económicas y políticas no fueron diseñadas: la identidad digital.

Cada búsqueda, desplazamiento, conversación, compra, interacción social o expresión de opinión puede generar información susceptible de ser almacenada, analizada, correlacionada y explotada a escala masiva. La acumulación de estos datos ha producido una concentración inédita de conocimiento sobre los individuos y ha dado lugar a una nueva forma de poder basada en la capacidad de observar, perfilar, predecir e influir sobre el comportamiento humano.

La información se ha convertido en uno de los recursos estratégicos más valiosos de nuestra era. Los datos personales alimentan sistemas de inteligencia artificial, mercados publicitarios, plataformas digitales, infraestructuras financieras y mecanismos automatizados de toma de decisiones. Sin embargo, quienes generan continuamente ese valor rara vez ejercen un control efectivo sobre él y, en la mayoría de los casos, no participan de manera significativa en los beneficios, decisiones o condiciones que derivan de su explotación.

Esta asimetría ha alterado el equilibrio entre individuos, instituciones y organizaciones. Cuanto más depende la sociedad de los datos, menos capacidad real tienen muchas personas para controlar la información que las describe. Cuanto más valiosa se vuelve la identidad digital, más urgente resulta reconocer mecanismos que protejan la autonomía personal frente a sistemas capaces de clasificar, condicionar o influir sobre la vida humana.

Por ello, la privacidad ya no puede concebirse únicamente como un derecho defensivo destinado a ocultar información. Constituye una condición indispensable para la libertad individual, la autonomía moral, la dignidad humana y el ejercicio efectivo de los derechos fundamentales en la era digital. Cuando una persona pierde el control sobre la información que la representa, no pierde solo privacidad: pierde capacidad de decisión, negociación, autodeterminación y libertad.

Este manifiesto sostiene que ha llegado el momento de reconocer una nueva generación de derechos digitales capaces de restaurar el equilibrio entre individuos e instituciones, devolver a las personas el control efectivo sobre su identidad digital y garantizar que la transformación tecnológica continúe sirviendo a la libertad humana en lugar de erosionarla.

I. La identidad digital es una extensión de la persona

La identidad digital no constituye un simple conjunto de registros tecnológicos. Representa la proyección de la personalidad humana en el entorno digital. Los atributos digitales, las credenciales, las interacciones, la reputación y la huella informacional forman parte de la representación contemporánea del individuo. Por tanto, la identidad digital debe recibir una protección jurídica equivalente a la otorgada a otros elementos fundamentales de la personalidad. Ninguna persona debería perder el control efectivo sobre la representación digital de sí misma.

II. La concentración de datos genera concentración de poder

Los datos personales son actualmente uno de los recursos más valiosos de la economía global. La acumulación masiva de información permite construir perfiles detallados, anticipar comportamientos y ejercer influencia sobre decisiones individuales y colectivas. Cuando el control de dichos datos se concentra en un número reducido de actores, también se concentra el poder. La desigualdad digital no surge únicamente de la diferencia en acceso a la tecnología, sino también de la diferencia en acceso al conocimiento derivado de los datos. La defensa de la privacidad constituye, por tanto, una defensa contra la concentración excesiva de poder informacional.

III. De la protección de datos a la soberanía digital individual

La Soberanía Digital Individual es la capacidad jurídica, técnica e institucional de una persona para controlar efectivamente su identidad digital, limitar su exposición, revocar autorizaciones, exigir transparencia y participar en las decisiones que afecten a su representación digital.

Las últimas décadas han sido testigo de avances importantes en la protección jurídica de la privacidad y de los datos personales. Instrumentos normativos como el Reglamento General de Protección de Datos de la Unión Europea han fortalecido los derechos de las personas frente al tratamiento de información personal por parte de organizaciones públicas y privadas. El reconocimiento de derechos como el acceso, la rectificación, la supresión, la oposición, la limitación del tratamiento y la portabilidad constituye uno de los desarrollos más relevantes en la evolución contemporánea de los derechos digitales.

Sin embargo, la protección de datos y la soberanía digital individual no son conceptos equivalentes. La protección de datos establece límites sobre cómo terceros pueden recopilar, utilizar y almacenar información personal. La soberanía digital individual, en cambio, exige que la persona conserve una capacidad efectiva de decisión sobre la identidad digital que la representa en el entorno tecnológico.

A pesar de los avances regulatorios, el modelo dominante de Internet continúa basado en arquitecturas donde la identidad, los atributos personales y los datos de los usuarios son almacenados, gestionados y explotados principalmente por organizaciones que controlan plataformas, servicios e infraestructuras digitales. En la práctica, el individuo suele ejercer derechos sobre información que ya ha sido recopilada, almacenada y procesada por terceros.

La siguiente etapa en la evolución de los derechos digitales requiere avanzar desde un paradigma centrado exclusivamente en la protección de datos hacia un paradigma centrado en la persona. La soberanía digital individual no exige eliminar a las organizaciones como custodios o procesadores de información ni impedir el intercambio legítimo de datos. Su finalidad es reequilibrar la distribución del poder informacional, garantizando que la persona conserve control efectivo sobre los elementos digitales que conforman o afectan a su identidad.

Esta soberanía implica, como mínimo, la capacidad de conocer qué información existe sobre uno mismo, determinar quién puede acceder a ella, decidir con qué finalidad puede utilizarse, establecer límites temporales, revocar autorizaciones, trasladar atributos entre sistemas y demostrar únicamente aquellos atributos estrictamente necesarios para una interacción digital legítima.

La protección de datos fue una respuesta necesaria a los desafíos de la sociedad de la información. La soberanía digital individual representa el siguiente paso en la evolución de los derechos fundamentales para una sociedad definida por la inteligencia artificial, la economía de los datos y la identidad digital.

IV. Definiciones fundamentales

Para delimitar el alcance de esta propuesta, el presente manifiesto utiliza los siguientes conceptos en el sentido que se expone a continuación.

Por identidad digital debe entenderse el conjunto de atributos, credenciales, identificadores, registros, interacciones, reputación, metadatos, inferencias y representaciones que permiten describir, reconocer, clasificar o vincular a una persona en entornos digitales. No se reduce a una cuenta, un nombre de usuario o un documento electrónico, sino que constituye una proyección informacional de la persona.

Por atributo digital debe entenderse toda característica, condición, cualidad, autorización, capacidad, relación o dato verificable asociado a una persona en el entorno digital, como la mayoría de edad, la residencia, una cualificación, una licencia, una pertenencia institucional o una autorización concreta.

Por credencial verificable debe entenderse una declaración digital emitida por una entidad competente o reconocible, susceptible de ser comprobada por terceros, mediante la cual una persona puede acreditar un atributo, derecho, condición o cualificación sin revelar más información de la necesaria.

Por dato personal debe entenderse toda información que identifique, describa, afecte o pueda vincularse razonablemente a una persona física, ya sea de forma directa o indirecta, incluyendo información proporcionada, observada, registrada, generada, correlacionada o tratada a partir de su actividad.

Por dato inferido debe entenderse toda información, predicción, clasificación, valoración, perfil o conclusión elaborada sobre una persona a partir del análisis de otros datos, aunque dicha persona no haya proporcionado directamente tal información.

Por perfil digital debe entenderse toda representación estructurada, total o parcial, de una persona construida mediante datos personales, datos observados, datos inferidos, patrones de comportamiento, valoraciones algorítmicas o correlaciones estadísticas, capaz de influir en decisiones que la afecten.

Por exposición de identidad debe entenderse la revelación, comunicación o puesta a disposición de elementos que permiten identificar, reconocer, rastrear o vincular a una persona en un contexto determinado.

Por identificación debe entenderse el proceso mediante el cual se determina o confirma quién es una persona. Por autenticación, el proceso mediante el cual se comprueba que una persona es quien afirma ser o que controla una determinada credencial, cuenta, dispositivo o medio de acceso. Por verificación de atributos, el proceso mediante el cual se acredita una característica específica sin revelar necesariamente la identidad completa.

Por custodia de datos personales debe entenderse la posición de responsabilidad asumida por toda organización, entidad o sistema que solicite, almacene, procese, conserve, analice o permita el acceso a información personal. Implica deberes proporcionales de justificación, seguridad, minimización, trazabilidad, confidencialidad, rendición de cuentas y reparación.

Por soberanía digital individual debe entenderse la capacidad jurídica, técnica, práctica e institucional de una persona para ejercer control efectivo sobre los elementos que conforman su identidad digital, determinar las condiciones legítimas de su utilización, limitar su exposición, revocar autorizaciones, exigir transparencia y participar de manera justa en las decisiones que afecten a la representación digital de sí misma.

Por valor generado por datos personales debe entenderse el beneficio económico, estratégico, organizativo, predictivo, publicitario, tecnológico o comercial que una entidad obtiene mediante la recopilación, análisis, inferencia, agregación, explotación o monetización sistemática de información vinculada a personas. Reconocer dicho valor no implica reducir la dignidad humana a una mercancía, sino exigir mecanismos de justicia, control y responsabilidad.

V. El derecho a la identidad verificable y la exposición mínima

Las sociedades democráticas requieren espacios en los que las personas puedan expresarse, participar y relacionarse sin quedar sometidas a una exposición permanente e innecesaria de su identidad. Al mismo tiempo, la convivencia digital exige mecanismos que permitan atribuir responsabilidad cuando se produzcan conductas ilícitas, abusivas o contrarias al interés público.

Durante años, el debate sobre la identidad en Internet se ha presentado como una elección entre anonimato absoluto e identificación permanente. Ambos modelos son insuficientes. El anonimato absoluto puede dificultar la atribución de responsabilidades; la identificación permanente, por su parte, obliga a exponer información personal ante organizaciones que no siempre necesitan conocerla ni están preparadas para custodiarla adecuadamente.

La necesidad de poder identificar a una persona cuando exista causa legítima y procedimiento adecuado no implica que dicha persona deba revelar permanentemente su identidad completa en todas sus interacciones digitales. Uno de los errores fundamentales de la arquitectura digital contemporánea consiste en asumir que identificación y exposición son inseparables. No lo son.

Una sociedad digital avanzada debe poder verificar identidades, atributos o credenciales sin exigir exposición constante de identidad. Del mismo modo que una persona puede demostrar su mayoría de edad sin revelar toda la información contenida en su documento de identidad, también debe poder acreditar residencia, condición profesional, titularidad de una credencial o condición de persona real sin exponer innecesariamente nombre, dirección, documentos identificativos u otros datos adicionales.

El principio es claro: ninguna persona debería verse obligada a revelar más información sobre sí misma de la estrictamente necesaria para participar en una interacción digital legítima. La exposición de identidad debe ser mínima, controlada y proporcional a la finalidad perseguida.

La tecnología contemporánea ya permite construir sistemas basados en credenciales verificables, pruebas criptográficas y validación de atributos que reducen significativamente la necesidad de compartir información personal. La cuestión central ya no es solo técnica, sino jurídica, política y social.

El objetivo no es eliminar la responsabilidad ni impedir la actuación legítima de las autoridades cuando resulte necesaria. El objetivo es garantizar que la participación en la sociedad digital no requiera una renuncia desproporcionada a la privacidad y al control sobre la propia identidad. La libertad digital del siglo XXI dependerá de nuestra capacidad para construir sistemas en los que las personas puedan ser identificables cuando sea necesario, pero no permanentemente identificadas por defecto.

VI. Límites legítimos, garantías y debido proceso

La Soberanía Digital Individual no constituye un derecho absoluto ni puede interpretarse como una barrera frente a toda forma legítima de identificación, investigación, supervisión o cumplimiento normativo. La protección reforzada de la identidad digital debe coexistir con la seguridad jurídica, la protección de terceros, la prevención del fraude, la persecución de conductas ilícitas y el interés público legítimo.

Sin embargo, la existencia de fines legítimos no justifica por sí sola la exposición permanente, indiscriminada o preventiva de la identidad de las personas. La posibilidad de identificar a una persona cuando exista causa legítima no exige que todas las personas deban permanecer permanentemente identificadas, rastreables o expuestas en cada interacción digital.

Toda limitación a la Soberanía Digital Individual debe someterse a criterios estrictos de legalidad, necesidad, proporcionalidad, finalidad específica, minimización, control independiente y debido proceso. La identificación forzosa, el acceso a información personal, la revelación de atributos sensibles o la intervención sobre credenciales digitales solo deberían admitirse cuando exista una base jurídica suficiente, una finalidad legítima claramente determinada y garantías efectivas contra el abuso.

La identificación legítima debe distinguirse de la vigilancia generalizada. Una cosa es permitir que una autoridad competente, bajo condiciones legales y garantías adecuadas, pueda atribuir responsabilidad por una conducta ilícita. Otra muy distinta es imponer arquitecturas digitales que obliguen a revelar la identidad completa de manera constante, innecesaria o desproporcionada.

La privacidad, el pseudonimato, la exposición mínima y la autonomía informativa no amparan el fraude, el acoso, la extorsión, la suplantación de identidad, la explotación de menores, la manipulación ilícita, la discriminación abusiva ni otras conductas contrarias a la dignidad, la seguridad o los derechos de otras personas.

Del mismo modo, los sistemas de identidad digital soberana no deben derivar en una identidad única obligatoria, una infraestructura de trazabilidad universal ni un mecanismo centralizado que permita vigilar de forma sistemática la actividad de una persona en distintos ámbitos de su vida.

Por ello, toda arquitectura jurídica o tecnológica inspirada en la Soberanía Digital Individual debe incorporar mecanismos de control, revisión, impugnación, trazabilidad y reparación. La persona debe poder conocer cuándo su identidad o sus atributos han sido accedidos, por quién, con qué finalidad y bajo qué base jurídica, salvo en supuestos excepcionales legalmente justificados y sometidos a supervisión adecuada.

La finalidad de este manifiesto no es debilitar el Estado de Derecho, sino impedir que la sociedad digital confunda responsabilidad con exposición total. La libertad digital exige que existan mecanismos legítimos y proporcionados para atribuir responsabilidad, sin imponer una identificación permanente por defecto.

VII. El valor económico de la identidad digital y la participación justa en sus beneficios

La economía digital contemporánea se sustenta sobre un flujo continuo de información generado por miles de millones de personas a través de sus actividades cotidianas. Cada interacción, búsqueda, desplazamiento, compra, publicación, conexión o patrón de comportamiento puede contribuir a conjuntos de datos que alimentan sistemas de inteligencia artificial, plataformas digitales, mercados publicitarios, infraestructuras financieras y modelos predictivos de enorme valor económico.

Sin embargo, existe una profunda asimetría entre quienes generan continuamente información y quienes poseen la capacidad tecnológica, jurídica, económica y organizativa para transformarla en valor.

Los individuos contribuyen de forma constante a los ecosistemas digitales que permiten la creación de riqueza, pero los beneficios derivados de la recopilación, análisis, inferencia, agregación, entrenamiento, perfilado y monetización de dicha información se concentran principalmente en las organizaciones que controlan las infraestructuras y sistemas de explotación de datos.

Esta situación plantea una cuestión fundamental de justicia, autonomía y distribución del poder en la sociedad digital. Si la identidad digital constituye una extensión de la persona y si la información vinculada a dicha identidad contribuye de forma sistemática a la generación de valor económico, no resulta legítimo que los individuos permanezcan estructuralmente excluidos de toda capacidad de decisión, control, negociación o participación respecto de los beneficios obtenidos a partir de su información.

No obstante, la participación en el valor generado por los datos personales no debe entenderse como una simple compraventa de privacidad ni como una reducción de la dignidad humana a mercancía. La persona no debe verse obligada a vender exposición, intimidad o vulnerabilidad para participar en la economía digital. Una sociedad verdaderamente libre no debe construir mercados donde quienes tienen menos recursos se vean empujados a ceder más información personal a cambio de ventajas económicas inmediatas.

Por ello, el reconocimiento del valor económico de la identidad digital debe formularse desde la justicia, la gobernanza y la responsabilidad, no desde una mercantilización absoluta de la persona. La cuestión no consiste en afirmar que todo dato personal tenga un precio individual directamente calculable ni en atribuir una propiedad patrimonial absoluta sobre toda información que involucre a una persona. Muchos datos son relacionales, inferidos, agregados, derivados o producidos dentro de sistemas complejos.

La cuestión central es otra: cuando una organización obtiene valor económico, estratégico, predictivo o comercial de manera sistemática a partir de información vinculada a personas, deben existir mecanismos que garanticen transparencia, control, equidad, rendición de cuentas y, cuando corresponda, formas justas de participación, compensación o beneficio equivalente.

La participación justa en el valor de los datos personales debe ser especialmente cautelosa cuando afecte a personas en situación de vulnerabilidad, menores, trabajadores, consumidores dependientes, migrantes, personas con discapacidad, pacientes, usuarios de servicios esenciales o colectivos expuestos a formas intensas de perfilado. En tales contextos, la capacidad formal de aceptar un intercambio económico no garantiza necesariamente una decisión libre, informada o justa.

La Soberanía Digital Individual exige reconocer simultáneamente dos ideas. La primera es que la información personal no puede ser tratada como una materia prima gratuita, ilimitada y permanentemente disponible para la extracción económica. La segunda es que la dignidad, la privacidad y la identidad de la persona no deben reducirse a activos comerciados sujetos únicamente a precio, contrato y consentimiento formal.

El desafío de la sociedad digital no consiste simplemente en pagar por los datos, sino en rediseñar la distribución del poder, del control y de los beneficios derivados de la explotación sistemática de la información personal.

VIII. Deberes de las organizaciones, garantías y remedios

El reconocimiento de la Soberanía Digital Individual carecería de eficacia si no se tradujera en deberes concretos para las organizaciones que solicitan, recopilan, almacenan, procesan, analizan, infieren, comparten o monetizan información personal. Los derechos digitales no pueden depender únicamente de declaraciones abstractas ni de la capacidad individual de cada persona para enfrentarse a sistemas jurídicos, técnicos y económicos profundamente asimétricos.

Toda organización que intervenga en el tratamiento de información vinculada a una persona debe asumir, como mínimo, un deber de justificación, minimización, seguridad, trazabilidad y rendición de cuentas. Ningún dato personal debería solicitarse, conservarse o tratarse sin una finalidad específica, legítima, comprensible y proporcional. Cuando una interacción digital pueda realizarse mediante la verificación de un atributo concreto, no debería exigirse la exposición completa de la identidad.

La custodia de datos personales debe implicar un estándar de protección proporcional a la sensibilidad, volumen, finalidad y riesgo de la información tratada. Cuanto mayor sea el riesgo que la recopilación de datos genera para la persona, mayor debe ser la responsabilidad de quien decide recopilarlos, conservarlos o explotarlos.

Las organizaciones que utilicen sistemas automatizados, modelos de inteligencia artificial, mecanismos de perfilado o decisiones algorítmicas que puedan afectar significativamente a una persona deben asumir deberes reforzados de transparencia, explicación, revisión e impugnación.

La persona no debe quedar reducida a un objeto pasivo de clasificación, predicción o decisión automatizada sin posibilidad efectiva de comprender, cuestionar o corregir sus efectos.

También debe reconocerse un deber de revocabilidad efectiva. Cuando una persona haya autorizado el uso de determinados datos, atributos o credenciales, debe poder retirar dicha autorización de manera sencilla, comprensible y proporcionada, sin obstáculos artificiales, penalizaciones abusivas ni diseños destinados a dificultar el ejercicio de sus derechos.

La Soberanía Digital Individual exige además un deber de no explotación de asimetrías informacionales. Las organizaciones no deben aprovechar la complejidad técnica, la dependencia del servicio, la falta de alternativas reales o la vulnerabilidad del usuario para obtener consentimientos formalmente válidos pero materialmente desequilibrados.

Cuando estos deberes sean vulnerados, deben existir remedios efectivos. Entre ellos pueden incluirse, según la naturaleza y gravedad del caso, información clara sobre la vulneración, rectificación, supresión, limitación del tratamiento, revocación, suspensión de usos abusivos, portabilidad, revisión humana, auditoría independiente, compensación proporcional y sanciones cuando exista negligencia, abuso o incumplimiento grave.

La reparación no debe limitarse a multas administrativas. Cuando una vulneración de la identidad digital, la privacidad, la custodia de datos o la exposición mínima cause perjuicios reales o riesgos significativos para una persona, el sistema debe ofrecer vías accesibles, rápidas y efectivas de reclamación.

Asimismo, la protección de la Soberanía Digital Individual requiere garantías institucionales: autoridades competentes, mecanismos de supervisión, procedimientos de reclamación, auditorías, estándares técnicos, obligaciones de documentación y formas de control independiente capaces de impedir que estos principios queden reducidos a compromisos voluntarios sin consecuencias.

La legitimidad de una organización en la sociedad digital no debe medirse únicamente por su capacidad de innovar, escalar o generar valor económico, sino también por su capacidad de respetar la identidad, la autonomía, la privacidad y la dignidad de las personas cuyos datos hacen posible su actividad.

IX. La dimensión relacional y colectiva de la privacidad digital

La Soberanía Digital Individual parte de la persona como centro de protección, pero no debe entenderse como una teoría aislada o puramente individualista. En la sociedad digital, la información personal rara vez existe de manera completamente separada. Muchos datos son relacionales, compartidos, inferidos o derivados de interacciones en las que intervienen varias personas, comunidades, organizaciones o contextos sociales.

Una conversación, una fotografía, una ubicación compartida, una agenda de contactos, una relación profesional, un historial de comunicaciones o un conjunto de datos genéticos pueden revelar información no solo sobre una persona, sino también sobre terceros. Del mismo modo, los perfiles algorítmicos contruidos a partir de ciertos individuos pueden utilizarse para inferir características, riesgos o comportamientos de otras personas o grupos similares.

Por ello, el control individual sobre los datos personales debe coexistir con deberes de respeto hacia la privacidad, la dignidad y los derechos de otras personas. Nadie debería poder invocar su propia soberanía digital para exponer injustificadamente información ajena, revelar datos compartidos sin consideración a terceros o facilitar formas de perfilado colectivo que generen discriminación, vigilancia o exclusión. La soberanía digital debe reconocer también una dimensión colectiva. Determinadas prácticas de recopilación, inferencia, perfilado o monetización de datos pueden afectar no solo a individuos concretos, sino también a grupos, comunidades o categorías de personas.

En ámbitos como inteligencia artificial, publicidad segmentada, scoring, vigilancia predictiva, selección laboral, crédito, seguros, salud, educación, migración o servicios esenciales, las decisiones basadas en datos pueden reproducir desigualdades, amplificar sesgos o generar consecuencias significativas para personas que ni siquiera conocen el origen de las inferencias que les afectan.

Por ello, la Soberanía Digital Individual debe complementarse con principios de responsabilidad relacional y justicia colectiva. Las organizaciones no solo deben responder por el tratamiento de datos identificables de una persona concreta, sino también por los efectos agregados, inferenciales o colectivos que sus sistemas puedan producir sobre grupos de personas.

El reconocimiento de esta dimensión no debilita la centralidad de la persona. La fortalece. Una teoría seria de la identidad digital debe proteger al individuo sin ignorar que los datos circulan, se combinan, se interpretan y producen efectos dentro de sistemas sociales complejos.

X. Principios de la Soberanía Digital Individual

La Soberanía Digital Individual se fundamenta en un conjunto de principios rectores destinados a orientar el diseño de tecnologías, marcos regulatorios, infraestructuras de identidad, modelos de gobernanza y prácticas organizacionales en la sociedad digital. Su finalidad común es preservar la dignidad, la autonomía, la libertad y la capacidad efectiva de decisión de la persona frente al poder informacional.

1. Principio de Centralidad de la Persona

Toda arquitectura digital que recopile, procese, infiera, comparta o monetice información personal debe partir de la premisa de que la persona no es una mera fuente de datos, un perfil explotable ni un objeto pasivo de clasificación algorítmica.

2. Principio de Soberanía de la Identidad

Toda persona debe conservar una esfera primaria de decisión sobre los atributos, credenciales, identificadores, representaciones y elementos que conforman o afectan a su identidad digital.

3. Principio de Control Efectivo

Toda persona debe disponer de medios jurídicos, técnicos y prácticos para conocer, autorizar, limitar, revocar, trasladar, corregir, impugnar o impedir determinados usos de los datos, atributos y credenciales que afectan a su identidad digital.

4. Principio de Autodeterminación Informativa Reforzada

Toda persona debe poder conocer, comprender y decidir cómo se utiliza la información que la describe, especialmente cuando sea empleada para perfilarla, clasificarla, influir sobre ella o adoptar decisiones que afecten a sus derechos, oportunidades o reputación.

5. Principio de Exposición Mínima de Identidad

Ninguna persona debe verse obligada a revelar más información sobre su identidad de la estrictamente necesaria para una interacción digital legítima. Siempre que sea posible acreditar un atributo específico sin exponer la identidad completa, deberá preferirse la solución menos intrusiva.

6. Principio de Proporcionalidad y Finalidad Específica

Toda recopilación, acceso, conservación, inferencia, comunicación o explotación de información personal debe responder a una finalidad legítima, específica, comprensible y proporcionada.

7. Principio de Transparencia, Explicabilidad y Trazabilidad

Los sistemas que recopilen, procesen, infieran o utilicen información personal deben operar de manera comprensible, verificable y auditable. La persona debe poder conocer qué información se utiliza, con qué finalidad, por quién, durante cuánto tiempo y con qué efectos relevantes.

8. Principio de Responsabilidad y Custodia

Toda organización que solicite, almacene, procese, infiera, comparta o monetice información personal asume un deber de custodia proporcional a la sensibilidad, volumen, finalidad y riesgo de los datos tratados.

9. Principio de Revocabilidad y Reparación Efectiva

Toda autorización relativa al uso de datos, atributos o credenciales personales debe poder ser revocada de forma sencilla y efectiva, salvo base jurídica legítima en contrario. Toda vulneración significativa debe dar lugar a remedios accesibles, proporcionales y eficaces.

10. Principio de Portabilidad e Interoperabilidad

Toda persona debe poder trasladar sus atributos, credenciales e información personal entre sistemas, plataformas, organizaciones y jurisdicciones sin perder control sobre ellos ni quedar sometida a dependencias tecnológicas artificiales.

11. Principio de No Centralización Obligatoria

La Soberanía Digital Individual no debe derivar en una identidad digital única, obligatoria, centralizada o universalmente trazable. Los sistemas de identidad deben permitir separación de contextos, pseudonimato legítimo y protección frente a la vigilancia generalizada.

12. Principio de Inclusión, Accesibilidad y Usabilidad

La Soberanía Digital Individual solo será real si puede ser ejercida por cualquier persona, con independencia de su edad, nivel educativo, condición económica, discapacidad, idioma, situación migratoria, alfabetización digital o acceso a tecnología avanzada.

13. Principio de Participación Justa en el Valor de los Datos

Cuando la información personal genere valor económico, estratégico, predictivo o comercial de manera sistemática, deben existir mecanismos justos de transparencia, control, gobernanza, compensación, participación o beneficio equivalente.

Toda tecnología, regulación, política pública, infraestructura de identidad digital o modelo de negocio basado en datos personales debería evaluarse a la luz de estos principios.

XI. Hacia una Carta de Derechos para la Soberanía Digital Individual

La transformación tecnológica ha alterado profundamente la forma en que las personas se identifican, se relacionan, trabajan, acceden a servicios, participan en la vida pública y son evaluadas por instituciones públicas y privadas. Del mismo modo que las revoluciones políticas, industriales y constitucionales impulsaron nuevas generaciones de derechos, la revolución digital exige actualizar el marco jurídico destinado a proteger la libertad, la dignidad y la autonomía humana.

La presente propuesta sostiene que toda persona debería ser reconocida como titular, al menos, de los siguientes derechos digitales fundamentales. Estos derechos no deben entenderse como absolutos ni aislados del resto del orden jurídico. Su ejercicio debe articularse conforme a la ley, la protección de terceros, la seguridad jurídica, el interés público legítimo, la proporcionalidad, la finalidad específica, la minimización y el debido proceso.

1. Derecho a la Identidad Digital Soberana

Toda persona debe conservar una esfera primaria de decisión sobre los atributos, credenciales, identificadores, representaciones, reputación, datos y elementos que conforman o afectan a su identidad digital.

2. Derecho a la Privacidad Efectiva

Toda persona debe poder participar en la sociedad digital sin quedar sometida a vigilancia permanente, recopilación desproporcionada de información, exposición innecesaria de identidad o tratamientos incompatibles con su dignidad, autonomía y derechos fundamentales.

3. Derecho a la Identificación Verificable con Exposición Mínima

Toda persona debe poder acreditar atributos, derechos, condiciones o credenciales necesarias para una interacción digital legítima sin revelar más información personal de la estrictamente necesaria.

4. Derecho a la Autodeterminación Informativa Reforzada

Toda persona debe poder conocer, comprender, decidir, limitar y revocar el uso de la información que la describe o afecta, especialmente cuando sea utilizada para clasificarla, perfilarla, influir sobre ella o adoptar decisiones relevantes.

5. Derecho a la Protección frente a Inferencias y Perfilado Abusivo

Toda persona debe estar protegida frente a inferencias, perfiles, predicciones, valoraciones o clasificaciones opacas, desproporcionadas, discriminatorias, incompatibles con la finalidad original o capaces de producir efectos significativos sobre su vida, derechos u oportunidades.

6. Derecho a la Transparencia Algorítmica y a la Explicación Significativa

Toda persona debe poder conocer cuándo una decisión relevante que le afecta ha sido adoptada, influenciada o condicionada por sistemas automatizados, modelos algorítmicos o sistemas de inteligencia artificial, y recibir información comprensible sobre su lógica general, finalidad, datos utilizados, efectos y vías de impugnación.

7. Derecho a la Revisión Humana e Impugnación de Decisiones Automatizadas

Toda persona debe poder solicitar revisión humana, formular objeciones, aportar contexto, corregir información y obtener una respuesta efectiva cuando una decisión automatizada o algorítmicamente asistida produzca efectos significativos sobre sus derechos, oportunidades, reputación o condiciones de vida.

8. Derecho a la Portabilidad Universal de Identidad, Datos y Atributos

Toda persona debe poder trasladar sus credenciales, atributos e información personal entre plataformas, organizaciones, servicios y jurisdicciones sin perder control sobre ellos ni quedar sometida a dependencias tecnológicas artificiales.

9. Derecho a la Revocación Efectiva

Toda persona debe poder retirar autorizaciones previamente concedidas para el uso de sus datos, atributos o credenciales de forma sencilla, comprensible y efectiva, salvo cuando exista una base jurídica legítima que justifique su conservación o tratamiento.

10. Derecho a la Custodia Responsable de los Datos Personales

Toda persona tiene derecho a exigir que las organizaciones que soliciten, almacenen, procesen, infieran, compartan o monetizen información personal adopten medidas proporcionales a la sensibilidad, volumen, finalidad y riesgo de los datos tratados.

11. Derecho a la Trazabilidad y Rendición de Cuentas

Toda persona debe poder conocer, en términos claros y accesibles, qué información se conserva sobre ella, quién ha accedido a ella, con qué finalidad, durante cuánto tiempo, bajo qué base jurídica y con qué terceros se ha compartido, salvo excepciones legalmente justificadas y supervisadas.

12. Derecho a la Reparación Efectiva

Toda persona debe disponer de vías accesibles, rápidas y eficaces para reclamar frente a vulneraciones de su identidad digital, privacidad, exposición mínima, autodeterminación informativa, custodia de datos o derechos frente a sistemas automatizados.

13. Derecho a no ser Sometido a una Identidad Digital Única Obligatoria

Toda persona debe estar protegida frente a sistemas que impongan una identidad digital única, centralizada, universalmente trazable o necesaria para toda forma de participación social, económica o política.

14. Derecho a la Inclusión, Accesibilidad y Usabilidad

Toda persona debe poder ejercer sus derechos digitales con independencia de su edad, idioma, nivel educativo, condición económica, discapacidad, situación migratoria, alfabetización digital o acceso a tecnología avanzada.

15. Derecho a no ser Explotado mediante Asimetrías Informacionales

Toda persona debe estar protegida frente a prácticas que aprovechen la complejidad técnica, la dependencia del servicio, la falta de alternativas reales, la opacidad contractual, los diseños manipulativos o la vulnerabilidad del usuario para obtener consentimientos formalmente válidos pero materialmente desequilibrados.

16. Derecho a Participar Justamente en el Valor Generado por los Datos Personales

Cuando la información personal genere valor económico, estratégico, predictivo o comercial de forma sistemática y previsible, las personas deben disponer de mecanismos justos de transparencia, control, gobernanza, compensación, participación o beneficio equivalente.

Estos derechos no pretenden sustituir los derechos fundamentales reconocidos por los ordenamientos jurídicos contemporáneos. Su finalidad consiste en extender, profundizar y adaptar dichos derechos a una realidad en la que la identidad digital, los datos personales, los atributos verificables, los sistemas algorítmicos y la economía de la información se han convertido en elementos esenciales para el ejercicio efectivo de la libertad humana.

La Carta de Derechos para la Soberanía Digital Individual no debe concebirse como un catálogo cerrado, sino como una base doctrinal para la evolución jurídica, técnica e institucional de los derechos de la persona en la sociedad digital.

Conclusión

La cuestión fundamental de nuestro tiempo no es únicamente quién posee la tecnología, sino quién ejerce el poder derivado de la información. La revolución digital ha dado origen a una forma de poder particularmente profunda: la capacidad de recopilar, conservar, analizar, inferir, perfilar, predecir y explotar información sobre la vida de millones de personas.

En este contexto, la identidad digital se ha convertido en una extensión de la persona. Los datos personales, los atributos verificables, las credenciales, las interacciones, la reputación, los metadatos, los perfiles y las inferencias algorítmicas pueden condicionar la forma en que una persona es reconocida, evaluada, clasificada, aceptada, excluida, vigilada o influida por sistemas públicos y privados.

La libertad en la era digital no depende únicamente del acceso a la tecnología. Depende de la capacidad real de cada persona para conservar control sobre la identidad que la representa, sobre la información que la describe y sobre los sistemas que pueden afectar a sus derechos, oportunidades y condiciones de vida.

La sociedad digital no será verdaderamente libre mientras la participación en la vida económica, social, cultural y política requiera una exposición permanente e innecesaria de la identidad. Tampoco será plenamente justa mientras quienes generan el valor que alimenta la economía de los datos permanezcan excluidos de toda capacidad de decisión, control, gobernanza, reparación o participación respecto de los beneficios derivados de dicha explotación.

La defensa de la soberanía digital individual no exige aislar al individuo del Derecho ni negar fines legítimos de identificación, seguridad, prevención del fraude o protección de terceros. Exige que la identificación no se convierta en exposición permanente; que la responsabilidad no derive en vigilancia generalizada; que la innovación no justifique la extracción ilimitada de datos; y que el consentimiento formal no oculte relaciones estructuralmente desequilibradas.

La próxima evolución de los derechos fundamentales no debe limitarse a proteger datos como objetos aislados. Debe proteger a las personas frente a las formas de poder que se ejercen a través de los datos. Debe reconocer la identidad digital como parte de la esfera de autonomía individual, exigir custodia responsable, garantizar exposición mínima, someter los sistemas automatizados a rendición de cuentas y ofrecer remedios efectivos cuando la identidad digital sea vulnerada.

La defensa de la privacidad es, en última instancia, una defensa de la libertad humana. La defensa de la identidad digital es una defensa de la dignidad humana. La defensa de la soberanía digital individual es una defensa de la capacidad de cada persona para seguir siendo dueña de sí misma en la era de los datos, sin quedar reducida a perfil, producto, predicción o recurso explotable.

La historia de los derechos fundamentales ha sido la historia de la expansión progresiva de la libertad frente a nuevas formas de poder. La soberanía digital individual constituye una propuesta para continuar esa historia en la era de la inteligencia artificial, la economía de los datos y la identidad digital.

Sobre este documento

El presente manifiesto constituye un documento fundacional para el desarrollo de una teoría jurídica, tecnológica, social y filosófica de la Soberanía Digital Individual. Su finalidad no es ofrecer una regulación definitiva, una propuesta legislativa cerrada ni una solución técnica única, sino establecer los principios, conceptos, derechos, deberes y garantías que deberían orientar la protección de la persona en la era de la identidad digital, la inteligencia artificial y la economía de los datos.

La Soberanía Digital Individual se formula aquí como una categoría doctrinal destinada a ampliar y profundizar los marcos existentes de protección de datos, privacidad, identidad, transparencia, responsabilidad tecnológica y derechos fundamentales. No pretende sustituir dichos marcos, sino señalar sus límites estructurales y proponer una evolución hacia un modelo en el que la persona ocupe el centro del ecosistema digital.

Este documento debe entenderse como una base intelectual abierta al desarrollo, la crítica y la mejora. Su desarrollo completo requerirá una obra posterior en la que se analicen sus fundamentos históricos, filosóficos, jurídicos, técnicos e institucionales, así como sus riesgos, límites, objeciones, mecanismos de implementación y formas de tutela, reparación y gobernanza.

Londres, junio de 2026

JC Roura

Autor de la Fundación de los Principios de la Soberanía
Digital Individual

Versión fundacional 2.0