Integración Regional & Derechos Humanos / Revista Regional Integration & Human Rights / Review

Año XIII – Nº 1 – 1º semestre 2025

Centro de Estudios Integración Regional & Derechos Humanos

IR & DH

Facultad de Derecho Universidad de Buenos Aires

Integración Regional & Derechos Humanos /Revista Regional Integration & Human Rights /Review

Revista del Centro de Estudios
Integración Regional & Derechos Humanos
Facultad de Derecho
Universidad de Buenos Aires – Argentina

Año XIII – N°1 – Primer Semestre 2025

ISSN: 2346-9196

Av. Figueroa Alcorta 2263 (C1425CKB)
Buenos Aires - Argentina
revistairydh@derecho.uba.ar

Índice

Sección Especial / *“Derecho, IA y nuevas tecnologías”*

EL DERECHO HUMANO A LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA: DESAFÍOS DE IMPLEMENTACIÓN E INTERRELACIONES CON LOS DERECHOS FUNDAMENTALES

Juliana Estévez[1]

Fecha de recepción: 27 de mayo de 2025
Fecha de aceptación: 3 de julio de 2025

Resumen

El presente artículo analiza la emergente necesidad de conceptualizar y potencialmente consagrar un derecho humano a la ciberseguridad en el marco jurídico de la UE. Se exploran los complejos desafíos de implementación –prácticos, jurídicos e institucionales– que tal derecho plantearía, considerando el robusto y evolutivo entramado normativo existente, que incluye el Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689), la Directiva NIS2 (Directiva (UE) 2022/2555), el Reglamento de Ciberresiliencia (Reglamento (UE) 2024/2847), el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679), la Ley de Datos (Reglamento (UE) 2023/2854) y la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva 2002/58/CE). Se incorpora jurisprudencia relevante del Tribunal de Justicia de la Unión Europea (TJUE) y se hace referencia a informes y estrategias de instituciones europeas. Asimismo, se examina la intrincada relación de un eventual derecho a la ciberseguridad con otros derechos fundamentales reconocidos, como la protección de datos, la privacidad y la libertad de expresión, identificando sinergias y tensiones. Finalmente, se aborda la ciberseguridad en el contexto de los derechos humanos de cuarta generación.

Palabras clave: Ciberseguridad, Derechos Humanos, Unión Europea, Implementación, Derechos Fundamentales, Protección de Datos, Privacidad, Libertad de Expresión, Reglamento de IA, NIS2, Reglamento de Ciberresiliencia, RGPD, Ley de Datos, Directiva ePrivacy, Derechos de Cuarta Generación, TJUE, Estrategia de Ciberseguridad UE.

[1] Abogada (Universidad de Buenos Aires, Argentina). Profesora de Derecho de la Integración (Universidad de Buenos Aires, Argentina).

Title: THE HUMAN RIGHT TO CYBERSECURITY IN THE EUROPEAN UNION: IMPLEMENTATION CHALLENGES AND INTERRELATIONS WITH FUNDAMENTAL RIGHTS

Abstract

This article analyzes the emerging need to conceptualize and potentially enshrine a human right to cybersecurity within the legal framework of the European Union. It explores the complex implementation challenges – practical, legal, and institutional – that such a right would pose, considering the robust and evolving existing regulatory landscape, which includes the Artificial Intelligence Act (Regulation (EU) 2024/1689), the NIS2 Directive (Directive (EU) 2022/2555), the Cyber Resilience Act (Regulation (EU) 2024/2847), the General Data Protection Regulation (Regulation (EU) 2016/679), the Data Act (Regulation (EU) 2023/2854), and the ePrivacy Directive (Directive 2002/58/EC). Relevant case law from the Court of Justice of the European Union (CJEU) is incorporated, and reference is made to reports and strategies from European institutions. Furthermore, it examines the intricate relationship of a potential right to cybersecurity with other recognized fundamental rights, such as data protection, privacy, and freedom of expression, identifying synergies and tensions. Finally, cybersecurity is addressed in the context of fourth-generation human rights.

Keywords: Cybersecurity, Human Rights, European Union, Implementation, Fundamental Rights, Data Protection, Privacy, Freedom of Expression, AI Act, NIS2, Cyber Resilience Act, GDPR, Data Act, ePrivacy Directive, Fourth-Generation Rights, CJEU, EU Cybersecurity Strategy.

I. Introducción

La transformación digital ha reconfigurado indeleblemente las sociedades contemporáneas, convirtiendo el ciberespacio en una dimensión fundamental de la vida económica, social y personal. La Unión Europea (UE) ha estado a la vanguardia de la regulación de este espacio, impulsada por una visión estratégica reflejada en documentos como la "Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro" de 2013 (COMISIÓN EUROPEA, 2013) y la más reciente "Estrategia de Ciberseguridad de la UE para la Década Digital" de 2020 (COMISIÓN EUROPEA, 2020). Estas estrategias han cimentado un creciente corpus normativo que busca un delicado equilibrio entre la innovación tecnológica, la seguridad digital y la protección de los derechos fundamentales.

Instrumentos legislativos clave como el Reglamento General de Protección de Datos (RGPD) (Reglamento (UE) 2016/679), que establece normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos (PARLAMENTO EUROPEO & CONSEJO, 2016: art.1), y la Directiva sobre seguridad de las redes y sistemas de información (Directiva NIS), recientemente actualizada por la Directiva NIS2 (Directiva (UE) 2022/2555), han sentado las bases. A estos se suman propuestas y actos legislativos más recientes que abordan facetas específicas del entorno digital: el Reglamento de Inteligencia Artificial (RIA) (Reglamento (UE) 2024/1689), cuyo propósito es mejorar el funcionamiento del mercado interior mediante un marco jurídico uniforme para el desarrollo, la comercialización y el uso de sistemas de IA (PARLAMENTO EUROPEO & CONSEJO, 2024a: art 1); el Reglamento de Ciberresiliencia (CRA) (Reglamento (UE) 2024/2847), que establece requisitos horizontales de ciberseguridad para los productos con elementos digitales (PARLAMENTO EUROPEO & CONSEJO, 2024b: art. 1 a); la Ley de Datos (Reglamento (UE) 2023/2854), que armoniza las normas sobre la puesta a disposición de los datos de los productos y servicios conexos (PARLAMENTO EUROPEO & CONSEJO, 2023: art. 1); y la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva ePrivacy) (Directiva 2002/58/CE), que particulariza y complementa el RGPD en su sector (Artículo 1(2) de la Directiva ePrivacy). Este conjunto normativo evidencia un esfuerzo integral por parte de la UE para regular el ciberespacio (BYGRAVE, 2025; JIMÉNEZ SERRANÍA, s.f.:

p. 7). El Reglamento sobre la Ciberseguridad (Reglamento (UE) 2019/881) también juega un papel crucial al redefinir el mandato de ENISA[2] y establecer el marco europeo de certificación de la ciberseguridad (PARLAMENTO EUROPEO & CONSEJO, 2019: art. 1).

A pesar de la densidad y sofisticación de estos avances, la constante evolución de las ciberamenazas, la intrínseca vulnerabilidad de las infraestructuras digitales y la profunda dependencia social de los sistemas interconectados, junto con los emergentes desafíos que plantea la inteligencia artificial para la seguridad (COTINO HUESO & SIMÓN CASTELLANO, 2024), han alimentado un debate académico y jurídico sobre la necesidad de una capa adicional de protección: la conceptualización y eventual consagración de un derecho humano a la ciberseguridad en el ordenamiento jurídico de la UE (CHIARA, 2024; PANA, 2021: p. 200). Dicho derecho no solo buscaría reforzar y dotar de mayor coherencia a la normativa existente, sino que también podría ofrecer un anclaje iusfundamental para la protección integral de los individuos en el entorno digital.

El presente artículo se inscribe en este debate con el objetivo primordial de analizar dos dimensiones cruciales inherentes a esta propuesta: primero, los desafíos multifacéticos (jurídicos, prácticos e institucionales) que conllevaría su implementación en el complejo marco normativo de la UE; y segundo, su intrincada interrelación con otros derechos fundamentales ya reconocidos y consolidados en el acervo de la Unión. Adicionalmente, se explorará la noción de la ciberseguridad como un posible exponente de los derechos humanos de cuarta generación (BUSTAMANTE DONAS, 2001).

Para alcanzar estos objetivos, el análisis se estructurará en tres secciones principales. La primera sección se dedicará a una exploración detallada de los desafíos de implementación de un derecho fundamental a la ciberseguridad. Esto incluirá la problemática delimitación de su contenido y alcance, la atribución de

[2] "La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por el Reglamento de Ciberseguridad de la UE, la Agencia contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante sistemas de certificación de ciberseguridad, coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para los retos cibernéticos del futuro" (AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD [ENISA], s.f.)

responsabilidades entre actores estatales y privados, el diseño de mecanismos de supervisión eficaces y la garantía de una tutela judicial efectiva, sin olvidar las implicaciones para el mercado único digital. La segunda sección abordará la compleja red de interrelaciones entre un eventual derecho a la ciberseguridad y derechos fundamentales preexistentes, como el derecho a la protección de datos personales (Artículo 8 de la Carta de los Derechos Fundamentales de la UE (CDFUE) y RGPD), el derecho al respeto de la vida privada y familiar (Artículo 7 CDFUE y Directiva ePrivacy), y la libertad de expresión e información (Artículo 11 CDFUE). En este contexto, se examinarán las sinergias y tensiones previsibles, con especial atención a la jurisprudencia del TJUE y la necesaria ponderación de derechos. En esta misma sección, se contextualizará la ciberseguridad dentro del debate sobre los derechos de cuarta generación.

II. Desafíos de Implementación de un Derecho Fundamental a la Ciberseguridad en la UE

La aspiración de consagrar un derecho fundamental a la ciberseguridad en el ordenamiento de la Unión Europea, si bien responde a una necesidad sentida de protección reforzada en la era digital, se enfrenta a un conjunto de desafíos de notable envergadura en su implementación. Estos desafíos no son meramente teóricos, sino que se proyectan sobre las dimensiones jurídica, institucional y práctica, debiendo además articularse con un ya denso y dinámico ecosistema normativo. La UE ha tejido una red legislativa que incluye la Directiva NIS2 (DIRECTIVA (UE) 2022/2555), el Reglamento de Ciberresiliencia (REGLAMENTO (UE) 2024/2847), el Reglamento de IA (REGLAMENTO (UE) 2024/1689), el Reglamento sobre la Ciberseguridad (REGLAMENTO (UE) 2019/881) y la Ley de Datos (REGLAMENTO (UE) 2023/2854). Estos instrumentos ya persiguen, entre otros fines, asegurar un elevado nivel de ciberseguridad en el mercado interior. La introducción de un derecho fundamental, con su jerarquía normativa superior, exige una cuidadosa reflexión sobre su contenido, sus titulares y garantes, y los mecanismos para su efectividad.

II.i. Desafíos Jurídicos

La primera categoría de desafíos se sitúa en el plano estrictamente jurídico, comenzando por la delimitación del contenido y alcance del derecho. Un derecho a la ciberseguridad podría concebirse de diversas formas: como un derecho de prestación que exija una acción positiva de los poderes públicos para garantizar un entorno digital seguro; como un derecho de defensa frente a interferencias indebidas en la seguridad digital de los individuos; o, más probablemente, como un derecho complejo que combine ambas facetas (PANA, 2021: p. 249). La propia definición de "seguridad" en el ciberespacio es polisémica y evolutiva, sujeta a la constante emergencia de nuevas amenazas y a la diversidad de contextos tecnológicos y de uso (SERINI, 2024: p. 1; CHIARA, 2024: p. 1).

El Reglamento de Ciberresiliencia[3] (CRA), por ejemplo, define "producto con elementos digitales" como "*un producto consistente en programas informáticos o equipos informáticos y sus soluciones de procesamiento de datos remoto, incluidos los componentes consistentes en programas informáticos o equipos informáticos que se introduzcan en el mercado por separado*" (Artículo 3(1) de la CRA) y establece "requisitos esenciales de ciberseguridad" para estos productos, como la obligación de comercializarse "sin vulnerabilidades aprovechables conocidas" (Anexo I, Parte I, punto (2)(a) de la CRA) y de garantizar que "las vulnerabilidades puedan abordarse mediante actualizaciones de seguridad" (Anexo I, Parte I, punto (2)(c) de la CRA), a su vez, que los productos deben de garantizar "la protección contra el acceso no autorizado mediante mecanismos de control adecuados" (Anexo I, Parte I, punto (2)(d) de la CRA). Por su parte, el RIA exige para los sistemas de IA de alto riesgo que alcancen un "nivel adecuado de precisión, robustez y ciberseguridad" (Artículo 15(1) del RIA) y sean resilientes "frente a los intentos por parte de terceros no autorizados de alterar su utilización, comportamiento o rendimiento explotando las vulnerabilidades del sistema" (Artículo 15(5) del RIA). Un derecho fundamental a la ciberseguridad debería trascender la especificidad de productos o sistemas concretos, para articular un estándar de protección general, posiblemente

[3] Es pertinente aclarar que el Reglamento de Ciberresiliencia se encuentra vigente, pero los Estados de la Unión Europea poseen diversas etapas para acomodar su legislación (REGLAMENTO (UE) 2024/2847, 2024).

inspirándose en estos requisitos, pero confiriéndoles una dimensión iusfundamental.

Otro desafío crucial es la atribución de responsabilidades. En un ecosistema digital caracterizado por su transnacionalidad y la multiplicidad de actores –Estados, proveedores de infraestructuras, desarrolladores de software, fabricantes de hardware, proveedores de servicios digitales, y los propios usuarios–, determinar quién es el garante último de este derecho y quién responde por su vulneración resulta una tarea compleja (BOEKEN, 2024: p. 1). La CRA ya asigna responsabilidades detalladas a los "fabricantes", "representantes autorizados", "importadores" y "distribuidores" de productos con elementos digitales (Capítulo II de la CRA, Artículos 13-22). De forma análoga, el RIA establece un entramado de obligaciones para los "proveedores", "distribuidores", "importadores" y "usuarios" de sistemas de IA (Capítulo III, Sección 3 y Capítulo V, Sección 2 del Reglamento de IA). La Directiva NIS2 también responsabiliza a los órganos de dirección de las entidades esenciales e importantes de aprobar y supervisar la aplicación de medidas de gestión de riesgos de ciberseguridad (JIMÉNEZ SERRANÍA, s.f., p. 32). Un derecho fundamental podría exigir una ampliación o una jerarquización de estas responsabilidades, o incluso identificar nuevas categorías de sujetos obligados.

La doctrina ha debatido si un nuevo derecho a la ciberseguridad es redundante frente al derecho a la seguridad ya consagrado en el Artículo 6 de la CDFUE (CHIARA, 2024). Si bien este último podría interpretarse extensivamente para cubrir aspectos de la seguridad digital, la especificidad y la naturaleza transversal de las ciberamenazas podrían justificar un derecho autónomo y más detallado.

Finalmente, la relevancia del mercado único común en la UE añade una dimensión ineludible. Gran parte de la legislación europea en ciberseguridad,

incluyendo la CRA (Considerando 1)[4] y el Reglamento de IA (Artículo 1(1))[5], se fundamenta en el Artículo 114 del TFUE, buscando la armonización para facilitar la libre circulación de bienes y servicios digitales (CHIARA, 2024: p. 2). Un derecho fundamental a la ciberseguridad debería diseñarse e implementarse de manera que refuerce este objetivo, evitando la fragmentación normativa entre Estados miembros y la creación de barreras injustificadas al mercado único digital (BYGRAVE, 2025).

II.ii. Desafíos Institucionales y Prácticos

Desde una perspectiva institucional, la implementación de un derecho a la ciberseguridad plantea interrogantes sobre los mecanismos de supervisión y la tutela judicial efectiva. La UE ya cuenta con una red de autoridades, como las autoridades de protección de datos (APDs) bajo el RGPD, las autoridades competentes designadas bajo la Directiva NIS2, las autoridades de vigilancia del mercado bajo la CRA (Artículo 52 de la CRA), y las autoridades nacionales competentes junto con la Oficina Europea de IA bajo el Reglamento de IA (Artículos 70 y 64 y ss. del RIA). ENISA, fortalecida por el Reglamento sobre la Ciberseguridad (REGLAMENTO (UE) 2019/881), desempeña un papel central en la asistencia a los Estados miembros y las instituciones de la UE, el desarrollo de esquemas de certificación (Título III del Reglamento sobre la Ciberseguridad) y el apoyo a la

[4] "La ciberseguridad es uno de los principales retos para la Unión. El número y la variedad de dispositivos conectados aumentará exponencialmente en los próximos años. Los ciberataques constituyen un asunto de interés público, ya que tienen un impacto crítico no solo en la economía de la Unión, sino también en la democracia y en la salud y la seguridad de los consumidores. Por lo tanto, es necesario reforzar el enfoque de la Unión respecto a la ciberseguridad, abordar la ciberresiliencia a escala de la Unión y mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la introducción de productos con elementos digitales en el mercado la Unión. Deben abordarse dos problemas importantes que suponen un aumento de los costes para los usuarios y la sociedad: un bajo nivel de ciberseguridad de los productos con elementos digitales, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y la insuficiencia de la comprensión de la información y del acceso a ella por parte de los usuarios, que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura."

[5] "El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación."

cooperación operativa, como la secretaría de la red EU-CyCLONe (JIMÉNEZ SERRANÍA, s.f., pp. 10-11). La cuestión es si estas estructuras existentes, incluso con sus recientes refuerzos y la creación de nuevas entidades como la Oficina de IA, serían suficientes para supervisar un derecho fundamental de alcance transversal, o si se requeriría una nueva agencia o una reconfiguración significativa de las competencias actuales (PANA, 2021: pp. 108-118). Los esquemas europeos de certificación voluntaria de la ciberseguridad, como el EUCC (Reglamento de Ejecución (UE) 2024/482 de la Comisión) basado en criterios comunes (JIMÉNEZ SERRANÍA, s.f.: p. 19), son indicativos del enfoque actual, pero un derecho fundamental podría exigir mecanismos de aseguramiento más vinculantes.

La tutela judicial efectiva es otro componente esencial. Se necesitaría claridad sobre las vías de recurso (nacionales o europeas, como el TJUE) para los individuos en caso de vulneración de este derecho, y sobre los remedios disponibles. El RGPD (Artículo 79) y el Reglamento de IA (Artículos 79 y 85) ofrecen modelos en cuanto al derecho a un recurso judicial efectivo y el derecho a presentar reclamaciones, pero la naturaleza difusa de los daños en ciberseguridad podría complicar su aplicación.

En el plano práctico, la efectividad de un derecho a la ciberseguridad dependería de la disponibilidad de recursos técnicos y financieros considerables. Esto afectaría tanto a las autoridades públicas responsables de la supervisión y el cumplimiento, como a las entidades privadas, grandes y pequeñas, que tendrían que adaptar sus infraestructuras, sistemas y procesos. La UE ya reconoce una brecha en capacidades y profesionales de ciberseguridad (SERINI, 2024: p. 2), y un nuevo derecho intensificaría esta demanda. Iniciativas como los programas de trabajo de la Comisión para la certificación europea (COMISIÓN EUROPEA, 2024a) o los informes de ENISA buscan mejorar la preparación, pero la escala de un derecho fundamental impondría retos mayores. La "cooperación informativa" y una "consciencia situacional colectiva", aunque cruciales, son difíciles de materializar plenamente (SERINI, 2024: pp. 1-2).

Finalmente, el *"pacing 176eep176ema"* –el desfase entre la rápida evolución tecnológica y la capacidad de adaptación del derecho– (BOEKEN, 2024: p. 2) representa un desafío estructural. Un derecho fundamental a la ciberseguridad debería ser formulado con un alto grado de abstracción y neutralidad tecnológica

para mantener su relevancia y eficacia a lo largo del tiempo, adaptándose a amenazas y desarrollos tecnológicos emergentes sin caer en la obsolescencia.

III. Relación con Otros Derechos Fundamentales y la Noción de Derechos de Cuarta Generación

El reconocimiento de un derecho fundamental a la ciberseguridad en la UE no se produciría en un vacío iusfundamental, sino que entraría en diálogo –y potencialmente en tensión– con el robusto catálogo de derechos fundamentales ya consagrados, principalmente en la Carta de los Derechos Fundamentales de la UE (CDFUE). Este análisis requiere una cuidadosa ponderación, guiada por la jurisprudencia del TJUE, para identificar sinergias y gestionar conflictos. Además, es pertinente considerar la ciberseguridad en el marco conceptual de los derechos humanos de cuarta generación.

III.i. Derecho a la Protección de Datos Personales y Derecho al Respeto de la Vida Privada y Familiar

La conexión entre la ciberseguridad y los derechos consagrados en el Artículo 8 CDFUE (protección de datos personales) y el Artículo 7 CDFUE (respeto de la vida privada y familiar) es la más evidente y explorada. Una ciberseguridad efectiva es una condición habilitante esencial para la protección de los datos personales contra el acceso no autorizado, la alteración, la pérdida o la destrucción (Artículo 5(1)(f) y Artículo 32 del RGPD), y para la salvaguarda de la esfera privada frente a intrusiones indebidas (Artículo 5 de la Directiva ePrivacy)[6]. El RGPD, en su Artículo 32, impone a responsables y encargados del tratamiento la obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras, "la seudonimización y el cifrado de datos personales", "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento" y "un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento". El

[6] Dicho artículo refiere a la confidencialidad de las comunicaciones.

principio de "protección de datos desde el diseño y por defecto" (Artículo 25 del RGPD) subraya esta interdependencia.

No obstante, la implementación de medidas de ciberseguridad puede generar tensiones con estos mismos derechos. Técnicas como la monitorización del tráfico de red, el análisis de metadatos, la inspección profunda de paquetes (DPI) o la retención de datos para la investigación de incidentes (PANA, 2021: pp. 365-368) pueden implicar un tratamiento intensivo de datos personales y una injerencia en la privacidad de las comunicaciones. El Reglamento de IA, por ejemplo, reconoce la necesidad de tratar categorías especiales de datos personales para la detección y corrección de sesgos en sistemas de IA de alto riesgo, aunque sujeta a salvaguardias (Artículo 10(5) del RIA).

La jurisprudencia del TJUE, especialmente en relación con los Artículos 7, 8 y 52(1) de la CDFUE, es crucial. El Tribunal ha reiterado que el derecho a la protección de datos personales no es un derecho absoluto, sino que "debe ponderarse en relación con su función en la sociedad[7]". Como analiza PIZZOLO (2025), en casos como Schwarz v. Stadt Bochum (Asunto C-291/12)[8] y R.L. v. Landeshauptstadt Wiesbaden (Asunto C-61/22)[9], relativos a la inclusión de huellas dactilares (datos biométricos según el Artículo 4(14) del RGPD y el Artículo 3(34) de la Ley de IA) en pasaportes y documentos de identidad, el TJUE ha seguido un "recorrido interpretativo" de varios pasos para evaluar la justificación de las limitaciones. Este recorrido implica verificar que la injerencia:

- Esté prevista por una ley que sea clara y previsible.
- Respete el contenido esencial de los derechos a la vida privada y a la protección de datos. En R.L., el TJUE consideró que la inclusión de dos huellas en documentos de identidad no vulneraba la esencia de estos derechos.

[7] TJUE, sentencia de 9 de noviembre de 2010, *Volker und Markus Schecke y Eifert*, asuntos acumulados C-92/09 y C-93/09, ap. 48, véase que el Tribunal establece que el derecho a la protección de datos personales no es un derecho absoluto.

[8] TJUE, sentencia de 17 de octubre de 2013, *Michael Schwarz c. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670. En este asunto, el Tribunal analizó la conformidad con los artículos 7 y 8 de la CDFUE del Reglamento (CE) nº 2252/2004 en lo relativo a la obligación de incluir huellas dactilares en los pasaportes.

[9] TJUE, sentencia de 21 de marzo de 2024, *R.L. c. Landeshauptstadt Wiesbaden*, C-61/22, ECLI:EU:C:2024:251. Este caso abordó la legalidad de la inclusión obligatoria de dos huellas dactilares en los documentos de identidad bajo el Reglamento (UE) 2019/1157.

- Persiga objetivos de interés general reconocidos por la Unión o la necesidad de proteger derechos y libertades de terceros. En los casos citados, estos objetivos incluían la lucha contra la falsificación de documentos, la prevención de la entrada ilegal, y la lucha contra la delincuencia y el terrorismo.
- Sea necesaria y proporcionada para alcanzar dichos objetivos, recurriendo a la medida menos onerosa y asegurando que las desventajas no sean desproporcionadas. Esto implica examinar la idoneidad y necesidad de la medida, incluyendo la existencia de alternativas menos intrusivas y garantías contra el tratamiento abusivo, como la prohibición de centralización de los datos o su uso para fines distintos.

El razonamiento del TJUE, como subraya PIZZOLO (2025), *"resiste la normalización de las prácticas de vigilancia masiva bajo la apariencia de innovación tecnológica"* y afirma *"un modelo de regulación digital en el que la confianza, la legalidad y la contención son centrales"*. Un derecho a la ciberseguridad debería, por tanto, integrar estas exigencias jurisprudenciales, asegurando que las medidas adoptadas en su nombre sean compatibles con los Artículos 7, 8 y 52(1) de la CDFUE. La Ley de Ciberresiliencia, en su Considerando 32[10], ya anticipa sinergias con el RGPD en materia de normalización y certificación, así como la cooperación entre autoridades.

[10] "El presente Reglamento debe entenderse sin perjuicio del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, incluidas las disposiciones relativas a la implantación de mecanismos de certificación en materia de protección de datos y sellos y marcas de protección de datos a fin de demostrar la conformidad con ese Reglamento de las operaciones realizadas por los responsables y los encargados del tratamiento. Este tipo de operaciones podrían integrarse en un producto con elementos digitales. La protección de datos desde el diseño y por defecto, así como la ciberseguridad en general, son elementos clave del Reglamento (UE) 2016/679. Al proteger a los consumidores y a las organizaciones de los riesgos de ciberseguridad, los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento también contribuyen a mejorar la protección de los datos personales y la privacidad de las personas. Deben tenerse en cuenta las sinergias tanto en materia de normalización como de certificación de los aspectos relativos a la ciberseguridad a través de la cooperación entre la Comisión, las organizaciones europeas de normalización, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Comité Europeo de Protección de Datos creado por el Reglamento (UE) 2016/679 y las autoridades nacionales de supervisión de la protección de datos. También deben fomentarse las sinergias entre el presente Reglamento y el Derecho de la Unión en materia de protección de datos en el ámbito de la vigilancia del mercado y la ejecución de las normas. A tal fin, las autoridades nacionales de vigilancia del mercado designadas con arreglo al presente Reglamento deben cooperar con las autoridades responsables de supervisar la aplicación del Derecho de la Unión en materia de protección de datos. Estas últimas también deben tener acceso a la información pertinente para el desempeño de sus tareas."

III.ii. Libertad de Expresión e Información

La interrelación con la libertad de expresión e información (Artículo 11 CDFUE) también es dual. Por una parte, la ciberseguridad es un habilitador de este derecho, al proteger la disponibilidad e integridad de las plataformas digitales y los canales de comunicación contra la censura técnica (ej. Ataques de denegación de servicio) o la manipulación de contenidos.

Por otra parte, ciertas medidas de ciberseguridad, como el filtrado de contenidos, la eliminación de información considerada maliciosa o constitutiva de desinformación, o las restricciones de acceso a redes o servicios por motivos de seguridad, podrían interpretarse como limitaciones a la libertad de expresión. El Reglamento de Servicios Digitales (REGLAMENTO (UE) 2022/2065) ya regula las obligaciones de las plataformas en línea en la moderación de contenidos, buscando un equilibrio. El RIA, en su Artículo 50, impone obligaciones de transparencia para sistemas que generan "180eep fakes", exigiendo la divulgación de que el contenido ha sido generado o manipulado artificialmente, con excepciones para el ejercicio legítimo de la libertad de expresión y artística, siempre que se salvaguarden los derechos de terceros y no se induzca a error. Un derecho a la ciberseguridad debería, por tanto, incorporar salvaguardas robustas para que las medidas de seguridad no se conviertan en instrumentos de censura o restricción desproporcionada de la libertad de expresión, alineándose con los criterios del Artículo 52(1) CDFUE.

III.iii. La Ciberseguridad como Derecho de Cuarta Generación

La doctrina ha explorado la emergencia de una "cuarta generación" de derechos humanos, intrínsecamente ligada a los desafíos y oportunidades que plantea la sociedad tecnológica y la digitalización de la existencia humana. Estos derechos no surgen ex novo, sino que a menudo representan una reinterpretación o una expansión de los derechos tradicionales para hacer frente a nuevas realidades. Como argumenta BUSTAMANTE DONAS (2001), la tecnología "modifica el concepto de espacio o ámbito en el que se manifiestan, profundizan, y desarrollan los derechos humanos", exigiendo una reformulación conceptual.

En este marco, se ha propuesto que un derecho a la ciberseguridad, o a la "seguridad informática" o "paz cibernética", podría encuadrarse como un derecho de cuarta

generación. Su naturaleza sería tanto habilitadora –permitiendo el ejercicio seguro de otros derechos en el entorno digital (como el acceso a la información, la participación política, los servicios esenciales en línea)– como protectora –defendiendo a los individuos contra nuevas formas de vulnerabilidad y daño específicas del ciberespacio–. Este enfoque, aunque objeto de debate académico respecto a la utilidad de la categorización por "generaciones" de derechos, ofrece un marco conceptual valioso para reflexionar sobre las nuevas exigencias de protección que impone la era digital y para justificar la necesidad de un anclaje iusfundamental específico para la seguridad en el ciberespacio.

IV. Conclusiones

El análisis de la potencial consagración de un derecho humano a la ciberseguridad en el marco de la Unión Europea revela una iniciativa de considerable complejidad, pero también de creciente pertinencia. Dicha consagración no solo respondería a la escalada de ciberamenazas y a la profunda conexión de lo digital en todos los aspectos de la vida, sino que también se insertaría en un panorama legislativo europeo ya denso y en constante evolución, como lo demuestran el Reglamento de IA, la Directiva NIS2, el Reglamento de Ciberresiliencia, el RGPD, la Ley de Datos y la Directiva ePrivacy. Las estrategias de ciberseguridad de la UE y la jurisprudencia del TJUE, especialmente en casos como Schwarz y R.L., perfilan un compromiso de la Unión hacia un ciberespacio que, además de seguro, sea respetuoso con los derechos fundamentales.

Los desafíos de implementación identificados son sustanciales y multifacéticos. Desde una perspectiva jurídica, la delimitación precisa del contenido y alcance del derecho, la clara atribución de responsabilidades entre una miríada de actores públicos y privados, y su coherente articulación con el acervo normativo existente y los objetivos del mercado único digital, representan tareas de gran envergadura. El Reglamento de Ciberresiliencia, con sus requisitos esenciales para productos (Anexo I de la CRA), y el Reglamento de IA, con sus exigencias para sistemas de alto riesgo (Artículos 8-15 del RIA), ya establecen marcos de diligencia que un nuevo derecho fundamental debería complementar o subsumir. Institucionalmente, la supervisión de tal derecho exigiría una reflexión profunda

sobre el papel de ENISA (REGLAMENTO (UE) 2019/881), las autoridades nacionales competentes designadas bajo diversas normativas (NIS2, CRA, RIA, Ley de Datos), y la necesidad de mecanismos de tutela judicial efectiva que sean ágiles y accesibles. Los recursos técnicos, financieros y humanos necesarios para dar efectividad a este derecho, así como el persistente "*pacing problem*" entre tecnología y regulación, añaden capas de complejidad práctica.

La relación con otros derechos fundamentales es intrínsecamente compleja. Un derecho a la ciberseguridad exhibe sinergias evidentes con la protección de datos personales (Artículo 8 CDFUE; Artículo 32 y 25 del RGPD) y la privacidad (Artículo 7 CDFUE; Artículo 5 de la Directiva ePrivacy), actuando como un prerrequisito para su ejercicio efectivo. Sin embargo, las medidas técnicas y organizativas implementadas para asegurar la ciberseguridad pueden generar tensiones, como ha reconocido el TJUE, exigiendo una rigurosa ponderación basada en los principios de legalidad, necesidad y proporcionalidad (Artículo 52(1) CDFUE), tal como se desprende de su jurisprudencia (PIZZOLO, 2025). De forma similar, aunque la ciberseguridad puede salvaguardar la libertad de expresión e información (Artículo 11 CDFUE) al proteger la integridad de las plataformas, las medidas de control deben ser cuidadosamente calibradas para no devenir en formas de censura, considerando los equilibrios que ya intenta establecer el RIA.

La conceptualización de la ciberseguridad como un derecho de cuarta generación (BUSTAMANTE DONAS, 2001) proporciona un marco intelectual estimulante, subrayando su carácter instrumental y habilitador para el pleno disfrute de un amplio espectro de derechos en la sociedad digital interconectada.

En conclusión, si bien la idea de un derecho humano a la ciberseguridad en la UE es doctrinalmente atractiva y socialmente relevante, su materialización exigiría un esfuerzo legislativo y político considerable para superar los desafíos de implementación y para asegurar su integración armónica en el sistema de protección de derechos fundamentales de la Unión. En sentido, hay más interrogantes que certezas al momento de plantear una modificación a la Carta de Derechos Fundamentales de la UE.

Futuras líneas de investigación podrían explorar modelos específicos de gobernanza y supervisión para tal derecho, el desarrollo de criterios de ponderación

más detallados para resolver enfrentamientos con otros derechos, y un análisis comparado con otras jurisdicciones que estén abordando desafíos similares.

V. Bibliografía

BOEKEN, J. (2024). From compliance to security, responsibility beyond law. *Computer Law & Security Review, 52*, 105926. Accesible en: https://doi.org/10.1016/j.clsr.2024.105926

BUSTAMANTE DONAS, J. (2001). Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica. *CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación*, (1).

BYGRAVE, L. A. (2025). The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. *Computer Law & Security Review, 56*, 106071. Accesible en: https://doi.org/10.1016/j.clsr.2025.106071

Carta de los Derechos Fundamentales de la Unión Europea (CDFUE). (2012). *DO C 326, 26.10.2012, pp. 391–407*.

CHIARA, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review, 53*, 105961. Accesible en: https://doi.org/10.1016/j.clsr.2023.105961

COMISIÓN EUROPEA. (2013). *Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*.

- (2020). *Estrategia de Ciberseguridad de la UE para la Década Digital*.
- (2024a). *Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024* (DO L, 2024/482, 7.2.2024).
- (2024b). *Union Rolling Work Programme for European cybersecurity certification*.

COTINO HUESO, L., & SIMÓN CASTELLANO, P. (Dirs.). (2024). *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*. Aranzadi.

DIRECTIVA (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 (Directiva NIS2). *DO L 333, 27.12.2022.*

DIRECTIVA 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la

intimidad en el sector de las comunicaciones electrónicas. *DO L 201, 31.7.2002.*

JIMÉNEZ SERRANÍA, V. (s.f.). *Aspectos legales y regulatorios de la ciberseguridad*. doinGlobal. [Material de lectura del Curso Superior en Derecho Oficial de Protección de Datos y Ciberseguridad].

MANTELERO, A. (2022). *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. T.M.C. Asser Press.

PANA, A. C. (2021). *La Seguridad Cibernética y los Derechos Humanos: Los límites de la restricción de derechos humanos para la protección del espacio cibernético* [Tesis doctoral, Universidad Carlos III de Madrid].

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2016). *Reglamento (UE) 2016/679, 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)*. DO L 119, 4.5.2016, pp. 1–88. Accesible en: https://eur-lex.europa.eu/eli/reg/2016/679/oj

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2019). *Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a ENISA (la Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad)*. DO L 151, 7.6.2019, pp. 15–69. Accesible en: https://eur-lex.europa.eu/eli/reg/2019/881/oj

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2023). *Reglamento (UE) 2023/2854, de 13 de diciembre de 2023, relativo a normas armonizadas sobre el acceso y uso justo de los datos (Ley de Datos)*. DO L 2023/2854, 22.12.2023. Accesible en: https://eur-lex.europa.eu/eli/reg/2023/2854/oj

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2024a). *Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican determinados reglamentos (Ley de Inteligencia Artificial)*. DO L 2024/1689, 12.7.2024. Accesible en: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2024b). *Reglamento (UE) 2024/2847, de 23 de octubre de 2024, relativo a requisitos horizontales para la ciberseguridad de los productos con elementos digitales (Ley de Ciberresiliencia)*. DO L 2024/2847, 20.11.2024. Accesible en: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

PIZZOLO, C. (2025). AI, biometric data, and the effective protection of fundamental rights in the recent ECJ case-law. *Unión Europea e Diritti*, 1/2025.

RUSSELL, S. J., & NORVIG, P. (2010). *Artificial Intelligence: A Modern Approach* (3.ª ed.). Prentice Hall.

SERINI, F. (2024). Collective cyber situational awareness in EU. A political project of difficult legal realisation? *Computer Law & Security Review, 55*, 106055. Accesible en: https://doi.org/10.1016/j.clsr.2023.106055

Todas nuestras actividades en:
www.derecho.uba.ar/institucional/centro-estudios-integracion-regional-y-ddhh/