La protección de los derechos digitales: Una cuestión identitaria europea

The protection of digital rights: A European identity issue

Antonio Lazari
Profesor Titular de Derecho Internacional Público y Relaciones Internacionales
Universidad Pablo de Olavide

Recibido: 02.11.2023 / Aceptado: 10.01.2024
DOI: 10.20318/cdt.2024.8425

Resumen: El almacenamiento de datos personales no pone en peligro solo el denominado derecho individual a la privacidad, sino que afecta a un espectro social y político más amplio, relacionado con la salud de la vida democrática. Frente a la visión soberanista china y a la idea segmentada y mercantilista estadounidense de seguridad digital, la Unión Europea va proponiendo en esta última década una concepción estrechamente ligada a la jurisprudencia del TJUE en torno a la esencia del derecho fundamental a la identidad digital. Este estudio aborda los aspectos esenciales de la protección de datos en la nueva globalización, diseñando un cuadro estratégico donde tanto dentro del territorio de la Unión como fuera de ello las instituciones comunitarias han de dialogar necesariamente sobre el alcance de los derechos fundamentales.

Palabras clave: Derechos digitales, Derecho a la privacidad, Tribunal de Justicia de la Unión Europea, Identidad de la Unión.

Abstract: The storage of personal data does not endanger only the so-called individual right to privacy, but covers a wider social and political spectrum, related to the health of democratic life. Faced with the Chinese sovereignty vision and the segmented and mercantilist American idea of digital security, the European Union has been proposing in the last decade a conception closely linked to the jurisprudence of the CJEU around the essence of the fundamental right to digital identity. The primary issues that arise when studying cybersecurity must be addressed from a broader, (arguably, inevitably existential) perspective, underlining that cybersecurity refers to public goods and private property and that the organizations and bodies designated to protect them must be subject to the scrutiny of constitutionally relevant norms, lest they become true CyberLeviathans. This study addresses the essential aspects of data protection and citizens' rights in the new globalization era, designing a strategic framework where both within the territory of the Union and outside it the Community institutions must necessarily dialogue on the scope of fundamental rights in the face of the requirements of national security.

Keywords: Digital Rights, European Union Law, Court of Justice of European Union, European Union Identity.

I. Prólogo: los términos de la cuestión

1. El anunciado "tsunami digital" es el resultado no solo de las oportunidades proporcionadas por la tecnología, sino también del hecho de que los datos personales son arrastrados a la órbita omnívora de las empresas y organizaciones de seguridad. Se ha constituido un nuevo espacio difícil de definir según los marcos tradicionales de referencia público/privado, nacional/internacional, en el cual no se ven afectados solo los aspectos individuales tradicionales de la privacidad personal. El almacenamiento de datos personales cubre un espectro social y político más amplio, relacionado con la salud de la vida democrática. Frente a la visión soberanista china y a la idea segmentada y mercantilista estadounidense de seguridad digital, la Unión Europea va proponiendo en esta última década una concepción estrechamente ligada a la jurisprudencia del TJUE sobre la esencia del derecho fundamental a la identidad digital. En consecuencia, las cuestiones primordiales que surgen al estudiar la ciberseguridad deben abordarse de manera compleja, comparativa e inevitablemente axiológica, subrayando que la ciberseguridad se refiere a bienes públicos y propiedades privadas y que las organizaciones y organismos designados para protegerlos deben estar sujetos al escrutinio de normas constitucionalmente relevantes, para que no se conviertan en verdaderos *CyberLeviathans*[1]. Este estudio aborda los aspectos comparativos y europeos de la protección de datos y derechos de los ciudadanos en la nueva globalización. Se divide en dos segmentos especulares: el primero abordará el heterogéneo panorama regulatorio estatal sobre la protección de la privacidad desde una perspectiva comparativa y empírico-descriptiva. El segundo fragmento, tras constatar la reconocida imposibilidad de abordar la cuestión intrínsecamente transnacional de la ciberseguridad a través de disciplinas exclusivamente nacionales, profundizará en el estudio de la disciplina regulatoria (y la *gobernanza* subyacente) perseguida por la Unión Europea y el Consejo de Europa; segmento que representa el núcleo esencial de este trabajo[2].

II. Los principales modelos normativos fuera del territorio de la Unión Europea

1. El panorama normativo en los Estados Unidos de América

2. La visión subyacente a la protección de datos está potentemente marcada por la jurisprudencia y doctrina estadounidense de finales del siglo XIX expresada por Warren y Brandeis[3]. La privacidad, en esencia, consistía en el "*derecho a ser dejado en paz*"[4]. El propio Brandeis, esta vez como juez, comentó en la famosa *dissenting opinion* en el caso Olmstead v. United States[5] que "*personal privacy matters were more relevant to constitutional law*", llegando a afirmar que "*the government was identified as a potential privacy invader"*[6]. Argumenta que "*discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet*".[7] A pesar de las aspiraciones regulatorias de Brandeis, ni el "formante"[8]

[1] Sobre la posibilidad de que resurjan nuevos Leviatanes, véase la reciente obra de J. Gray, *The New Leviathans: Thoughts After Liberalism*, Penguin Books Ltd., 2023.

[2] Para una profundización sobre estos temas se permita remitir a trabajos previos A. Lazari*, De ciberataques y ciberleviatanes: cartografía de la "governance" en el prisma del derecho europeo y comparado*, en *Ciberataques y ciberseguridad en la escena internacional*, coord. por L. Millán Moro, 2019, pp. 175-204; IDEM, "La protezione reticolare europea dei diritti digitali nello scenario internazionale" (Iª Parte), *Studi sull'integrazione europea*, XVII (2022), pp. 229-255; y IDEM, "La protezione reticolare europea dei diritti digitali nello scenario internazionale" (IIª Parte), *Studi sull'integrazione europea*, XVII, 2022, pp. 453-486.

[3] D. W. Samuel y L. D. Brandeis, "The Right to Privacy"*, Harvard Law Review* 4, 1890, p. 193.

[4] D. W. Samuel y L. D. Brandeis, *op. cit.*, p. 193.

[5] Olmstead v. United States, 277 U.S. 438 (1928).

[6] Olmstead v. United States, 277 U.S. 438 (1928), p. 93.

[7] *Ibídem*, p.94.

[8] El formante jurídico es una figura del derecho comparado, acuñada por Rodolfo Sacco utilizando terminología lingüística, con el fin de analizar los sistemas nacionales mediante la descomposición de un modelo nacional en sus componentes. Véase R. Sacco, "Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II), *The American Journal of Comparative Law,* Vol. 39, No. 1 (Winter, 1991), pp. 1-34.

judicial, ni la legislación estadounidense han abordado el tema de la protección de datos de manera integral y constitucional[9].

3. En las últimas dos décadas, el marco regulatorio de los Estados Unidos no ha contrarrestado el aumento de los poderes privados de las corporaciones digitales, sino que ha defendido firmemente el concepto de libertad consagrada en el álveo de la Primera Enmienda, como se reiteró recientemente en *Packingham v. Carolina del Norte*[10].

4. La Constitución de los Estados Unidos no menciona explícitamente el término "privacidad" o "protección de datos". De hecho, no existe un derecho individual explícito a la privacidad en el sistema estadounidense, ni existe una legislación general de protección de la privacidad hasta la fecha[11]. Emerge un mosaico legal de protecciones de la privacidad producido por múltiples fuentes, como la Primera Enmienda, la Cuarta Enmienda, la Quinta Enmienda y la Decimocuarta Enmienda a la Constitución y la correspondiente jurisprudencia constitucional. Como resultado, el derecho de Estados Unidos ha centrado su atención principalmente en la privacidad frente a la acción del gobierno y en la idea de que las personas tienen derecho a la privacidad en virtud de la Cuarta Enmienda[12].

5. Desde una perspectiva comparativa, Whitman argumenta significativamente que la mayor amenaza histórica a la privacidad no han sido las empresas privadas, sino el gobierno, ya sea federal o estatal[13]. El enfoque liberal de los Estados Unidos también podría considerarse una expresión del constitucionalismo digital que denota el diferente sesgo cultural del derecho constitucional de los Estados Unidos, que considera a las plataformas digitales como un "facilitador" de la libertad y la democracia, en lugar de verlas en términos de amenaza para esos valores. Esta concepción ha sido progresivamente abandonada en la vertiente oriental del Atlántico, donde el *humus* constitucional diferente basado en la dignidad humana ha allanado el camino hacia una nueva fase constitucional, como veremos en la segunda parte.

6. A finales de 2015, después de años de largas negociaciones parlamentarias, el Congreso aprobó una legislación para permitir a las empresas compartir voluntariamente información sobre amenazas de ciberseguridad contra el gobierno federal y otras empresas: la ***Ley de Ciberseguridad***[14]. A pesar de los requisitos directos para que las entidades privadas tomen medidas para eliminar la información personal antes de compartir indicadores de amenazas cibernéticas, los aspectos críticos de esta ley son evidentes con respecto a las empresas que potencialmente violan los derechos de privacidad de las personas, sin contribuir activamente a su ciberseguridad. Del mismo modo, al no equilibrar el eje de la disciplina de ciberseguridad con la protección de la privacidad de los ciudadanos, los estándares estadounidenses inicialmente no consideran la ciberseguridad como una cuestión de seguridad nacional. Un enfoque más amplio basado en el interés nacional requerirá una cooperación más estrecha entre los Estados Unidos y otras naciones; estrategia que aún no había surgido en la adopción de la Ley de la Agencia de Seguridad de Ciberseguridad e Infraestructura de noviembre de 2018[15]. Solo a partir de 2018 la dinámica entre el formante judicial y legislativo ha contribuido a aclarar parte del enfoque de los Estados Unidos sobre la protección de datos personales, aunque aún persisten profundas ambigüedades. Estos desarrollos in-

[9] Según J. Fischer, "The Challenges and Opportunities for a US Federal Privacy Law", en F. Fabbrini, E. Celeste y J. Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, 2021, p. 76: "*The current approach to privacy in the US can be summed up nicely in one word: fragmented*".

[10] Packingham v. Carolina del Norte (2017) 582 Estados Unidos _(2017).

[11] La American Data Privacy and Protection Act ("ADPPA") introducida en 2022 fue el intento más avanzado de presentar un proyecto de ley federal de privacidad integral. Sin embargo, el proyecto de ley no proliferó.

[12] Roe contra Wade, 410 US 113 (1973).

[13] Whitman, James Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal*, 2017, 113, pp. 1211-12; J.L. Fischer, *op. cit.*, pp. 86-90.

[14] Cybersecurity Act H. R. 2029-694.

[15] H.R.3359 - Cybersecurity and Infrastructure Security Agency Act de 2018.

cluyen el caso de Microsoft en el formante judicial, y la ***Clarifying Lawful Overseas Use of Data Act*** (conocida como la Ley CLOUD) en la vertiente legislativa[16].

7. Durante mucho tiempo se ha verificado una clara falta de atención a la recopilación de inteligencia por parte de los actores no gubernamentales[17]: "*there have already been attempts to use class action lawsuits as a mechanism to enforce privacy*"[18]. Las demandas colectivas presentadas contra *Facebook*[19] *Yahoo!* [20] *, PayPal*[21]*, Google Cheggy*[22], y en particular, la decisión de enero de 2019 *In re Equifax Securities Litigation*[23] constituyen todos síntomas claros de una reciente tendencia a la protección horizontal *inter privatos de* los ciberataques, como de hecho demuestra el caso inglés *Google v. Lloyd* en el ámbito de las acciones colectivas[24]. Los rasgos idiosincrásicos del sistema normativo estadounidense se hallan, al fin y al cabo, en el territorio privatista de la protección del derecho a la privacidad y en el derecho inicial a la privacidad, entendido como situación jurídica a "ser dejado en paz".

8. Cuando vuelve a asomarse esporádicamente la necesidad "vertical" de índole gubernamental, el insuficiente equilibrio constitucional, emerge una vez más, principalmente en la jurisprudencia de la Corte Suprema[25]. En la sentencia de 2018 *Carpenter vs. Estados Unidos*[26], la coincidencia inicial, o al menos la convergencia, entre las demandas del gobierno federal y los intereses de las empresas se resquebrajó, dejando espacio para un progresivo conflicto de intereses entre las multinacionales estadounidenses y las reclamaciones del gobierno de los Estados Unidos en el enjuiciamiento de delitos graves. Vuelve a aflorar la preocupación brandeisiana de tutelar el derecho "dejado en paz" en la infoesfera. En una decisión problemática redactada por el juez Roberts el tribunal sostuvo que el gobierno había violado la Cuarta Enmienda de la Constitución de los Estados Unidos al acceder a documentos que contenían las ubicaciones físicas de los teléfonos celulares sin una orden judicial fuera del territorio de los Estados Unidos[27] "«[T]he privacies of life»" must be secure "against «arbitrary power»". En virtud de la aprobación de la *Ley CLOUD*, la Corte Suprema anuló el caso en abril de 2018, remitiéndolo al tribunal inferior para su resolución, ya que el gobierno había emitido una nueva orden[28]. Las solicitudes destinadas a la protección de datos personales en términos de seguridad nacional han surgido sólo en los últimos tiempos y, como tendremos modo de analizar, sin una ponderación jurisprudencial del derecho a la identidad digital.

9. Sin embargo, la cuestión inherente a la regulación del flujo de datos personales adquiere inevitablemente una dimensión transfronteriza, que *ad extra* implica su soberanía cibernética o cibersoberanía.

---

[16] Clarifying Lawful Overseas Use of Data Act (Ley CLOUD), Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018) (codificado en secciones dispersas de 18 U.S.C.) [en adelante Ley CLOUD]. Un lugar privilegiado en este análisis está reservado para la Ley de Privacidad de California de 2018. El Parlamento de California ha aprobado la Ley de Privacidad del Consumidor de California, que la mayoría de la doctrina más atenta a estos temas considera la base de una posible ley federal estadounidense inspirada en el modelo europeo GDPR. La medida legislativa, que entró en vigor en 2020, puede considerarse la disciplina jurídica más garante de los derechos individuales en los Estados Unidos y debe leerse en un contexto más amplio donde surge la intención de la Corte Suprema también en la sentencia Carpenter de 2018 de limitar las intervenciones de las autoridades estatales en la esfera privada de los ciudadanos (en este caso, estas acciones estaban relacionadas con las grabaciones de la ubicación de dispositivos de telefonía móvil). La American Data Privacy and Protection Act ("ADPPA").

[17] J.Q. Whitman, *op. cit.*, pp. 1211-1212.

[18] J.L. Fischer, *op. cit.*, p. 76.

[19] Adkins v Facebook, Inc, No 3:18-cv-05982, 2019 WL 7212315 (ND Cal, 26 de November de 2019)

[20] In re Yahoo! Inc. Shareholder Litig., Caso n. 17-CV-307054, (Cal. Supp. Ct 4 January 2019).

[21] PayPal Holdings, Inc., n. 3:17-cv-06956 (N.D. Cal.).

[22] Frank v. Gaos, 586 U.S. (2019).

[23] In re Heartland Payment system. Second. Litig., No 09-1043 (D. N.J. 7 December 2009).

[24] In re Equifax, Inc. Secur. Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 28 January 2019).

[25] R. Moshell, "And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection", *Texas Technology Law Review*, 2005, p. 362: "*Supreme Court decisions reiterate that most US jurisprudence related to privacy involves protections against the state, and not in the private sector. The current approach to privacy in the private sector is fragmented and complex, often relying on industries to self-regulate*".

[26] United States, n. 16-402, 585 U.S. (2018).

[27] Carpenter v. United States, 138 S Ct 2206 (2018).

[28] United States v. Microsoft, No. 17-2, 3 (2018).

La mentada *Ley CLOUD* requiere que los proveedores de servicios de comunicaciones electrónicas proporcionen los datos solicitados por la policía federal a través de una orden judicial, independientemente de la ubicación geográfica donde se recopilaron y almacenaron, siempre que la empresa esté sujeta a la jurisdicción de los Estados Unidos y que los datos recaigan dentro de la "posesión, custodia o control" de la misma corporación. De la misma manera que el Reglamento General de Protección de Datos (a partir de ahora designado con el acrónimo GDPR), que amplió el alcance territorial de la Directiva de Protección de Datos 95/46 / CE, la Ley *CLOUD* extiende el ámbito geográfico de la anterior *Stored Communications Act*[29]. La reciente aprobación de la *Strengthening American Cybersecurity Act* del 1 de marzo de 2022 en el formante legislativo y la sentencia *FBI v. Fazaga*[30] en el formante judicial refuerzan la idea de una preocupación desproporcionada por la seguridad nacional hacia elementos ajenos, colocada por encima de cualquier protección individual, denotando, al menos, una carencia de equilibrio en los intereses en juego. En la reciente decisión judicial del Tribunal Supremo en ningún momento se hace referencia a los derechos fundamentales de los ciudadanos islámicos ni, por consiguiente, a ningún tipo de equilibrio judicial de los derechos constitucionales con respecto a la *Foreign Intelligence Surveillance Act* de 1978 (FISA).[31]

10. El hecho es que ya en un primer examen afloran dos pilares legales que constituyen el nuevo principio de extraterritorialidad digital con dos concepciones subyacentes distintas de la protección de la identidad personal: el Reglamento General de Protección de Datos (GDPR) y, en particular, su art. 3, y la Ley CLOUD de los Estados Unidos. Estas dos legislaciones demuestran claramente cómo los Estados hayan desarrollado métodos alternativos para ejercer su poder soberano, que no se basan principalmente en el concepto de territorio. Este fenómeno implicaría un uso exorbitante del poder soberano, generando lo que Lessig llama "*competition among sovereigns*" [32], lo que inevitablemente conduciría, a su vez, a una erosión del estado de derecho tanto a nivel nacional como internacional. Definiremos a estos nuevos cibersoberanos con los términos hobbesianos de Cyberleviatanos.

11. Recientemente, esta tendencia a reafirmar los límites en el ecosistema digital ha ido acompañada de intentos de los Estados de recuperar el control sobre los datos y la infraestructura digital; es decir, reterritorializar la legislación en materia de ciberseguridad. Varios gobiernos nacionales han adoptado leyes de localización de datos, que requieren que los controladores almacenen físicamente los datos dentro del Estado, máxime el sistema cibernético chino.

2. El panorama normativo en la República Popular China

12. En primer lugar, "*unlike the EU and the U.S., data protection regulations in China are overdue*"[33]. En la comparación dinámica con la cultura jurídica china se destaca el predominio de la estrategia estatista cibersoberanista, sin olvidar las fuertes tensiones con la protección conferida a la privacidad en la versión china, principalmente en los últimos tiempos. En los últimos tiempos, la estrategia internacional del gobierno chino para la cooperación en el ciberespacio, cuyo texto fue publicado en *Xinhua News* en marzo de 2017, aclara los objetivos del gobierno chino con respecto a la ciberseguridad, la cooperación internacional y los medios para lograr sus objetivos[34].

[29] S.W. Smith, "Clouds on the Horizon: Cross-Border Surveillance Under the US CLOUD Act", en F. Fabbrini, E. Celeste y J. Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, 2021, p. 343.

[30] Tribunal Supremo, FBI *c*. *Fazaga*, 595 U.S. (2022), donde los jueces ampliaron el poder del gobierno de los Estados Unidos para invocar el secreto de Estado en disputas relacionadas con operaciones de inteligencia por parte de sus agencias de investigación sin hacer ninguna mención de las posiciones individuales correspondientes.

[31] Foreign Intelligence Surveillance Act del 1978 (FISA), 92 Stat. 1783, 50 U. S. C. par. 1801 ss.

[32] L. Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*, Nueva York, 2006, cap. 16.

[33] E. Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?", *Penn State Journal of Law and International Affaires*, 2020, p. 49.

[34] Administración de Ciberseguridad de China. "Estrategia Internacional de Cooperación en el Ciberespacio", publicado el 1 de marzo de 2917 en http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_5.htm.

13. Al tiempo que expresa una posición conceptual abierta en tema de soberanía y seguridad en el ciberespacio a través de la permanencia y colaboración en la comunidad internacional, el primer punto afirma una visión parcialmente proteccionista, contraria a cualquier interferencia supranacional con las regulaciones en el ciberespacio nacional[35]. La cuarta sección muestra el apoyo del gobierno chino a una red libre y abierta, en la que todos los ciudadanos disfruten de plenos derechos, acceso a la información, participación dentro de los parámetros establecidos en las leyes de gobernanza en el ciberespacio. En otras palabras, el gobierno chino promueve el libre flujo de información, siempre y cuando se garanticen los intereses públicos y nacionales. Los seis puntos pueden dibujar un escenario muy contradictorio, pero sustancialmente tienden a promover claramente los intereses chinos en el ciberespacio[36], particularmente cuando se permite una posible gobernanza internacional en la que no se produzca interferencia directa o indirecta en los ciudadanos de cada Estado, es decir, a nivel nacional[37].

14. La **Ley de Ciberseguridad de China de 2016** fue diseñada principalmente para fortalecer las redes locales contra la piratería maliciosa y todo tipo de ataques cibernéticos, especialmente desde servidores estadounidenses[38].[39] Sin embargo, desde el punto de vista de las empresas extranjeras, este fragmento de la legislación parece un "caballo de Troya tecnonacionalista"[40]. Alejándose del enfoque sectorial estadounidense de las disciplinas de privacidad, la Ley de Ciberseguridad de 2016[41] creó un amplio marco regulatorio, que incluye protecciones de privacidad de datos y se aplica a casi todas las entidades públicas y privadas[42].

15. Estas disposiciones incluyen requisitos de localización de datos para información personal y datos confidenciales. La localización de datos en China está impulsada fundamentalmente por preocupaciones de seguridad nacional que por la protección de la información personal y los derechos de los interesados. En junio de 2019, el gobierno chino publicó un borrador de medidas para las transferencias transfronterizas de datos llamado *Personal Information Outbound Transfer Security Assessment Measures*[43]. En

[35] El concepto de "cibersoberanía" (网络主权) aparece en el Diario del Pueblo, el órgano oficial del Partido Comunista Chino, donde se lo conoce como un "tema inevitable para la afirmación misma de la soberanía nacional en la era de Internet". Cfr. WANG YUAN, Xin Qiang, "Internet Sovereignty, an Inevitable Issue", *People's Daily*, 23rd ed., 23/4/2014.

[36] Ibídem.

[37] Cabe destacar la publicación en el sitio web oficial de la Administración del Ciberespacio de China de un documento titulado "Cibersoberanía: Teoría y Práctica (versión 2.0)", escrito en colaboración con la Universidad de Wuhan, el Instituto Chino de Relaciones Internacionales Modernas y la Academia de Ciencias Sociales de Shanghai en el que, además de reiterar la mencionada definición de cibersoberanía, se esbozan sus características y principios: un elemento central de este análisis es la jurisdicción del Estado soberano en el espacio digital, que también incluye "datos e información de red dentro de sus fronteras de acuerdo con la ley", hacia la cual los Estados tienen "deberes de prudencia y prevención" para evitar que terceros países pongan en peligro la seguridad y los intereses nacionales. Universidad de Wuhan et al., *Cyber Sovereignty: Theory and Practice (Version 2.0)*, publicado el 25/11/2020 en el sitio web de la Administración del Ciberespacio de China, accesible en el enlace http://www.cac.gov.cn/2020-11/25/c_1607869924931855.htm.

[38] Cfr. Z. Weiwei, *The China Wave: Rise of a Civilizational State*, New Jersey, 2012, p. 41.

[39] R. Vatanparast, "Data Governance and the Elasticity of Sovereignty", *Brooklyn Journal of International Law*, 2020, p. 28.

[40] S. Tiezzi, *Xi Jinping Leads China's New Internet Security Group", The Diplomat*, 28 febrero 2014, disponible en http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/

[41] Cfr. Y. Wu, T. Lau, D. Atkin, C.A. Lin, "A Comparative Study of Online Privacy Regulations in the U.S. and China", *Telecommunications Policy*, 2019, p. 603-616.

[42] K. Cai, "Jurisdictional Report: People's Republic of China in Regulation of Cross -Border Tran sfers of Personal Data in Asia", en GIROT Clarisse (ed.), Regulation of Cross-Border Transfers of Personal Data in Asia (editor)*Asian Business Law Institute*, 2018, p. 62 ss.

[43] C. Qiheng Chen, L. Shi, A. Mingli y K. Neville, "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China", *New America*, 13 junio 2019, disponible en https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Cfr. SHACKELFORD Scott - ALEXANDER, Frank, "China's Cyber Sovereignty: Paper Tiger or Rising Dragon?", *Asia & the Pacific Policy Society* (18 de enero de 2018), disponibile en www.policyforum.net/chinas-cyber-sovereignty/; L. De Nardis, G. Goldstein, Y D. A. Gross, "The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance", Paper presentado al *Columbia SIPSTech & Policy Initiative*, Columbia SIPA November 2016, disponible en www.policyforum.net/chinas-cyber-sovereignty/; Wagner, Daniel, "What China's Cybersecurity Law says about the future"*, Sunday Guardian*, 11 mayo 2019*,* disponible en *https://www.sundayguardianlive.com/news/chinas-cybersecurity-law-says-future/;* y R. Vatanparast, *op. cit.*, p. 90: "*China's*

resumen, "*the EU and U.S. models are indeed well established, yet antagonistic. Both sides of the Atlantic have a different philosophy underlying their approach, which leads to differences in the legal instruments used and the level of protection afforded to individuals. The EU model is proven to be increasingly influential on third-countries' laws at the expense of the U.S. way which has not attained the same success*"[44].

16. La estrategia Cyberleviathan de China tiende no solo a crear una infraestructura de red transnacional centralizada por su propio gobierno, sino que también expande la influencia política y económica de China a nivel mundial. Estas políticas, la primera dirigida a controlar el flujo de datos dentro de sus fronteras y la segunda encaminada a expandir su infraestructura de red transnacional, podrían explicar el movimiento para reterritorializar y, al mismo tiempo, tener un alcance extraterritorial[45]. Sin embargo, como ya se ha tenido ocasión de precisar, ninguna realidad se presenta de manera granítica. Recientemente, junto a las consideraciones realizadas hasta ahora en el campo de la soberanía cibernética, se abre paso una normación en constante evolución, que se desarrolla en una dirección distinta y, a veces, opuesta. El Código Civil de 2020, que incorpora plenamente la presencia del derecho chino en la familia jurídica romana, contemplaba la epifanía del derecho a la privacidad, definido como "[derecho] de una persona física [a] una vida privada tranquila y a su espacio privado, actividades privadas e información privada que no quiere revelar a otros", la protección separada de la información personal, obligando (y por lo tanto dando lugar a un derecho) a cualquier organización o individuo "que necesite acceso a la información personal de otros a hacerlo exclusivamente en "cumplimiento de la ley y garantizando la seguridad de dicha información".[46]

17. El Libro IV, capítulo VI describe los contornos de "dos sistemas (de protección), dos derechos": el primer derecho, el de la privacidad (yinsi quan隐私权), visto como un derecho "negativo", es decir, a la no intrusión en la vida privada de los demás por cualquier medio que pueda perturbar el "ámbito privado" de un individuo. El segundo, el de la protección de la información personal, un derecho "positivo", vinculado no solo a la personalidad de la persona física sino también al valor de uso de la información personal y, por lo tanto, al derecho a controlar quién hace uso de su información y cómo se extrae valor del uso de la información personal para objetar, corregir o solicitar una compensación a la autoridad judicial.

18. También es cierto que recientemente han surgido nuevos "filones occidentalistas" en la aprobación de la **Ley de Protección de Datos Personales** (conocida por las siglas "PIPL"), adoptada el 20 de agosto de 2021 por el Comité Permanente de la Asamblea Popular Nacional en tercera lectura y promulgada el mismo día por orden del Presidente de la República No. 91 y entró en vigor el 1 de noviembre de 2021[47]. La normativa, que consta de setenta y cuatro artículos, se propone como objetivo proteger los derechos e intereses relacionados con la información personal, estandarizando sus actividades de procesamiento y promoviendo un uso racional de la misma[48].

---

approach to governance of cross-border data flows reflects its broader approach to the regulation of content and information over the internet, some of which are filtered or blocked within its borders".

[44] E. Pernot-Leplay, *op. cit*., p. 49.

[45] J.E. Cohen, "Between Truth and Power: The Legal Constructions of Informational Capitalism", *International Journal of Communication*, 2019, p. 216.

[46] La disposición del artículo 1032, apartado 1, del Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Código Civil de la República Popular China], debe estar relacionada con el artículo 110, que reconoce el disfrute del derecho a la intimidad a toda persona física, distinguiéndolo explícitamente de otros derechos, como el derecho a la reputación y al honor; y el art. 990, que incluye el derecho a la intimidad entre los derechos de la personalidad, y con art. 994, que establece que el cónyuge, los hijos, los padres o, en su defecto, los parientes más cercanos tienen derecho de acción contra quien haya violado la privacidad de su fallecido.

[47] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) (Ley de Protección de Información Personal de la República Popular China] (adoptada en la 30ª reunión del Comité Permanente de la 13ª Asamblea Popular Nacional y promulgada por Orden del Presidente de la República No. 91/2021). En el futuro, se adoptará el acrónimo inglés "PIPL".

[48] A. Qi, G. Shao, y W. Zheng, "Assessing China's Cybersecurity Law"*, Computer Law & Security* Review, 2018, p. 1342.

19. Incluso en el sistema chino, por lo tanto, está surgiendo un modelo dual de ciberseguridad y protección de los derechos individuales, perfeccionado aún más por la entrada en vigor de la mencionada Ley sobre la protección de la información personal, cuya conexión con la dimensión cibersoberanista está expresamente establecida por la voluntad del legislador chino.

20. El panorama, por tanto, adquiere connotaciones cada vez más matizadas, ciertamente dominadas por el predominio de un concepto estatalista y lineal de soberanía digital, que, sin embargo, deja espacio para aperturas, a menudo no recogidas en el rango legislativo, tendentes a dar cabida a la protección de los derechos fundamentales, tal y como está estructurado en la legislación europea[49]. De hecho, las tensiones vinculadas a la aprobación del PIPL deben leerse cuidadosamente, ya que si, por un lado, se introducen principios similares al Reglamento General de la Unión, por otro, el trasfondo sigue permeado de la sustancia de la Ley de Ciberseguridad[50]. Completamente ausente es el diálogo judicial o, cuando menos, la ponderación entre los intereses de la seguridad nacional y la salvaguardia d los derechos individuales.

21. El modelo chino denota, por lo tanto, un predominio tendencial del elemento de cibersoberanía, entendido incluso en el sentido tradicional de control gubernamental sobre una población asentada en un territorio determinado, en comparación con el componente de protección de los derechos individuales, con una clara propensión de reciente formación a la introducción de una legislación sobre la privacidad individual. Sin embargo, el modelo chino (Zhongguo tese 中国特色) no reproduce un elemento existencial del propio modelo de identidad europeo: la concordancia judicial de las necesidades de seguridad estatal con la salvaguardia de la esfera de los derechos fundamentales del ciudadano[51].

III. El modelo relacional europeo

22. El modelo europeo es muy complejo. Ello se articula internamente en varios núcleos normativos (formantes legislativo y judicial) en constante interacción, como también a nivel vertical, es decir en relación con los sistemas nacionales. Como tendremos modo de ver, este paradigma complejo y relacional se extiende (y funciona solo en la medida que se reproduce también) más allá de los confines europeos. Su clave identitaria reside en un mecanismo osmótico de apertura. Al contrario de la cerrazón soberanista, el modelo europeo, esencialmente elaborado a nivel judicial, funciona coordinando los diferentes sistemas jurídicos regulados mediante la bisagra conceptual del respeto de los derechos fun-

[49] Véase D. Clementi, "La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?", *Diritti comparati*, 2022, p. 34: "*A distanza di un secolo dal seminale articolo di Warren e Brandeis sul diritto alla privacy, anche la dottrina cinese ha cominciato a individuare nel diritto alla privacy un certo grado di autonomia, distinguendolo e allo stesso tempo ricomprendendolo fra i diritti di personalità. Tale incompiuta autonomia rilevata dai giuristi cinesi è stata infine sanata con la promulgazione della Legge sulla responsabilità civile del 2009, ove il diritto alla privacy trova espresso riconoscimento quale diritto civile, autonomo e distinto dagli altri*".

[50] Sin embargo, la disposición de que las nuevas leyes o reglamentos administrativos pueden derogar directamente el PIPL permitiría a la Administración China del Ciberespacio de China (CAC) complementar o ampliar la aplicabilidad del PIPL fuera de la lista, lejos de ser exhaustiva, del art. 3, co. 2, nn. 1-2. Queda en manos de la Administración del Ciberespacio de China, la evaluación y autorización de la transferencia de datos personales solo si el operador pasa la evaluación de seguridad de conformidad con el art. 40 del PIPL. Además, la ley no impone las mismas obligaciones a las que deben estar sujetos los gestores de tratamiento también a las autoridades estatales.

[51] Aunque cabe destacar la intervención del Tribunal Supremo Zuigao Renmin Fayuan <Guanyu shenli shiyong ren lian shibie jishu chuli geren xinxi xiangguan minshi anjian shiyong falü ruogan wenti de guiding> Fashi [2021] 15, <<关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定>>, 法释 [2021] 15号[Interpretación sobre disposiciones sobre varias cuestiones de aplicación de la ley en casos civiles relacionados con el uso probatorio de la tecnología de reconocimiento facial para procesar información personal], Interpretación legal No. 15/2021 (adoptada en la 1841ª reunión del Jurado del Tribunal Popular Supremo el 8 de junio de 2021 y entró en vigor el 1 de agosto 2021), que prohíbe el uso obligatorio del reconocimiento facial sobre la base de una lectura restrictiva del Código Civil.

damentales. Donde este mecanismo se consagra es, como veremos *infra*, en la sentencia Kadi de 2008[52], en vía general, y en la saga Schrems[53], en el tema que nos ocupa.

1. El formante legislativo de la Unión: el derecho primario

23. "Europa ofrece la posibilidad de ser una alternativa de resistencia y cambio frente a la distopía tecnológica que Estados Unidos y China proyectan sobre el futuro"[54]. El conjunto de competencias de las que disponen las instituciones de la Unión, por tanto, constituye una *gobernanza* digital, basada en una revisión de la dignidad humana a través de una generación de derechos fundamentales que protejan a la persona y den sentido a su relación con la Inteligencia Artificial y la robótica[55]. La Unión Europea y el espacio legal europeo a una escala normativa más amplia no solo serían los portadores de un proyecto forjado en torno al derecho, como argumenta Zuboff[56], sino de una regulación íntima y firmemente anclada en los derechos fundamentales[57]. En esta operación estratégica ha sido, y es, esencial el papel desempeñado por el Tribunal de Justicia, que, desde una perspectiva amplia, ha esbozado los contornos de la esencia del derecho fundamental a la intimidad y a la protección de los datos personales.

24. En primer lugar, el marco jurídico competente está constituido **por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (**CFUE), que consagra el derecho a la protección de datos, y las disposiciones de los artículos **39 Tratado de la Unión Europea (a partir de ahora designado con el acrónimo TUE)** y **16 Tratado de Funcionamiento de la Unión Europea (a partir de ahora designado con el acrónimo TFUE**), que confieren a la Unión competencia legislativa en materia de protección de datos. Ante una idea de ciberespacio, defendida por Estados como China y Rusia, o ante el reciente aumento de la vigilancia gubernamental por parte de las administraciones estadounidenses Trump y Biden, se erige un conjunto de competencias, íntimamente ligadas al respeto de los derechos fundamentales, como se desprende de las tres disposiciones mencionadas. Esto significa, en definitiva, que no es posible ejercer dichas competencias a escala comunitaria sin respetar los límites inherentes a los derechos fundamentales (artículo 8, apartado 1, de la Carta de los Derechos Fundamentales y 16 TFUE), el derecho de acceso a los datos (artículo 8, apartado 2, de la Carta de los Derechos Fundamentales y el control sobre ellos ejercido por una autoridad independiente (artículo 8 TUE, apartado 3, y artículo 39 TUE)[58].

25. Es el primer nudo de la tela de araña normativa europea, vertebrado por límites y responsabilidades para el papel de la tecnología e inscrito en la identidad misma de la cultura europea. Un pacto que también parte de una idea de libertad lockeana, no sólo de obediencia hobbesiana. Un pacto liberal como el defendido por Locke, pero que, entrando en el siglo XXI, se desarrolla según una ética tecnológica basada en una nueva idea de responsabilidad. Esta comprensión, como argumentó Hans Jonas, debe inspirarse en un imperativo que salvaguarde el derecho a una vida auténtica en términos humanos[59].

---

[52] Sentencia del Tribunal de Justicia (Gran Sala), 3 de septiembre de 2008 en los asuntos acumulados C-402/05 P y C-415/05 P, Yassin Abdullah Kadi y Al Barakaat International Foundation c. Consejo y Comisión.

[53] Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559

[54] J.M. Lassalle, *Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital*, Barcelona, 2019, p. 138.

[55] M. Dunn Cavelty, F. Egloff, "The Politics of Cybersecurity: Balancing Different Roles of the State", *St Antony's International Review* 15 no.1, 2019, pp. 37-57.

[56] S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology*, 2015, p. 75; Idem, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization" *Organization Theory*, (3), 2022, p. 3.

[57] M. Dunn Cavelty, F. Egloff, *op. cit*., pp. 37-57.

[58] Cfr. A. Moreno Bobadilla, I. Serrano Maíllo (eds.), *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*, Tirant lo Blanch, Valencia, 2021.

[59] H. Jonas, *The Imperative of Responsibility. In Search of an Ethics for the Technological Age*, University of Chicago Press, 1984, y S. Rodotà, *Il diritto di avere diritti*, Laterza, Bari, 2012.

2. El derecho derivado de la UE

26. A partir del marco competencial se deriva la legislación de segundo grado ejercida por las instituciones comunitarias, que llamaremos formante legislativo. La primera década del siglo vio la emergencia de una especie de soberanía corporativa digital *de facto*. "*It is that form of controlling power that is supported by those who argue that corporate self-regulation is sufficient, that legislative intervention is unwelcome and unnecessary, and that any required checks and balances of corporate digital power will come from a competitive, laissez-faire approach, and market-based equilibria*"[60]. La primera fase de la reglamentación europea se sustenta en una concepción liberalismo y armonizadora del mercado digital.

27. Las teorías libertarias, como hemos tenido la oportunidad de destacar en el modelo estadounidense, se basan en un único supuesto fundamental, podríamos decir ontológico. Las características del *cosmos* digital obligarían a gobiernos y legisladores a adoptar regulaciones basadas en el libre mercado. En una de sus obras, Froomkin define Internet como la "moderna Hidra"[61]. Cada vez que alguien corta las cabezas de la bestia mítica, crecen otras nuevas. El mismo paralelismo ocurre cuando los reguladores estatales intentan interferir con el ámbito digital (cortando una de las cabezas de Hydra) y los usuarios eluden fácilmente las nuevas reglas (el crecimiento de nuevas cabezas). Esta metáfora ilustra no solo el compromiso al que los gobiernos se enfrentaron a fines del siglo pasado entre la innovación y la protección de los derechos constitucionales, sino también por qué los Estados (democráticos) adoptaron un enfoque de libre mercado en relación con el entorno digital (es decir, el liberalismo digital). Este marco liberal ha caracterizado la política de la UE a principios de este siglo, principalmente en la **Directiva** europea **sobre comercio electrónico** [62], y la **Directiva** europea **sobre protección de datos**[63].

28. Solo más tarde, la Estrategia Global sobre Ciberseguridad fue acompañada por una **Directiva Europea sobre seguridad de las redes y de la información**[64]. Esta Directiva ha dado lugar a un claro movimiento centrípeto en la legislación nacional, imponiendo obligaciones tanto a los Estados miembros como a los operadores de infraestructuras críticas y a los proveedores de servicios de la sociedad de la información (incluidas las redes sociales, los servicios *cloud* y los motores de búsqueda). De esta manera, la UE dejaba atrás el enfoque voluntario, optando por un enfoque prescriptivo que impone a los operadores privados la obligación de tomar medidas de seguridad, así como la obligación de compartir información con las autoridades sobre los incidentes que se han producido.

29. La protección de los datos personales ha alcanzado un nuevo nivel de consolidación no solo después de la adopción del Tratado de Lisboa gracias principalmente al papel del Tribunal de Justicia, como veremos a continuación, sino también con la adopción del Reglamento General de Protección de Datos (RGPD)[65]. El cambio en la estrategia de la Unión puede examinarse poniendo en tensión los primeros considerandos del RGPD con la Directiva de Protección de Datos para comprender el papel central de los derechos fundamentales de los sujetos interesados en el marco de la legislación europea de protección de datos. Este nuevo marco jurídico que gravita en torno a los derechos fundamentales no implica la destrucción de otros derechos y libertades constitucionales en juego, ni siquiera de los intereses de la Unión en garantizar el buen desarrollo del mercado interior mediante el fomento de la innovación en el contexto de la industria de los datos. Sin embargo, este cambio de paradigma en el enfoque de la

[60] L. Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU", *Philosophy & Technology, 33*(3), 2020, p. 371.

[61] A.M. Roomkin, "The Internet as a Source of Regulatory Arbitrage"*,* en B. Kahin, C. Nesson (eds.) *Borders in Cyberspace*, 1999, p. 129.

[62] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000.

[63] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

[64] Directiva UE 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas para garantizar un elevado nivel común de seguridad de las redes y sistemas de información en toda la Unión

[65] Reglamento 2016/679 del Parlamento Europeo Y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Unión subraya el compromiso de proteger los derechos fundamentales y los valores democráticos en una sociedad algorítmica.

30. Toda la estructura del RGPD se basa en principios generales que giran en torno a la responsabilidad del controlador de datos, que debe garantizar y demostrar el cumplimiento del sistema de ley de protección de datos. No se trata, por tanto, de construir un sistema estatalista/soberanista en el modelo chino, ni de elevar al sector privado a portavoz de la Primera Enmienda, como en el paradigma estadounidense: el mismo proceso de consulta al sector privado identifica el modelo de gobernanza europeo.

31. Al igual que en el caso del contenido, el enfoque de la Unión se ha centrado en aumentar la responsabilidad (entendida como rendición de cuentas) del sector privado, al tiempo que limita la discrecionalidad en el uso de tecnologías algorítmicas por parte de poderes irresponsables. La impronta característica de la legislación de la UE, además de su capacidad de armonización, que ya hemos descrito, radica principalmente en la sustancia de la persecución de los derechos garantizados por la Carta de los Derechos Fundamentales y en la aprobación de las normas, que implica a la mayoría de las posibles *stakeholders,* sin dejarles la última palabra al respecto.

32. En el dilema "regulación versus libertad absoluta", o dicho en términos estratégico-políticos de estrategias internacionales, regulación china o vietnamita contra el modelo estadounidense, la Unión Europea y el Consejo de Europa han marcado un hito intermedio basado en la defensa de los derechos fundamentales. Y en el siguiente dilema "Autorregulación versus heterorregulación" se han posicionado en una perspectiva claramente favorable a la consulta de todas las partes interesadas y, en definitiva, a la decisión política institucional, con el posterior control judicial de la firme jurisprudencia del Tribunal de Justicia (y en parte del Tribunal Europeo de Derechos Humanos) sobre el tema de la férrea protección de los derechos fundamentales del ciudadano[66].

IV. El formante judicial europeo

33. La acción legislativa ahora analizada está íntimamente asociada a la interacción de la jurisprudencia de los tribunales europeos, de la que extrapolaré solo algunas decisiones que van en la misma dirección de protección de los derechos fundamentales en el ámbito de la ciberseguridad. En el perímetro jurídico europeo, la forma judicial es el componente más importante (el formante en términos juscomparativos). De hecho, la característica fundacional de la Unión es su apertura no sólo a las organizaciones internacionales vecinas, como el Consejo de Europa, sino también a la comunidad internacional en su conjunto[67]. Frente a extensas regulaciones legislativas de cibersoberanía como la Ley CLOUD de los Estados Unidos de 2018 y la legislación china de ciberseguridad de 2016, el Tribunal de Justicia de la Unión Europea (en adelante, el acrónimo TJUE) erige algunos elementos importantes de la *gobernanza* europea sobre ciberseguridad en el cumplimiento de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE[68].

34. La protección de la libertad de expresión, la privacidad y la protección de datos en el contexto europeo se basaba no solo en el nivel estatal interno, sino también en la jurisprudencia del TEDH[69]. El Tribunal de Estrasburgo ha desempeñado un papel crucial no solo en la protección de los derechos fundamentales, sino también en la puesta de relieve de los desafíos derivados de las tecnologías digitales.

[66] A.N. Guiora, *Cybersecurity Geopolitics, Law, and Policy*, New York, 2017; A. López, "Ciberseguridad en los Estados", *Revista de Occidente*, Nº 456, 2019 (Ejemplar dedicado a: Ciberseguridad: El reto del siglo XXI), pp. 16-31.

[67] Cfr. G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022.

[68] C. Kuner, "The Internet and the Global *Reach of EU Law*", en (CREMONA, Marise y SCOTT, Joanne eds.,) EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, 2019, p. 112.

[69] G. De Gregorio, "The rise of digital constitutionalism in the European Union", *Int. Const. Law Review* Vol. 19 No. 1, 2021, p. 52.

35. La adopción del Tratado de Lisboa fue el siguiente paso en este proceso[70]. Tanto en el ámbito de los contenidos como en el de los datos, el TJUE ha interpretado los derechos y libertades de la Carta de la UE con el objetivo de garantizar la protección efectiva de estos intereses constitucionales. Dada la falta de una revisión legislativa de la Directiva de Comercio Electrónico o la Directiva de Protección de Datos[71], el activismo judicial ha puesto de relieve los desafíos a los derechos fundamentales en la sociedad de la información, promoviendo así la transición de una perspectiva puramente económica a una nueva fase constitucional del constitucionalismo europeo (digital)[72]. "*In 2011, the CJEU shifted its approach from a merely economic perspective to a fundamental rights-based approach. It is not by accident that this turning point occurred in the wake of the Lisbon Treaty recognizing that the EU Charter has the same legal value as EU primary law*"[73].

36. La constelación de decisiones judiciales[74] perfila, de hecho, los contornos de la esencia del derecho fundamental a la identidad digital[75]. El primer enfoque constitucionalista se consume dentro del recinto normativo de la Unión, anulando por primera vez una directiva comunitaria 2006/24/CE. En la sentencia *Digital Rights Ireland*[76] , el Tribunal considera que sus efectos sobre los derechos fundamentales son desproporcionados al apreciar, de la misma guisa que un tribunal constitucional, la injerencia y las posibles justificaciones de los derechos a la intimidad y a la protección de datos de los ciudadanos de la Unión protegidos por la Carta de la Unión Europea.

37. Esta jurisprudencia comienza a interactuar con la acción legislativa y a menudo influye en sus estrategias políticas, así como en los trasplantes legislativos posteriores en otros sistemas nacionales. A menudo es el formante judicial quien se encarga de promover las directrices que los colegisladores europeos han cumplido posteriormente, como en el caso de las citadas normativas de la Directiva NIS y del RGPD. Su implementación a mediados de 2018 implicó no solo un proceso centrípeto de armonización *ad intra* de las diversas legislaciones nacionales, sino que promocionó también varias iniciativas de trasplante sobre seguridad y privacidad en países fuera de la Unión Europea. Los gobiernos de Canadá y Brasil ya han aprobado una legislación similar al GDPR, que ha entrado en vigor en 2020. Australia y Singapur han regulado la notificación de violaciones en un plazo de 72 horas inspiradas en esta regulación, la legislatura india está considerando una legislación similar al GDPR y el Estado de California ha aprobado una ley de privacidad inspirada evidentemente en la legislación de la UE, considerada la más completa en los Estados Unidos hasta la fecha.

1. El diálogo judicial en el espacio jurídico europeo

38. Este diálogo judicial ha adquirido recientemente una dimensión reticular y relacional tanto en la dirección que podríamos decir horizontal con el homólogo Tribunal Europeo de Derechos Humanos, como en la orientación vertical con los interlocutores privilegiados del Tribunal de Luxemburgo, es

[70] O. Pollicino, "Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech"*, 25 Eur. L.J.* 155, 2019, p. 25.

[71] O. Pollicino, "Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech", *Eur. L.J.*,155, 2019, p. 25.

[72] G. De Gregorio, "The rise of digital constitutionalism in the European Union"*, Int. Const. Law Review*, Vol. 19 No. 1, 2021, p. 52

[73] G. De Gregorio, *op. cit.*, p. 54.

[74] Sentencias del TJUE de 8 de abril de 2014, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources et al. y Kärntner Landesregierung et al.; C-362/14, Maximiliam Schrems c. Comité de Protección de Datos, 6 de octubre de 2015; Patrick Breyer/Bundesrepublik Deutschland, C-582/14, de 19 de octubre de 2016; Tele2 Sverige AB contra Post-och telestyrelseny, C-203/15; Secretaría de Estado del Departamento del Interior/Tom Watson y otro C-698/15; Ministerio Fiscal, C-207/16, de 2 de octubre de 2018.

[75] M. Brkan, *op. cit.*, p. 864.

[76] Sentencia TJUE C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Ministro de Comunicaciones, Recursos Marinos y Naturales y otros y Kärntner Landesregierung y otros, ECLI:EU:C:2014:238 (8 de abril de 2014)

decir, los jueces ordinarios. Este es un rasgo identitario del modelo europeo, que podríamos definir como relacional frente a la idea de cibersoberanía china y estadounidense.

39. En la reciente batería de decisiones adoptadas por el Tribunal de Justicia, la tendencia inicial a proteger el derecho esencial a la identidad digital se consolida, no se "diluye", en relación con las necesidades de seguridad nacional, subsumidas en la disposición del art. 4.2 TUE. Dos demandas existenciales para la Unión Europea chocan, o más bien deben ponderarse: la identidad digital en el sentido individual con connotaciones sociales y políticas, como hemos visto, y la identidad constitucional del Estado, cuya esencialidad se reitera dos veces en la misma norma mencionada del art. 4.2 TUE. La identidad, entendida en un sentido dialéctico-relacional, es, por lo tanto, el desafío actual del constitucionalismo europeo (digital)[77].

40. El Tribunal de Justicia no se limita únicamente a proteger un derecho, durante años considerado esencial; profundiza en la "ponderación fundamental" de las "voces" supranacionales y estatales[78]. Por lo tanto, actúa como juez constitucional, que maneja elementos no solo jurídicos (como en la primera fase constitucional europea), sino más bien identitarios. La tendencia pretoriana a no defender sólo un lado del cuerno del dilema, sino a equilibrar los intereses en juego, caracteriza el entero modelo europeo. Esta operación axiológica ha crecido al calor del art. 2 TUE, en primer lugar elaborada por las decisiones Tele2 Sverigel[79] y Ministerio Fiscal[80] , se extiende a las sentencias posteriores Privacy International[81], La Quadrature du Net[82] y Prokuratuur[83], y luego se consolida en el *arrêt* G.D./Commissioner de 5 de abril de 2022[84].

41. Mientras que en el primer bloque de jurisprudencia, en definitiva, se reitera la necesidad fundamental de crear un control judicial con respecto al escrutinio de los derechos en juego, en la fase posterior la corte luxemburguesa no se declara incompetente en la evaluación de estos intereses y traza un surco conciso y profundo en su balance, indicando algunos factores evaluativos que deben iluminar las decisiones legislativas y judiciales nacionales. "*The evolution of the Court's case-law highlights the intricate institutional architecture at play when it comes to defining the future of mass surveillance and democracy in the digital era, with a complex part played by the judiciary, the legislative and the executive in a multi-level polity such as the EU*"[85].

42. Como puede verse, se trata de una red de nudos jurisprudenciales, que se extiende en la doble dirección horizontal y vertical. Se teje, entonces, una tela de araña cognitiva y normativa, imprescindible para conocer el modelo europeo de protección de la identidad digital. El punto de partida sólo puede ser la *Grundnorm del* artículo 2 del TUE: nos enfrentamos a un elemento existencial de la Unión. La sentencia La Quadrature en el apartado 114 establece que "la interpretación del artículo 15, apartado 1, de la Directiva 2002/85 debe tener en cuenta tanto el derecho al respeto de la vida privada, garantizado por el artículo 7 de la Carta, como el derecho a la protección de los datos personales, consagrado en el artículo 8 de ésta, tal como se refleja en la jurisprudencia del Tribunal de Justicia, y el derecho a

[77] Cfr. A. Lazari, "*La cuestión de la identidad en el derecho internacional, europeo y comparado: por una visión relacional del Derecho*", *Rev. Esp. Der. Eur.*, 2022, (81), pp. 99–155.

[78] J. Weiler, *The Constitution of Europe. 'Do the New Clothes Have an Emperor* Harvard University Press, 1999, pp. 187 ss.

[79] TJUE, Tele2 Sverige AB v. Postoch telestyrelsen e Secretary of State for the Home Department v. Tom Watson and Others, C203/15 e C698/15; ECLI:EU:C:2016:970.

[80] TJUE, Ministerio Fiscal C207/16, C-207/16; ECLI:EU:C:2018:788.

[81] TJUE, Privacy International/Secretary of State of Foreign and Commonwealth affairs, C-623/17, ECLI:EU:C:2020:790

[82] TJUE, La Quadrature du Net y otros, French Data Network y otros y Ordre des barreaux francophones et germanophone y otros, ECLI:EU:C:2020:791

[83] TJUE, H.K. c. Prokuratuur, C-746-18; ECLI:EU:C:2021:152

[84] TJUE, G.D. c. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General, C140/20, ECLI:EU:C:2022:258.

[85] En V. Mitsilegas, E. Guild, E. Kuskonmaz, N. Vavoula, "Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks"*, Eur Law J.* 2022, p. 2.

la libertad de expresión, ya que este derecho fundamental, garantizado por el artículo 11 de la Carta, constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista, que forma parte de los valores en los que, en virtud del artículo 2 TUE, se fundamenta la Unión"[86].

43. En el apartado 43 de la posterior sentencia Commissioner of An Garda Síochána[87] esta afirmación se cita literalmente casi como un axioma conceptual, representando el punto de partida de la siguiente operación de ponderación con respecto a las necesidades de seguridad nacional. Por lo tanto, no se baja la guardia respecto a las crecientes instancias de seguridad nacional, sino que se exponen elementos garantes indispensables en la apreciación de las instancias de seguridad nacional protegidas por el art. 4.2 TUE.

44. Se esbozan los confines de la concepción de la identidad europea. Además, ambas sentencias añaden que "los datos de tráfico y los datos de localización pueden revelar información sobre un número significativo de aspectos de la vida privada de los interesados, incluida la información sensible, como la orientación sexual, las opiniones políticas, las creencias religiosas, filosóficas, sociales o de otro tipo y el estado de salud, que estos datos también gozan de una protección especial en virtud del Derecho de la Unión"[88]. Cabe añadir que los desafíos que plantea el capitalismo digital a los valores democráticos constituyen una de las principales razones que llevan a la Unión a emanciparse del optimismo tecnológico estadounidense, que, como ya se ha visto en la primera parte, considera la Primera Enmienda en términos de dogma del liberalismo digital. Al otro lado del Atlántico, las características del constitucionalismo europeo han animado cada vez más a la Unión a seguir un nuevo camino identitario para hacer frente a los retos de la sociedad algorítmica.

45. El juez de Luxemburgo no rechaza *a priori* el recurso al art. 4.2 TUE: es un derecho que podríamos definir constitucional. El Tribunal de Justicia deja claro que "[e]n vista de estas diversas obligaciones positivas, es necesario, por tanto, encontrar un equilibrio entre los diferentes intereses y derechos legítimos en juego"[89]. Pero en la ponderación fundamental se ve favorecida por la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos, que ha declarado que las obligaciones positivas derivadas de los artículos 3 y 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, cuyas garantías correspondientes se establecen en los artículos 4 y 7 de la Carta, implican: en particular, la adopción de disposiciones sustantivas y procesales y medidas de carácter práctico para combatir eficazmente los delitos contra las personas mediante investigaciones y enjuiciamientos eficaces.

46. Como se decía antes, estas afirmaciones se van contemperando con los otros protagonistas del dialogo judicial, tanto a nivel horizontal como horizontal.

47. En esta dirección, el fenómeno de *cross-fertilisation* es claro y ya robusto. Por esta razón, el Tribunal de Justicia ha declarado que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, no se opone a medidas legislativas que permitan, con el fin de salvaguardar la seguridad nacional, recurrir a un requerimiento judicial que obligue a los proveedores de servicios de comunicaciones electrónicas a conservar de forma general e indiscriminada datos de tráfico y datos de localización, en situaciones en las que el Estado miembro de que se trate se enfrente a una amenaza grave para la seguridad nacional que sea real y actual o previsible, cuando la medida que establece tal requerimiento judicial pueda ser objeto de un control efectivo por un órgano jurisdiccional o un órgano administrativo independiente cuya decisión tenga efecto vinculante, que pretenda demostrar la existencia de una de estas situaciones y el cumplimiento

[86] TJUE, La Quadrature du Net y otros, cit., punto 114.
[87] TJUE, G.D. contro Commissioner of An Garda Síochána, cit., punto 43.
[88] TJUE, La Quadrature du Net y otros, punto 117; CGUE, G.D. c. Commissioner of An Garda Síochána, cit., punto 56.
[89] TJUE, G.D. c. Commissioner of An Garda Síochána, cit., punto 62.

de los requisitos y garantías que deben establecerse, y dicho requerimiento judicial sólo puede dictarse por un período limitado a lo estrictamente necesario, pero puede ser renovable cuando persista dicha amenaza. El Tribunal de Justicia declaró que el objetivo de preservar la seguridad nacional corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad mediante la prevención y represión de las actividades que pueden desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país y, en particular, amenazar directamente a la sociedad, la población o el Estado como tal, como en particular las actividades terroristas.

48. Para determinar este nudo judicial, el tribunal luxemburgués se basa una vez más en la jurisprudencia del tribunal de Estrasburgo, tejiendo los primeros hilos horizontales de su red conceptual.

2. Los filamentos horizontales de la red: la relación con el Tribunal Europeo de Derechos Humanos

49. Al impulso emanado por el Tribunal de Luxemburgo responden en sentido horizontal la corte de Estrasburgo y verticalmente algunos altos jueces estatales. En la primera dirección, el fenómeno de *cross-fertilisation* es consolidado y fructífero "*When the CJEU released its Digital Rights Ireland decision, the question on the cross-fertilisation between the CJEU and the ECtHR arose. The Big Brother Watch and Centrum för Rättvisa decisions delivered by the Grand Chamber (GC) of the ECtHR has piqued the interest in that cross-fertilisation or fragmentation – if there is one – to determine the legal limitations of security and intelligence services in conducting surveillance operations under the Charter and the ECHR*" [90]. Desde hace algún tiempo, el TEDH ha comenzado a incluir en su jurisprudencia los requisitos legales para la interceptación permisible de las comunicaciones y la recopilación de información en relación con los intereses de seguridad nacional. En particular, en el marco de esta última forma de vigilancia, el TEDH consideró que la recogida de la información y su posterior utilización por las autoridades constituían una injerencia separada en el sentido del artículo 8[91]. Adoptó un enfoque similar al de la forma anterior de vigilancia, en particular en *Weber y Saravia*, donde declaró que "la transmisión de datos y su utilización por las autoridades [...] constituye una nueva injerencia separada en los derechos de los demandantes en virtud del artículo 8"[92].

50. En el citado asunto Digital Rights Ireland, el TJUE se basó en la opinión del TEDH para declarar que los proveedores de servicios de comunicaciones obligan a los proveedores de servicios de comunicaciones a conservar los datos de comunicaciones de sus usuarios y a proporcionar al público un acceso posterior a dichos datos consagrando el derecho a la intimidad establecido en el artículo 7 CEDH. De este modo, comenzó a instaurar los requisitos para justificar la injerencia resultante del acceso a los datos por parte de las autoridades, limitando el objetivo del acceso a la prevención o detección de delitos graves.

51. El camino de esta *cross-fertilization*[93] judicial entre el TEDH y el TJUE tomó un giro diferente después de Big Brother Watch y el Centrum för Rättvisac. Suecia[94], donde el tribunal de Estrasburgo también fue llamado a pronunciarse sobre el estado actual de la protección del individuo en la *sociedad post-Snowden* en el reciente caso ***Big Brother Watch y otros contra el Reino Unido***[95]**.**

[90] V. Mitsilegas, E. Guild, E. Kuskonmaz, N. Vavoula, *op. cit*., p. 27.

[91] *Leander c. Suecia* (1987) 9 EHRR 433, párr. 48; *Amann c. Suiza* (2000) 30 EHRR 843, párr. 69; *Rotaru c. Rumania* (2000) 8 BHRC 43, párr. 46.

[92] *Weber e Saravia c. Germania* (2008) 46 EHRR SE5, par. 79

[93] Cfr. A. Lazari, *La cross-fertilisation y la formación del paradigma comunitario de responsabilidad del Estado: «el esquema de la crisis»*, in *Revista de Derecho Comunitario Europeo*, enero-abril (2005), pp. 177-225, Idem, *La Nueva Gramática Del Constitucionalismo Judicial Europeo*, en *Revista de Derecho Comunitario Europeo* mayo/agosto (2009), pp. 501-538.

[94] Centrum För Rättvisa v. Sweden, n. 35252/08.

[95] Big Brother Watch y otros c. el Reino Unido n. 58170/13, 62322/14 e 24960/15.

52. En cuanto al fondo de la cuestión, el Tribunal de Justicia, aun suponiendo que "*sería erróneo suponer automáticamente que la interceptación masiva constituye una mayor intrusión en la vida privada de una persona que la interceptación selectiva, que por su naturaleza es más probable que dé lugar a la adquisición y el examen de un gran volumen de sus comunicaciones*"; llega a la conclusión que tal régimen de interceptaciones "*no puede ser conforme al derecho en el sentido del artículo 8*" [96].

53. A raíz de la jurisprudencia citada del TJUE, el Tribunal también ha dictaminado que, cuando estos parámetros están garantizados, este control debe acometerse mediante la creación de un organismo independiente, que pueda examinar el uso correcto de los datos recogidos. Una vez más, de la lectura de la sentencia de 25 de mayo de 2021, **Big Brother Watch & Others v**. **el Reino Unido**, se desprende claramente que es el equilibrio entre la necesidad legítima de seguridad nacional, llevada a cabo por GCHQ (Government Communications Headquarters*)* en ejecución de la Ley de Regulación de Poderes de Investigación (conocida con el acrónimo RIPA) de 2000, y la protección de los derechos fundamentales a la vida familiar y la privacidad consagrados en el art. 8 de la Convención[97].

3. Los filamentos verticales de la red: la relación con los órganos jurisdiccionales nacionales

54. No es posible comprender plenamente el modelo europeo de protección de la identidad digital sin recurrir comparativamente a ciertas decisiones de los tribunales nacionales, con las que el TJUE conversa a diario.

55. Para comenzar en el perímetro pretoriano italiano, en la decisión de la Cass. Penal. Sec. 3 No. 11991, 2022[98], del Consejo de Estado francés[99] y del Tribunal Constitucional belga[100]. Curiosamente, cada juez trazó diferentes caminos en las observaciones del TJUE en *La Quadrature du Net y otros*. Mientras que el juez citado anuló las disposiciones incompatibles de la legislación belga sobre conservación de datos, los primeros siguieron un enfoque encaminado a apoyar el régimen nacional de conservación de datos.

56. El *Conseil d'Etat* ha tratado de aceptar en la medida de lo posible los argumentos del Gobierno francés relativos a la prioridad de las consideraciones de seguridad y su importancia dentro del orden constitucional, como se alega en el contexto del art. 4 TUE, apartado 2, tratando de evitar una confrontación directa con el Derecho de la Unión y el TJUE[101]. Lo que está en juego, refiriéndose a la provisión de art. 4.2 TUE, es muy alto: afecta a la misma identidad constitucional francesa. El tribunal administrativo francés sostiene esta vez que no existe equivalencia entre los principios consagrados en el Derecho constitucional francés y las normas del Derecho de la Unión. "De hecho, los objetivos de valor constitucional de salvaguardar los intereses fundamentales de la nación, prevenir las amenazas al orden público, rastrear a los delincuentes y combatir el terrorismo no se reflejan en el derecho primario de la UE"[102]. Además, de manera apodíctica, el Consejo de Estado afirma que "la Constitución es la norma suprema del derecho nacional. En particular, el Consejo Constitucional considera que los objetivos de

[96] Big Brother Watch y otros c. el Reino Unido, cit., párrafo 316.

[97] Cabe destacar el aspecto comparativo que surgió en la sentencia del TEDH en cuestión, a saber, el estudio de dos sentencias del Tribunal de Apelación de La Haya de 14 de marzo de 2017 (apartados 253 a 262), y del Tribunal Constitucional Federal alemán de 19 de mayo de 2020 (1 BvR 2835/17), puntos 247-252.

[98] Cass. penal. Sección 3 No. 11991, 2022, 31/01/2022, confirmada por Sent. Cass. Criminal enviado. Sec. 6 núm. 6618 año 2022, 03/12/2021.

[99] Consejo de Estado, sentencia de 21 de abril de 2021, decisión núm. 393099

[100] Tribunal Constitucional de Bélgica, Decisión No. 57/2021, de 22 de abril de 2021, https://www.const-court.be/public/f/2021/2021-057f-info.pdf.

[101] Cfr. N. Perlo, "La decisione del Consiglio di Stato francese sulla Data retention: come conciliare l'inconciliabile", *Diritti Comparati* N. 2/2021, pp. 163-183.

[102] N. Perlo, *op. cit*., p. 181.

prevenir las amenazas al orden público y localizar a los delincuentes son "necesarios para salvaguardar los principios y derechos de valor constitucional"[103].

57. El *Conseil d'Etat* aceptó el vínculo entre los mecanismos nacionales de conservación de datos y la protección nacional de datos, sin declarar inválida o inaplicable el Derecho de la UE. Más bien, pretendía establecer los parámetros y límites de los sistemas nacionales de conservación de datos a través de una interpretación orientada a la seguridad de la jurisprudencia del TJUE.

58. De este modo, el *Conseil d'Etat* termina por aplicar la jurisprudencia del TJUE, en particular La *Quadrature du Net y otros.*, señalando que se permite la difusión generalizada de determinadas categorías de datos considerados menos sensibles, como el estado civil, la dirección IP, las cuentas y los datos de pago. La retención general de datos de tráfico y ubicación con fines de seguridad nacional también está justificada, pero el gobierno tiene el deber de evaluar periódicamente la existencia de una amenaza grave, real, real o previsible para la seguridad nacional. Por otra parte, la conservación general de datos telemáticos y de localización con fines distintos de la seguridad nacional, en particular la persecución de infracciones penales y la protección del orden público, es ilegal. Al hacerlo, el Consejo de Estado evitó una confrontación directa con el TJUE, interpretando en un sentido amplio la jurisprudencia del TJUE sobre las facultades del ejecutivo para conservar datos personales de manera generalizada.

59. El Tribunal Constitucional belga, por su parte, adoptó plenamente el razonamiento del TJUE en *la sentencia La Quadrature du Net y otros.* por la que se anula la legislación belga en materia de conservación de datos. El Tribunal de Justicia no dudó en señalar que la normativa pertinente permitía una obligación generalizada e indiscriminada para los proveedores de telecomunicaciones de conservar los datos personales de sus clientes con fines más amplios que la lucha contra la delincuencia grave y la protección de la seguridad pública. Según el Tribunal de Justicia, la sentencia del TJUE en el asunto *La Quadrature du Net y* otros Exigía un cambio en la perspectiva del legislador nacional: la obligación de conservar datos personales debe ser la excepción, no la regla. En el mismo sentido trazado por el *Conseil d'Etat* es la sentencia del **Tribunal Supremo español 727/2020[104]**.

60. También en este caso el examen de las decisiones anteriores del Tribunal de Justicia es muy exhaustivo, lo que lleva a la conclusión de que "la legislación española en su conjunto es respetuosa con los derechos reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea [..] Lo determinante a efectos del proceso penal es si la limitación que sufre cada investigado en sus derechos fundamentales supone una injerencia no respetuosa con la Carta de Derechos Fundamentales de la Unión Europea y, en general, con los derechos fundamentales reconocidos en nuestra Constitución".

4. Los rasgos relacionales del juez tejedor

61. Como hemos visto en el análisis realizado con respecto a la cultura jurídica estadounidense y china[105], que padecen de intervenciones judiciales de índole "ponderadora", en la protección de la identidad digital en juego no solo hay una dimensión individual (de protección de un derecho individual)[106]. "*This increasing importance of privacy protection in Europe is not only to be understood in relation to the protection of individuals' rights, however, but also with regard to its relevance for democratic so-*

[103] Conseil d'État, sentencia de 21 de abril de 2021, decisión núm. 393099.

[104] Penal Nº, Tribunal Supremo727/2020, Cfr. Sala de lo Penal, Sección 1, Rec 4218/2018 de 23 de Marzo de 2021-

[105] Y podríamos añadir a esta nómina también el modelo ruso, como evidencia J. Gray, *The New Leviathans: Thoughts After Liberalism,* op. cit., p. 23, en el capítulo *Russia's Orthodox Leviathan*.

[106] F. Bignami, "Schrems II: The Right to Privacy and the New Illiberalism", *Verfassungsblog (29 de julio de 2020), Www. Verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-lliberalism/?fbclid=IwAR1wXiMQ1HL_KwaOTw3TzTI-FOGRBtNzTaTMrd3mVMGovHyLonTjvNye-vMk,*

cieties; by strengthening people's personal freedom, European privacy protection is, at the same time, proving to be essential for the development and flourishing of democratic practices conceptualized as collective acts of free communication"[107].

62. El radio de acción de la red judicial europea trasciende una dimensión meramente individual (de protección del derecho) del derecho a la intimidad[108], revelando la importancia de la dimensión social, como lo demuestra la reciente intervención en la *account* del entonces presidente estadounidense Trump[109]. Las plataformas digitales pueden decidir por sí mismas no solo cómo interactúan las personas, sino también cómo pueden hacer cumplir sus derechos (y cuáles son esos derechos) regulando de forma privada su infraestructura digital[110]. En el contexto de esta comprensión social del concepto, la privacidad no solo se considera una relación de interacción y, por lo tanto, una práctica inherentemente social, sino que también se describe como un bien social, considerado de crucial importancia para las sociedades democráticas. "*The consolidation of private powers in the algorithmic society does not only challenge the protection of individual fundamental rights, such as freedom of expression, privacy and data protection but also democratic values*"[111].

63. Recientemente se ha precisado que "el principio de transparencia desempeña un papel cada vez más importante en el Derecho de la Unión y está actualmente consagrado en el Derecho primario, estando cubierto por los artículos 1 TUE y 10 TUE y 15 TFUE. En el marco del Derecho de la Unión, este principio se materializa principalmente en exigencias de transparencia institucional y procedimental relativas a actividades de carácter público, como la actividad legislativa o administrativa. A este respecto, la transparencia contribuye a reforzar los principios de democracia y respeto de los derechos fundamentales definidos en el artículo 6 del TUE y en la Carta. El propio Tribunal ha reconocido el vínculo entre transparencia y democracia, afirmando en su jurisprudencia que el objetivo del principio de transparencia es dar a los ciudadanos el acceso más amplio posible a la información, con el fin de reforzar el carácter democrático de las instituciones y de la administración"[112].

64. Pero hay más. ¿Cómo se pueden proteger estos derechos, entendidos individual y políticamente[113]? ¿En qué realmente se diferenciaría el modelo europeo de los paradigmas esencialmente soberanista y mercantilista?

65. Esta lucha contra los Leviatanes[114] tiene que llevarse a cabo a través de un trabajo continuo de integración jurisprudencial. La efectividad de la protección primaria y fundamental de los datos personales que, debe reclamarse también en la relación entre terceros Estados, controladores de datos y destinatarios de datos no comunitarios, representa una condición esencial para el intercambio de los mismos: la protección del GDPR y su *primauté* hacia los ciudadanos europeos. Leyendo la sentencia Schrems II a contraluz[115], se puede encontrar la función relacional del juez tejedor comunitario (tanto ad

[107] S. Seubert y C. Becker, "The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection", *German Law Journal* 22, 2021, pp. 31-44.

[108] S. Seubert y C. Becker, *op. cit.*, p. 44.

[109] L. Floridi, "Trump, Parler, and Regulating the Infosphere as our Commons", Philosophy and Technology 34 (1), 2021, pp. 1-5.

[110] I. Schuliaquer, ¿ *Can Twitter and Facebook Censor Trump in the Name of Democracy?*, *OpenDemocracy,* 13 de enero 2021 disponible en: https://www.opendemocracy.net/en/democraciaabierta/twitter-facebook-censura-trump-democracia-en/

[111] G. De Gregorio, *op. cit,* p. 34.

[112] Conclusiones del Abogado General Sr. P. Pitruzzella, presentadas el 20 de enero de 2022 en los asuntos acumulados C37/20 y C601/20 WM (C37/20), Sovim SA (C601/20)/Registros Mercantiles de Luxemburgo.

[113] Cfr. A. Lazari, "La nueva gramática del constitucionalismo judicial europeo", *Revista de Derecho Comunitario Europeo*, 33, 2009, pp. 501-538.

[114] "The new Leviathans offer meaning in material progress, the security of belonging in imaginary communities and the pleasures of persecution", así J. Gray, *The New Leviathans: Thoughts After Liberalism*, op. cit., p. 16.

[115] Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559

intra como *ad extra),* de la que Marta Cartabia diserta brillantemente[116]. "*The judgment is emblematic of the formal strength of the EU's fundamental rights approach to personal data protection but also its limits in the age of digital interdependency*"[117].

Por lo tanto, es imposible ignorar la referencia esencial que, entre los hilos de la sentencia, realiza el Tribunal de Justicia a la saga *Kadi*[118].

66. Examinando la sentencia seminal Schrems II a la luz del *arrêt* Kadi[119], aflora la imagen de un sistema europeo que construye un modelo autónomo; un paradigma que no permite interpretaciones arbitrarias o restricciones a los derechos fundamentales. Pero esta decisión también siembra la semillas de la relacionalidad del modelo europeo, descifrándose no en los términos de la *closure* de Glenn[120], tradicionalmente asociada con la propia noción de soberanía, presente, en cambio, en las fórmulas legislativas de Estados Unidos y China[121]. La autoridad judicial, basándose en la disposición legislativa del art. 3 del RGPD, sienta las bases para una extensión de la protección constitucional del derecho a la identidad digital, apoyando su argumento sobre un mecanismo de valores[122]. Es imprescindible que, en relación con los diferentes sistemas jurídicos con los que está vinculado el ordenamiento jurídico europeo, la protección de los derechos fundamentales constituya no sólo un baluarte insuperable, sino también un medio de recíproco enriquecimiento.

67. Todo ello representa una forma no tanto de ejercer la soberanía, que en esencia nunca se ha discutido, en el terreno último de los derechos fundamentales, de la misma manera que la Unión Europea sólo había conocido de manera relajada en su primera fase, atenuando la vocación puramente mercantilista de la construcción de la Comunidad. Los derechos fundamentales, antes relegados –como ya se ha señalado– a meras excepciones en manos de los Estados miembros para justificar restricciones a las libertades económicas proclamadas por los Tratados, se convierten así en un eje del sistema, constituyendo una «bisagra» que regula su apertura al exterior y al interior[123]. Esta propensión abierta está contenida en la vocación misma de la Unión y, en particular, en el art. 6.3 TUE, donde la propia existencia de los derechos fundamentales está vinculada a las tradiciones constitucionales comunes a los Estados miembros.

68. Por lo tanto, el papel de la Carta de los Derechos Fundamentales de la Unión Europea, que ya fue crucial en la sentencia Kadi, no puede pasar desapercibido o no considerarse esencial: es la metodología identitaria de la Unión. Sin embargo, debemos tener en cuenta una diferencia sustancial que parece poner aún más de relieve la autonomía relacional del ordenamiento jurídico comunitario.

---

[116] M. Cartabia, "Editorial: Courts' Relations", *I•CON* 18 (2020), p. 2.

[117] K. Irion, "Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law", *EU Law Blog* (24 de julio de 2020), www.europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/

[118] TJUE, 3 de septiembre de 2008 en los asuntos acumulados C-402/05 P y C-415/05 P, Yassin Abdullah Kadi y Al Barakaat International Foundation c. Consejo y Comisión.

[119] M.H. Murphy, "*Assessing the Implications of Schrems II for EU-US Data Flow", ICLQ*, 2020, p. 14.

[120] Indispensable para la reconstrucción de la idea de Estado moderno asociado a la exclusión/*closure* es la magnífica obra de H.P. Glenn, *The Cosmopolitan State,* Oxford University Press, Oxford, 2013. Recientemente cfr. H. Dedek (ed.), A *Cosmopolitan Jurisprudence: Essays in Memory of H. Patrick Glenn*, ASCL Studies in Comparative Law, Cambridge, 2021.

[121] C. Gentile, "La saga Schrems e la tutela dei diritti fondamentali", *Federalismi*, 2021, n. 1, p. 54: "*In definitiva, Schrems II potrebbe costituire il punto di partenza di un dibattito più articolato sull'applicazione extraterritoriale dei diritti fondamentali*". Véase también J.P. Meltzer, "The Court of Justice of the European Union in Schrems II: The impact of GDPR on Data Flows and National Security", *VoxEu*, 5.8.2020.

[122] Identifica elementos críticos R. Bifulco, "Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno, *DPER online,* 2/2020, p. 7. Véase tambien M. Tzanou, *Schrems I y Schrems II: assessing the case for the extraterritoriality of EU fundamental rights*, en F. Fabbrini, E. Celeste, J. Quinn (eds.), *Data Protection Beyond Borders Transatlantic Perspectives On Extraterritoriality And Sovereignty,* Hart Publishing, 2021.

[123] Muy interesantes las reflexiones de O. Pollicino, "La tutela de la privacy digital: el diálogo entre el Tribunal de Justicia de la Unión Europea y las jurisdicciones nacionales", *Revista de Estudios Políticos*, 2016, 173, p. 244.

69. En la decisión Kadi, la fuente exógena de la violación de los derechos fundamentales protegidos por la Carta fueron las obligaciones impuestas por un acuerdo internacional y, más concretamente, por una resolución del Consejo de Seguridad de las Naciones Unidas. El contenido de la Resolución del Consejo de Seguridad de la ONU era el término en el que el sistema comunitario debía distanciarse, interponiendo la protección de los derechos fundamentales como un obstáculo para una encarnación plena y servil de lo previsto en la fuente heterónoma en la que se basaba el reglamento del Consejo, luego parcialmente anulado.

70. Por su parte, en la saga *Schrems*[124], no se trata de una norma de Derecho comunitario, ni de Derecho internacional, sino del sistema de Puerto Seguro y, en particular, del ordenamiento jurídico de los Estados Unidos lo que expondría a la Unión a una amenaza para los derechos fundamentales de los ciudadanos europeos. Por consiguiente, el límite impuesto por la protección de los artículos 7, 8 y 47 de la Carta es contrario al derecho de un Estado tercero. También en virtud de la función relacional presente en la sentencia *Schrems*, no debe subestimarse un vínculo importante (esta vez con intraproyección) entre una parte de la sentencia y algunos precedentes relevantes del Tribunal Constitucional alemán.

71. El apartado 73 establece que "la expresión «nivel de protección adecuado» exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta". Esta decisión del Tribunal de Luxemburgo se asemeja mucho al contenido de dos sentencias muy importantes del Tribunal Constitucional alemán, conocidas como Solange I y Solange II[125]. Según el *Bundesverfassungsgericht,* considerando que la integración europea se encontraba todavía en una fase de integración parcial –atestiguada por la ausencia de un documento de protección de los derechos fundamentales y, más en general, por el problema de la debilidad democrática visible en la construcción de la entonces Comunidad Europea, dicha cláusula debía ser interpretada estrictamente. Por consiguiente, a falta de un catálogo de derechos fundamentales, el Tribunal Constitucional se reservó el derecho de no aplicar disposiciones del Derecho comunitario contrarias a los derechos protegidos por la Constitución alemana. La solución jurisprudencial ofrecida años más tarde por la referencia a tradiciones constitucionales comunes y en 2008 por la citada sentencia Kadi parece indicar el camino emprendido no solo por el constitucionalismo europeo, sino también la clave para entender la extraterritorialidad establecida por las sentencias Schrems. El modelo europeo, por lo tanto, funciona en la medida en que no es un medio de imposición soberanista, como apunta Bradford[126]: no es ***impuesto por el poder*****, sino** ***por el valor (siempre que sea realmente relacional, añadiria)***[127]. Por lo tanto, junto con el examen de las implicaciones implícitas en las autorizaciones externas, siempre debe evaluarse el alcance ad *intra* del espacio jurídico europeo, como las dos importantes intervenciones del Tribunal Constitucional alemán sobre el tema del "derecho al olvido"[128].

72. Si no damos lugar a una continuidad extra/intra osmótica, podríamos generar una distinción entre una extraterritorialidad basada en el poder, es decir asentada una vez más en aspiraciones neocoloniales y soberanistas, en lugar de una nueva categoría basada en los valores compartidos[129], la estrategia

[124] TJUE, *Schrems v. Facebook Ireland* del 19 octubre 2016, causa C-582/14; y Schrems II del 16 julio 2020, causa C-311/18, *Facebook Ireland* c. *Schrems*

[125] Tribunal Constitucional Federal 29 de mayo de 1974, 37 Decisiones del Tribunal Constitucional Federal [BVerfGE] 271, 285; e Tribunal Constitucional Federal [BVerfG] [Tribunal Constitucional Federal] 12 de octubre de 1993, 89 Decisiones del Tribunal Constitucional Federal [BVerfGE] 155.

[126] A. Bradford, *The Brussel Effect. How the European Union Rules the World*, Oxford, 2020*,* New. U. L. Rev. 1, 2015, p. 107.

[127] Cfr. O. Pollicino, "Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?", Hart, 2021; Idem, "Data Protection Beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty"*,* en F. Fabbrini, E. Celeste, J. Quinn (eds.), *op. cit*., Hart, 2021, pp. 342- 369.

[128] Tribunal Constitucional Federal de Alemania, sentencia de 6 de noviembre de 2019, 1 BvR 16/13, RTBF I.

[129] Además, habría que seguir reflexionando sobre la necesidad de compartir el paradigma europeo de defensa de los derechos fundamentales con respecto a la posibilidad de que una extensión extraterritorial pueda conducir a la aparición de una norma consuetudinaria internacional. Si los parámetros establecidos por la legislación europea fueran compartidos y reelabora-

impulsada por valores, de la que Gstrein y Zetter discuten[130]. Además, habría que seguir reflexionando sobre la necesidad de compartir el paradigma europeo de defensa de los derechos fundamentales con respecto a la posibilidad de que una extensión extraterritorial pueda conducir a la aparición de una norma consuetudinaria internacional. Si los parámetros establecidos por la legislación europea fueran compartidos y reelaborados por la gran mayoría de la comunidad internacional mediante acuerdos internacionales, podría producirse un fenómeno de interacción con el efecto constitutivo de la disposición convencional en una costumbre internacional.

73. El camino hacia una compartición del modelo europeo, con la lógica posibilidad de acuerdos que mejoren el estándar planteado por la Unión, es muy arduo. A pesar del nuevo acuerdo anunciado el pasado 10 de julio, (en su sigla inglés *Data Privacy Framework*) y de la influencia incluso indirecta ejercida en China por el RGPD, emerge un escollo podríamos decir epistemológico de comprensión de la ponderación de los intereses en juego. La decisión de adecuación concluye que el ordenamiento de Estados Unidos garantiza un nivel adecuado de protección, comparable al de la Unión Europea, para los datos personales transferidos desde la UE a empresas estadounidenses a efectos del artículo 45 del RGPD. Sin embargo, paradigmático es el caso de la citada decisión adoptada a principios de marzo de 2022 por la Corte Suprema de los Estados Unidos Fazaga[131], que limita el derecho individual a cuestionar las actividades de vigilancia del gobierno de los Estados Unidos[132]. Los jueces, de hecho, han ampliado el poder del gobierno de los Estados Unidos para invocar el secreto de Estado en disputas relacionadas con operaciones de inteligencia por parte de sus agencias de investigación, precisamente en el mismo periodo en que la jurisprudencia europea se movía en la dirección opuesta tanto en la sentencia SIA "SS" de febrero de 2022,[133] como en las conclusiones estimulantes del Abogado General Pitruzzella en los casos acumulados WM y Sovi[134].

74. En definitiva, es probable que el flujo de datos se divida o divida aún más entre regímenes normativos, más allá de lo que ha iniciado el GDPR de la UE, desde el Gran Cortafuegos de China hasta el oeste de Europa. Queda el hecho de que la localización de los datos asume diferentes significados, creando un espectro que va desde la soberanía china o comercial estadounidense hasta la gobernanza basada en valores: "*Localisation clauses reflect the identity challenges of the EU as a good global actor and a somewhat more protectionist one as to the parameters of "good" here*"[135].

dos por la gran mayoría de la comunidad internacional mediante acuerdos internacionales, podría producirse un fenómeno de interacción con el efecto constitutivo de la disposición convencional en una costumbre internacional.

[130] O.J. Gstrein, A. Zwitter, *op. cit.*, p. 4: "*we suggest that rather than relying on extraterritorial effect that adopts a power-based approach using the 'Brussels Effect', the universal protection and promotion of European values will be more sustainable when adopting value based strategies*". Desde una perspectiva juscomparada, las decisiones de adecuación tienen un efecto extraterritorial, ya que proporcionan un incentivo, en consonancia con el enfoque de armonización interna, para actualizar o revisar las leyes nacionales de protección de datos. Esto se demostró más recientemente en los casos de Japón y Corea del Sur, que actualizaron y alinearon sus leyes nacionales con el GDPR en un esfuerzo por tener un acceso privilegiado al mercado único de la UE. La decisión de adecuación para Japón se adoptó el 23 de enero de 2019 y es la primera en el marco de GDPR, mientras que las conversaciones con Corea del Sur concluyeron con éxito el 30 de marzo de 2021. Ambas evaluaciones de adecuación forman parte de un paquete de políticas más amplio que consiste principalmente en un acuerdo de libre comercio.

[131] Corte Suprema, Oficina Federal de Investigaciones *c*. *Fazaga*, 595 Estados Unidos (2022).

[132] En este tema importante es la obra de FAHEY, Elaine, *EU as global digital actor*, Hart, 2022.

[133] Sentencia del Tribunal de Justicia (Sala Quinta) de 24 de febrero de 2022, «SS» SIA/Valsts ieņēmumu dienests, asunto C-175/20, ECLI: ECLI:EU:C:2022:124

[134] Conclusiones del Abogado General Sr. P. Pitruzzella, presentadas el 20 de enero de 2022, asuntos acumulados C37/20 y C601/20 WM (C37/20) Sovim SA (C601/20) contra Registros Mercantiles de Luxemburgo: "¿Cuál es el equilibrio adecuado entre, por un lado, la necesidad de transparencia con respecto a los titulares reales y las estructuras de control corporativo, que desempeña un papel clave en la prevención del blanqueo de capitales y la financiación del terrorismo? y, por otro lado, el respeto de los derechos fundamentales de los interesados, es decir, los titulares reales, y, en particular, sus derechos al respeto de la vida privada y a la protección de los datos personales".

[135] E. Fahey, "Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?", *European Papers*, Vol. 8, 2023, No 2, p. 511.

VI. El diálogo judicial, clave de la afirmación del modelo europeo

75. Sin la protección de los derechos fundamentales, la defensa contra los ciberataques y la libertad de la que disfrutamos se convertiría en una libertad mutilada o asistida, distorsionada bajo la dirección de algoritmos biométricos que incluso condicionan nuestra sensibilidad y determinan nuestro comportamiento. Esto significa que la seguridad y el orden digital deben ir de la mano de una *gobernanza* que establezca una serie de derechos fundamentales que garanticen, parafraseando a Habermas, que el reto tecnológico no solo se responda con tecnología, sino también, y, sobre todo, con derechos digitales[136]. Se trata de una nueva soberanía, si así queremos definirla, asentada en los derechos fundamentales del ciudadano. A la necesidad urgente de seguridad ni siquiera se responde con los conceptos ya obsoletos de soberanía excluyente o incluso violenta, sino con una *gobernanza* abierta a asimilar los valores de los demás[137]. La creación del sistema basado en los valores no sólo depende de la aclaración y defensa de los marcos conceptuales existentes, sino también de la creación de espacios seguros para el diálogo sustantivo a fin de establecer un consenso internacional más amplio, así como el compromiso con una protección alta y efectiva de los derechos humanos, que están garantizados internacionalmente independientemente del privilegio o estatus individual[138].

76. La "infoesfera" es un Jano de dos caras. Sin duda, nos otorga una mayor libertad, pero al mismo tiempo nos expone a una vigilancia cada vez mayor, que nos afecta[139]. La respuesta del Tribunal de Justicia en la sentencia Quadrature es clara: los Estados miembros no pueden renunciar a sus obligaciones en materia de derechos fundamentales en virtud del Derecho de la UE externalizando la retención de datos a operadores del sector privado, obligándoles a transmitir datos a los servicios de seguridad e inteligencia con una simple referencia a la exención de la seguridad nacional.

77. Si bien el ciberespacio y los flujos de datos pueden, en cierto sentido, "escapar de la geografía"[140], es evidente que también están profundamente entrelazados con ella[141]. A través de un análisis comparativo de las regulaciones de transferencia de datos en tres jurisdicciones, a saber, China, la UE y los Estados Unidos, es evidente que existe una doble lógica con respecto a los datos y la territorialidad en cada uno de los enfoques regulatorios. Al mismo tiempo, se está intentando reterritorializar los datos, ubicándolos donde se encuentran la infraestructura, los interesados o los procesadores de datos. La diferencia conceptual radica en la función y las modalidades de esta retención de datos, a saber, si está dictada por una aspiración soberanista excluyente tradicional, o por la protección de los derechos fundamentales, que, sin embargo, no pueden y no deben interpretarse unilateralmente. Los valores de la Unión Europea, consagrados en el art. 2 TUE, debe interpretarse dialógicamente tanto a través del diálogo continuo con referentes judiciales nacionales, como fuera del territorio europeo, asimilando cualquier valor de los demás.

78. Se ha creado un nuevo espacio difícil de definir según los referentes tradicionales de lo público y privado y ni siquiera según las claras líneas geopolíticas tradicionales. En definitiva, las gigantescas nuevas recopilaciones de información aumentan la vulnerabilidad social, no sólo en la dirección que se suele destacar, la de ser concebidas como herramientas de control de las personas. Una nueva fase del constitucionalismo europeo (digital) se está interponiendo como un escudo contra el ejercicio discrecional del poder por parte de las plataformas en línea en el entorno digital[142]. Como señala Suzor a propósito de esos nuevos monstruos bíblicos que hemos llamado Cyberlevitans, "*digital constitutiona-*

[136] J. Habermas, *Technology and Science as 'Ideology*, trad. Jeremy J. Shapiro, Beacon Press, Boston, 1970.

[137] Cfr. L. Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU", *Philosophy & Technology*, 33(3), 2021, pp. 369–378.

[138] O.J. Gstrein, A. Zwitter, *op. cit*., p. 24.

[139] H. Byung-Chul, *Las no-cosas. Quiebras del mundo de hoy,* Taurus, 2021, p. 65.

[140] J. Goldsmith y T. Wu, *Who Controls The Internet?: Illusions Of A Borderless World,* 2006, p. vii.

[141] E.J. Cohen, "Cyberspace As/And Space", 107 *Colum. L. Rev.*, 2007, pp. 212–213.

[142] H. Roberts, J. Cowls, F. Casolari, J. Morley, M. Taddeo y L. Florido, "Safeguarding European values with digital sovereignty: an analysis of statements and policies", *Internet Policy Review*, 10, 2021, p. 3.

lism requires us to develop new ways of limiting abuses of power in a complex system that includes many different governments, businesses, and civil society organizations"[143]. En otras palabras, el constitucionalismo digital consiste en la articulación, principalmente de valores, de los límites al ejercicio del poder en una sociedad en red[144]. "*The logic behind the idea of digital sovereignty in the EU lies in the need to preserve the European 'DNA' of values and rights*"[145]. La UE no solo ha promovido un impacto en el desarrollo de normas de protección de datos a nivel mundial, sino que también ha "*taken an essential role in shaping how the world thinks about data privacy*"[146].

79. El implacable proceso legislativo comenzó con la primera ley regional de protección de datos en Alemania en 1970 y continúa desde entonces en muchos niveles políticos e institucionales diferentes[147]. La heterogeneidad normativa de la protección de datos ha sido durante mucho tiempo un estímulo para la armonización legislativa dentro de la Unión, del mismo modo que la adecuación de los sistemas jurídicos extranjeros en relación con el parámetro regulador europeo debe representar un incentivo similar para el diálogo transnacional[148].

80. Por tanto, a las principales preguntas que surgen en el estudio de los ciberataques y la ciberseguridad debe responderse de manera compleja y axiológica, subrayando que la ciberseguridad se refiere tanto a los bienes públicos como a la propiedad privada y que los organismos designados para su protección deben someterse al escrutinio de normas constitucionalmente relevantes y consensuadas, si no quieren convertirse ellos mismos en auténticos ciberleviatanes. La distancia conceptual entre la visión americana y europea está contenida en la comparación entre la mencionada saga Schrems, y la pronunciación *FBI vs. Fazaga*[149]. El perfil de mayor distancia se encuentra precisamente en el aspecto axiológico de la protección de la identidad digital en el Derecho de la Unión, donde asume una dimensión existencial e identitaria, asociada al art. 2 TEU. La Unión vincula su propia existencia a la protección dialógica de la identidad digital, apartándose así tanto de la visión estadounidense, china y rusa, como del grado de identidad de la misma protección de la jurisprudencia del tribunal de Estrasburgo. "*Though both European courts are in principle in alignment, their interaction is much more complex, and it is hoped that the seemingly more lenient approach of the ECtHR will not lead to further downgrading of the standards of protection as elaborated by the CJEU*"[150].

81. Por su parte, la Unión Europea debe evitar absolutamente el riesgo de degeneración en una forma de soberanismo o nacionalismo. Preservar la propia identidad es absolutamente necesario hoy en día, pero los genes de la Unión no tienen que transformarse en la identidad excluyente, ya que consisten precisamente en su aspecto relacional. Aunque Europa vio nacer a los primeros Leviatanes hace siglos, debe preservar su identidad axiológica dialogando, tanto en la esfera pública como en el foro privado, tanto ad *extra* como *ad intra*. Este es un factor existencial, yo diría antropológico. La experiencia que vivimos en el siglo XXI está subliminalmente ligada a la participación de los que están vigilados. No solo ser observado, sino también observar se ha convertido en una forma de vida. Mientras que en la visión panóptica los personajes de Orwell vivían atrapados por una incertidumbre aterradora sobre cuándo y por

[143] N. Suzor, *Lawless: The Secret Rules that Govern our Digital Lives*, London, 2019, p. 173.

[144] G. De Gregorio, "The rise of digital constitutionalism in the European Union"*, Int. Const. Law Review* Vol. 19 No. 1, 2021, pp. 41–70.

[145] E. Celeste, "Digital Sovereignty in the EU: Challenges and Future Perspectives", en F. Fabbrini, E. Celeste, J. Quinn (eds.), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, cit., p. 234. Apoya su tesis R. Vatanparast, "Data Governance and the Elasticity of Sovereignty", *Brooklyn Journal of International Law*, 2020, p. 23: "*The EU justifies the GDPRs extraterritoriality by its fundamental rights obligations*".

[146] P. Schwartz, "*Global Data Privacy: The EU Way*", *NYU Law Review*, 2019, p. 773. Cfr. L. Bygrave, *Data Privacy Law: An International Perspective,* Oxford, 2014, pp. 108–109.

[147] G. González Fuster, "The Right to the Protection of Personal Data and EU Law", en G. González Fuster (ed.), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, London, pp. 213–248.

[148] Cfr. O. Lynskey, "The 'Europeanisation' of Data Protection Law"*, Cambridge Yearbook of European Law Studies* 252, 2017, p. 19.

[149] Corte Suprema, Oficina Federal de Investigaciones *c*. *Fazaga*, 595 Estados Unidos ___ (2022)

[150] En V. Mitsilegas, E. Guild, E. Kuskonmaz, N. Vavoula, *op. cit*., p. 36.

qué estaban siendo observados, la vigilancia de hoy es posible gracias a los clics en nuestro sitio web, mensajes de texto e intercambios de fotos. En la época de *las no-cosas*, en el que el cuerpo se da por sentado y un algoritmo predice nuestros gustos y movimientos, se hace cada vez más difícil encontrarse y estar de acuerdo con el Otro. "La vigilancia se está infiltrando cada vez más en la vida cotidiana, en forma de conveniencia. En el acto de llevar a cabo tantas tareas para nosotros, los infómatas demuestran ser informantes muy eficientes que nos monitorean e influyen. Así, guiado por algoritmos, el ser humano pierde cada vez más su poder de actuar, su autonomía. [..] Acumulamos amigos y *seguidores* sin conocer nunca al Otro"[151].

82. La presencia del Otro es constitutiva de la acción comunicativa en el sentido esbozado por Habermas. Pero la acción comunicativa presupone un movimiento de ida y vuelta con respecto al Otro. La desaparición del Otro significa la eliminación del discurso. Según Eli Parisier, la personalización algorítmica de la red, la burbuja filtrante del Ego que escucha y lee solo opiniones similares a las suyas, aniquila el espacio público[152]. La creciente atomización y narcisificación de la sociedad nos hace sordos a la voz del Otro y conduce a la pérdida de empatía. La infocracia termina sustituyendo el discurso por la creencia y la adhesión tribal, convirtiendo la identidad excluyente en un escudo o fortaleza que rechaza la alteridad. La tribalización progresista, de la que los partidos populistas o excluyentes son un ejemplo, pone en peligro la democracia. Conduce a una cómoda dictadura tribal de opinión e identidad, desprovista de toda racionalidad comunicativa. La sociedad algorítmica se está descomponiendo en identidades atomizadas irreconciliables sin alteridad. Si no intervenimos profundamente en la arena constitucional, en lugar de un discurso público, tendremos una guerra continua de identidades. Escuchar es un acto político en la medida en que integra a las personas en una comunidad y las hace capaces de establecer un discurso y una narrativa del Nosotros relacional. "*Within Western societies, the hyper-liberal goal is to enable human beings to define their own identities. From one point of view this is the logical endpoint of individualism: each human being is sovereign in deciding who or what they want to be. From another, it is the project of forging new collectives, and the prelude to a state of chronic warfare among the identities they embody. Human beings can never be wholly self-defined. If their identity is to be more than a private fantasy, they must somehow induce others to accept it. Hyper-liberals aim to achieve this by capturing institutions that divide people into distinct categories, which then become competing groups. The stakes are not only the selves that are chosen but the positions in society that go with them*"[153].

83. El neofascismo y el tribalismo posmoderno surgen de esta estrechez de miras[154]. La solución propuesta por el espacio jurídico común europeo a la invasividad de las redes de vigilancia y al panopticón chino toma la forma de tela de araña, cuyos nodos y filamentos se construyen sólidamente solo a través de la relación con el Otro[155].

[151] H. Byung-Chul, *op. cit.*, p. 70.

[152] E. Parisier, *El filtro burbuja. Cómo la web decide lo que leemos y lo que pensamos*, Taurus, 2013.

[153] J. Gray, *op. cit.*, pp. 109-110.

[154] E. Díaz Álvarez, *La palabra que aparece. El testimonio como acto de supervivencia*, 2021, Barcelona, p. 56.

[155] "La vita degli abitanti d'Ottavia è meno incerta che in altre città. Sanno che più di tanto la rete non regge", así I. Calvino, *Le città invisibili*, Milano, 2016, p. 54.