

Citation: DOMÍNGUEZ DÍAZ, F.A. , “ZABALA ROLDÁN, P., La diplomacia digital de la Unión Europea: pandemia y lucha contra la desinformación, Madrid, Reus, 2022, 180 pp.”, *Peace & Security – Paix et Sécurité Internationales*, No 12, 2024.

ZABALA ROLDÁN, P., *La diplomacia digital de la Unión Europea: pandemia y lucha contra la desinformación*, Madrid, Reus, 2022, 180 pp. XVI Premio Andaluz de Investigación sobre Integración Europea.

Hay que resaltar que la digitalización desempeña un papel crucial en la Unión Europea (UE). Los efectos de la digitalización tienen múltiples efectos en diversos aspectos de la sociedad, la economía y la gobernanza. Entre todos ellos, nos parece especialmente interesante cómo la digitalización influye en la competitividad económica y el empleo, la investigación y el desarrollo sostenible, los servicios públicos digitales y la ciberseguridad. Consciente de estos retos, la Comisión europea propuso en el año 2021 un programa de política digital¹, aprobado por el Parlamento Europeo y el Consejo en virtud de la Decisión (UE) 2022/2481, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030. La propuesta consiste en establecer una Brújula Digital para traducir las ambiciones digitales de la UE para 2030 en objetivos concretos vinculados con cuatro puntos cardinales: (i) ciudadanos con capacidades digitales y profesionales del sector digital muy cualificados; (ii) infraestructuras digitales sostenibles que sean seguras y eficaces; (iii) transformación digital de las empresas y (iv) digitalización de los servicios públicos. Este impulso político hay que ponerlo en relación con los trabajos iniciados en el decenio pasado para acelerar la transformación digital de Europa y continuar avanzando hacia un verdadero mercado único digital.

La monografía de Zabala Roldán, que obtuvo en 2022 el XVI Premio Andaluz de Investigación sobre Integración Europea, de la Red de Información Europea de la Junta de Andalucía, tiene como objetivo el análisis de las iniciativas

¹ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones a través de su Comunicación “Brújula Digital 2030: el enfoque de Europa para el Decenio Digital”, COM(2021) 118 final.

de diplomacia digital del Servicio Europeo de Acción Exterior (SEAE) durante la pandemia ocasionada por la COVID-19, un complejo contexto influenciado no sólo por la necesidad de responder de forma coordinada a una amenaza global a la salud humana, sino por la distorsión de la realidad a través de la infodemia y la desinformación. El autor estructura la obra en cinco Capítulos, más Introducción y Conclusiones, exponiendo sistemáticamente el alcance del fenómeno de la diplomacia digital europea y sus transformaciones para luchar contra la desinformación durante la pandemia.

En su Introducción, el autor expone la importancia de la diplomacia digital y la ciberdiplomacia, y cómo estas prácticas se han convertido en herramientas esenciales para la UE en la promoción de seguridad cibernética, la lucha contra la desinformación y el fortalecimiento de su posición en el ámbito internacional. El autor señala como el SEAE ha reevaluado e implementado estrategias de diplomacia digital, particularmente en respuesta a los desafíos y retos presentados por la pandemia de la COVID-19. Igualmente destaca el propósito que el Consejo de la UE le confiere a la Diplomacia Digital Europea para la siguiente década, enfatizando su utilidad como herramienta esencial (junto a la ciberdiplomacia) en la promoción de seguridad cibernética, la lucha contra la desinformación y el fortalecimiento de la posición de la UE en el ámbito internacional. Presenta el Plan de Acción contra la Desinformación como un componente clave de la estrategia de diplomacia digital de la UE y remite su análisis al Capítulo IV y anuncia un hito histórico de suma importancia en clave geopolítica: la creación de la primera oficina diplomática digital europea en San Francisco. Desde luego, este hecho demuestra el notable esfuerzo por fortalecer las relaciones con la industria tecnológica americana y por avanzar en los objetivos digitales de la UE. Se menciona la Global Gateway como una estrategia para promover conexiones digitales seguras y los beneficios económicos, sociales y medioambientales a nivel mundial (p. 20).

El Capítulo I se centra en la revisión de la literatura contemporánea sobre diplomacia y diplomacia digital, pilares sobre los cuales el autor establece el enfoque teórico para su investigación. En este sentido, propone identificar los conceptos y categorías claves en los debates sobre la digitalización de la diplomacia, particularmente en el contexto de la política exterior de la UE y su adaptación a los desafíos presentados por la pandemia de COVID-19 y la era digital. Concluye el autor al respecto que “es precisamente la utilización

indistinta de prefijos y adjetivos tales como *digital*, *cyber*, *virtual*, *2.0*... lo que altera la posibilidad de establecer un marco teórico/normativo lo suficientemente homogéneo para lograr una consolidación temprana de esta disciplina” (p. 29), si bien asevera que “se identifican oportunidades subyacentes para profundizar los debates sobre el objeto de estudio” (p. 29). Igualmente se discute cómo la diplomacia digital ha evolucionado desde la diplomacia tradicional hasta convertirse en una nueva y poderosa herramienta para los diplomáticos. Ese proceso de transición hacia una diplomacia en red se ha visto impulsado por la proliferación de actores estatales y no estatales en la esfera política y diplomática. Esto ha llevado a una democratización de la actividad diplomática y a la expansión del acceso a la esfera internacional para la sociedad civil, gracias a la comunicación electrónica, el bajo costo del acceso a Internet, y la demanda de transparencia y libertad de acceso a información sensible (p.40). Así pues, Zabala Roldán identifica, citando a Rashica, que la diplomacia digital tiene distintos objetivos, tales como la gestión del conocimiento, la diplomacia pública, la gestión de la información, las comunicaciones consulares, la respuesta a catástrofes, la promoción de la libertad en Internet, el aprovechamiento de recursos externos y la planificación de políticas (p.42).

Por otro lado, se enfatiza que la diplomacia digital representa un desafío para la precisión y la consolidación del conocimiento en este campo, dado el uso aleatorio y simultáneo de distintos términos para referirse a fenómenos similares. Con este enfoque, el autor saca a la luz el concepto de ciberdiplomacia, calificándola “como una zona híbrida con manifiestos componentes de la diplomacia pública digital, como la utilización de las redes sociales, en conjunto con la introducción de aspectos de seguridad, como la desinformación y la proliferación de algoritmos como instrumentos de control de conversaciones online” (p.48). Finalmente alude al informe del Parlamento Europeo titulado «*Artificial Intelligence diplomacy: Artificial Intelligence governance as a new external policy tool*», en virtud del cual se afirma que la Inteligencia Artificial tiene un enorme potencial para alterar el orden internacional en áreas estratégicas en las que la UE debe actuar en consecuencia: competencia sino-estadounidense, control autoritario y nacionalismos, aumento de poder del sector privado frente al Estado y el poder militar y el sector de la defensa (p. 60).

El Capítulo II de la obra se centra en la estructura, gobernanza y funciones del SEAE, que acertadamente escoge el autor como estudio práctico idóneo

para aplicar los debates teóricos sobre diplomacia digital. Siguiendo esta lógica, analiza su autoridad, estructura institucional, función diplomática y su rol estratégico en la política exterior de la UE (p. 65). Además, explora cómo este servicio ayuda a los órganos de gobierno de la UE en política exterior, vinculándolo con el paradigma de transformación digital. Zabala Roldán revisa cuidadosamente los fundamentos de la acción y política exterior de la UE, destacando la importancia de la Política Exterior y de Seguridad Común (PESC), establecida por el Tratado de Maastricht de 1992 y reforzada por el Tratado de Lisboa de 2007. Tras recordar los objetivos de la PESC, entre los que destaco la defensa de valores comunes, la seguridad, el mantenimiento de la paz y la promoción de la cooperación internacional, opta el autor por introducir la estructura diplomática actual de la UE, resaltando la creación del SEAE y la figura del Alto Representante para Asuntos Exteriores y Política de Seguridad (AR/VP), como un paso decisivo hacia una diplomacia europea más coherente y efectiva. Se discuten las capacidades civiles y militares bajo la Política Común de Seguridad y Defensa (PCSD), y se relacionan de forma exhaustiva los instrumentos y agencias relevantes para la ejecución de esta política. Entre ellos, sobresale el Comité Político y de Seguridad (CPS), el Comité Militar de la UE (EUMC), la Agencia Europea de Defensa (EDA) y la Capacidad Civil de Planificación y Conducción (CPCC). Afirma el autor que “estos instrumentos se utilizan en combinación y se adaptan a las circunstancias particulares de las crisis y ajustando su uso a la evolución de las condiciones” (p. 76). A continuación, profundiza sobre la incidencia de la Brújula Estratégica de Política Exterior², que describe un “panorama de seguridad europeo y mundial más volátil, complejo y fragmentado que nunca debido a las amenazas de múltiples niveles” (p. 80). En este contexto, proclama el autor que la diplomacia digital tiene y tendrá un rol fundamental en la lucha contra las amenazas híbridas, ciberataques, campañas de desinformación e injerencias directas en procesos electorales. Prosigue con un análisis en perspectiva histórica de la diplomacia europea, desde su concepción hasta la creación del SEAE, como instrumento al servicio de un plan europeo de “protagonismo internacional, de defensa del multilateralismo y un orden

² Consejo de la Unión Europea. Una Brújula Estratégica para la Seguridad y la Defensa - Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. 7371/22. 21 de marzo de 2022. Disponible en: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf>.

internacional basado en normas” (p. 83).

Finalmente, describe profusamente el organigrama institucional del SEAE, así como el elenco de funciones genéricas y específicas, como el *EU Cyber Diplomacy Toolbox*. A nuestro juicio, hubiera sido más coherente (i) en primer lugar, incorporar este análisis de su evolución histórica después de anunciar los fundamentos de la PESC, y (ii) en segundo lugar, combinar en la parte final del capítulo la estructura institucional actual del SEAE y sus funciones con las estrategias y acciones contempladas en la Brújula Estratégica de Política Exterior. De esta forma, habría quedado más claro que lo realmente importante son los fines (por ejemplo, combatir las amenazas híbridas), para cuyo cumplimiento se disponen de múltiples medios (por ejemplo, la estructura orgánica del SEAE). Claro está, si esta era la intención del autor.

El Capítulo III se enfoca en identificar los programas e iniciativas de diplomacia digital del SEAE en el contexto de la pandemia de la COVID-19 y cómo estas iniciativas se han adaptado o surgido en respuesta a la crisis sanitaria global. A continuación, se relacionan las medidas descritas más significativas:

- La Estrategia Conjunta de Ciberseguridad del SEAE, orientada a mejorar la resistencia, la autonomía tecnológica y el liderazgo de la UE en los debates internacionales sobre el futuro del ciberespacio. Este marco incluye una “estrategia de ciberdiplomacia para hacer frente a incidentes cibernéticos accidentales o deliberados” la aplicación del *EU Cyber Diplomacy Toolbox* y la *EU Cyber Diplomacy Network* (p. 99).
- Las Campañas Estratégicas de Comunicación del SEAE durante 2020, mediante actividades de comunicación y sensibilización durante la pandemia, incluyendo la campaña #WeTakeYouHome para la repatriación de ciudadanos de la UE.
- El 22º Foro de Derechos Humanos UE-ONG sobre el impacto de las nuevas tecnologías en los derechos humanos.
- Un Análisis sobre las implicaciones de la COVID-19 en seguridad y defensa de la UE, destacando la agudización de amenazas como el “terrorismo, la migración irregular, la delincuencia organizada, y las actividades cibernéticas maliciosas” (p. 103).
- La iniciativa *Team Europe* como respuesta de acción exterior a la pandemia, destacando la coordinación y apoyo entre la UE, Estados miembros (en adelante EE.MM.), e instituciones financieras europeas para

asistir a países y regiones afectadas. En este contexto, surge el proyecto *Digital4Development Hub* con el objetivo de promover la transformación digital en países socios.

– La Implementación del Marco de Acción Conjunta para combatir las amenazas híbridas, con un papel estratégico del SEAE en este ámbito y reforzar la lucha contra la desinformación, especialmente en los Balcanes Occidentales.

Finalmente, Zabala Roldán comenta brevemente la Alianza Internacional para un Enfoque de la IA Centrado en el Ser Humano (IA-AI), la transformación digital del SEAE, así como el avance de su agenda y transición digital, distinguiendo la importancia de la conectividad y la cooperación internacional en el contexto de la pandemia.

En el Capítulo IV de la obra objeto de análisis se recurre al Plan de Acción contra la Desinformación (en adelante PdA) en el contexto de la COVID-19 y al concepto de “infodemia” como caso de estudio. Zabala Roldán recoge la definición que la UE la confiere a la desinformación³, para luego incidir en el hecho de que la pandemia proporcionó un terreno fértil para la proliferación de desinformación. Posteriormente discute el fenómeno de la posverdad, no de forma amplia, sino centrado en la dificultad de ejercer la diplomacia digital frente a la información falsa. También nos recuerda que la hiperconectividad y las redes sociales aceleran la difusión de *fake news*, complicando el panorama de la desinformación. Con un enfoque ilustrativo, examina como la Federación de Rusia ha utilizado sus redes de influencia para debilitar sistemas democráticos europeos, en tanto que “su *information warfare* se dirige a debilitar la cohesión social y los sistemas políticos” (p. 119). Se analizan los reportes del SEAE sobre desinformación en la era COVID-19, destacando la desinformación viral en pequeños mercados mediáticos y la desconfianza generada en torno a las vacunas occidentales. Se menciona la influencia rusa y china en las campañas de desinformación sobre la COVID-19, poniendo en valor las tareas del *East Stratcom Task Force*⁴. Ajustándose al PdA, el autor explora la

³ «Toda información verificablemente falsa o engañosa que se crea, presenta y difunde para obtener un beneficio económico o para engañar intencionadamente al público, y que puede causar un daño público». Comunicación sobre la lucha contra la desinformación en línea, COM(2018) 236 final de 26 de abril de 2018, p. 4.

⁴ A este respecto destaca el proyecto *EUnDisinfo* (Unión Europea versus desinformación). Se creó en 2015 para pronosticar, abordar y responder mejor a las campañas de desinformación

naturaleza multifacética de la desinformación y describe las acciones y medidas que la UE, de la mano del SEAE, ha puesto en marcha para promover la seguridad en entornos físicos y digitales. Entre estas medidas se incluye la creación de oficinas y la implementación de estrategias digitales para fomentar la transparencia y la veracidad de la información, estrechar la cooperación con socios estratégicos y promover campañas de concienciación. También se hace hincapié en el refuerzo de “las capacidades del SEAE de detección, análisis y exposición de la desinformación extranjera” (p. 141).

El Capítulo sigue profundizando con minuciosidad y alto grado de detalle los reportes del SEAE sobre Desinformación en la era COVID-19. Entre los múltiples sucesos estudiados en la obra, destaco la intensificación, a principios de 2021, de las campañas de “desinformación patrocinada por Estados como Rusia o China, dirigida en particular a las vacunas desarrolladas por Occidente” (p. 137). El Reporte Anual 2021 de la oficina STRATCOM del SEAE recapituló cómo estas y otras narrativas relacionadas con COVID-19 se utilizaron para socavar la posición de la UE. A modo conclusivo, el autor sostiene que, aunque se han hecho avances significativos en la lucha contra la desinformación, persisten desafíos importantes. Asimismo, enfatiza la necesidad de implementar una diplomacia digital efectiva y estratégica con enfoque integrador, involucrando a diversos actores como “gobiernos, la sociedad civil y la industria privada” (p. 142), para combatir eficazmente la desinformación y fortalecer la seguridad regional y nacional.

El Capítulo V de la monografía está destinado a sintetizar las conclusiones, discusiones y recomendaciones sobre la estructura, alcance, objetivos y actividades de la diplomacia digital de la UE, enfocándose en el SEAE. En sus conclusiones, el autor hace un esfuerzo por resumir en escuetas líneas los aspectos más significativos de su investigación. Por lo tanto, no nos parece oportuno efectuar más comentarios al respecto. En cambio, sí es sugerente la discusión del autor sobre las carencias y virtudes de la aplicación del PdA.

Respecto a las carencias, el autor critica que se utiliza un enfoque demasiado centrado en la seguridad y que no considera otras dimensiones importantes de la diplomacia digital, tales como la transformación digital interna o la mejora de la reputación de la UE. Igualmente, reprocha que la multiplicidad de actores en curso de la Federación de Rusia que afectan a la Unión Europea, sus Estados miembros y los países de la vecindad compartida. Véase: <https://euvsdisinfo.eu/> [consultado por última vez el 11.03.2024].

internos podría diluir la capacidad de respuesta rápida del SEAE, que a se vez tiende a adoptar un enfoque reactivo, en vez de proactivo. El autor cita con tino el informe especial del Tribunal de Cuentas Europeo sobre el impacto de la desinformación en la UE, si bien hubiera sido deseable integrar en el texto algunas de las críticas más acertadas del informe. Entre ellas, nos permitimos la licencia de reproducir las siguientes: “el PdA no incluye disposiciones en materia de coordinación para garantizar que las respuestas adoptadas por parte de la UE contra la desinformación sean coherentes y proporcionadas al tipo y a la escala de la amenaza” ni tampoco “se establecieron marcos de vigilancia, evaluación e información complementarios al Plan de Acción de la UE y al Plan de Acción para la Democracia Europea, lo que socava la rendición de cuentas”⁵.

En cuanto a las virtudes, se valora positivamente por el autor la orientación estratégica de los esfuerzos diplomáticos y de comunicación hacia Rusia y China, actores clave y principales difusores de campañas de desinformación relacionadas con la pandemia. También se reconoce que la implementación del PdA durante la pandemia ha incluido elementos significativos de diplomacia pública digital. Un ejemplo destacado es la campaña «*Think Before You Share*», que se desplegó en países al este de Europa, alcanzando a 14 millones de personas (p. 150). Otros de los aspectos positivos del PdA es su contribución a la aplicación de sanciones contra individuos y organizaciones responsables de ciberataques contra la UE o sus EE.MM. Desde nuestro punto de vista, habría adquirido mayor notoriedad estas afirmaciones si se hubieran acompañado de casos reales, habida cuenta que durante el año 2020 se produjeron ciberataques de indudable magnitud, públicamente conocidos como “WannaCry”, “NotPetya” y “Operation Cloud Hopper” o el intento de ciberataque contra la Organización para la Prohibición de las Armas Químicas (OPAQ). De hecho, fue la primera vez que el Consejo de la UE decidió “imponer medidas restrictivas contra seis personas y tres entidades responsables de diversos ataques informáticos”⁶.

⁵ TRIBUNAL DE CUENTAS EUROPEO (2021). *El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada. El Informe especial, N.º 09, 2021*, Oficina de Publicaciones. <https://data.europa.eu/doi/10.2865/89515>, párrs. 110 y 111.

⁶ Véase la nota de prensa de 30 de julio de 2020: <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/> (consultado el 25 de marzo 2024).

Finalmente, la obra concluye con una serie de recomendaciones para mejorar la respuesta diplomática digital de la UE, sugiriendo que se debe prestar atención no solo a la desinformación proveniente de actores externos como Rusia y China, sino también a la que surge dentro de la UE (recomendación n° 1, p. 151). De igual forma se recomienda una actualización de la terminología asociada a la desinformación para reflejar mejor su naturaleza y origen. A nuestro parecer, aquí el autor no desarrolla con la amplitud que merecen los conceptos infodemia, desinformación e información errónea. En su capítulo IV acude a las definiciones manejadas por la OMS y por algunos autores aislados⁷ y se limita a afirmar que, a diferencia de la información errónea, la desinformación “sí debe contemplar la creación, presentación y diseminación de información falsa con el propósito de obtener algún tipo de beneficio o causar un daño público” (p. 153). Seguidamente se esboza una serie de recomendaciones relativas al desempeño del SEAE. En este sentido, se propone que ha de adoptar un papel más estratégico y activo en la configuración de la política exterior de la UE en lo digital (recomendación n° 4), que participe en la actualización del Código de Prácticas contra la Desinformación (recomendación n° 5) y que se convierta en un laboratorio de ideas para la diplomacia digital (recomendación n° 6). Por último, se acentúa la importancia de la cooperación transatlántica en diplomacia digital para enfrentar desafíos comunes y promover un enfoque coherente y coordinado (recomendación n° 7).

En nuestra opinión, hubiera sido conveniente haber tratado, o al menos haber mencionado, algún otro gran reto en la materia. Entre ellos, indicamos a efectos meramente ilustrativos, el establecimiento de normas internacionales para la gobernanza del ciberespacio, el efecto Bruselas de la UE en privacidad y protección de datos de carácter personal u otros aspectos críticos relativos a la seguridad cibernética. Estos son también aspectos que inciden directamente en las acciones de la UE dirigidas a lidiar con los efectos adversos de la pandemia, como las tácticas de desinformación analizadas en la obra. Igualmente, se ha puesto de manifiesto, especialmente en el Capítulo I, la utilización de narrativas estratégicas en redes sociales, como Twitter (actualmente X), para gestionar la

⁷ Véase FAJARDO TRIGUEROS, C., and RIVAS-DE-ROCA, R., ‘La acción de la UE en España ante la “infodemia” de desinformación por el COVID-19’, *Revista de estilos de aprendizaje*, 2020, Vol. 16, N° 26, <https://idus.us.es/handle/11441/101941>; Hoja Informativa “Entender la infodemia y la desinformación en la lucha contra la COVID-19”, https://iris.paho.org/bitstream/handle/10665.2/52053/Factsheet-Infodemic_spa.pdf.

reputación de la UE. En esta línea, la obra ganaría con alusiones en materia de perspectiva de género de la diplomacia digital como un medio para el cambio de política exterior⁸. Otro de los aspectos que hubiera perfeccionado la monografía es la referencia al marco de la UE de la Salud, que se inserta en una de las seis prioridades de la Comisión Europea para el período 2019-2024, esto es, en la «Promoción de nuestro modo de vida europeo»⁹. Más aún, cuando uno de los pilares de la investigación llevada a cabo es precisamente la pandemia, que entronca directamente con las políticas de salud pública. De hecho, es abundante la bibliografía que profundiza sobre el rol de la Comisión Europea en los cambios estructurales para combatir la pandemia, incluyendo la lucha contra la información errónea¹⁰.

En general, el enfoque de la UE hacia la diplomacia digital y la ciberdiplomacia es multifacético y sus retos reflejan tanto las complejidades inherentes al espacio digital como los desafíos específicos de la UE en calidad de actor internacional. Zabala Roldán navega con solvencia sobre muchos de estos retos, destacando las acciones propagandísticas y la desinformación proveniente de Rusia y China, la adaptación a las herramientas del ciberespacio y la cooperación con múltiples actores, incluyendo terceros Estados, sector privado y sociedad civil. En definitiva, la obra plantea interesantes reflexiones sobre la diplomacia digital y a ciberdiplomacia como herramientas estratégicas para articular la identidad de la UE y reforzar los mensajes políticos centrales.

Francisco Antonio Domínguez Díaz
Profesor Sustituto Interino, Universidad de Cádiz

⁸ Véase, AGGESTAM, K., BERGMAN ROSAMOND, A., and HEDLING, E., 'Feminist Digital Diplomacy and Foreign Policy Change in Sweden', *Place Branding and Public Diplomacy*, 2022, Vol. 18.

⁹ Véase: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life_es (consultado el 28 de marzo de 2024).

¹⁰ Al respecto, resalta el estudio de EERENS, D., HRZIC, R., and CLEMENS, T., 'The Architecture of the European Union's Pandemic Preparedness and Response Policy Framework', *European Journal of Public Health*, 2023, Vol. 33, Issue 1.